www.intersec.co.uk

intersec

The Journal of International Security

May 2020

SECURITY IN A CRISIS

Lessons to be learned from COVID-19

FACE TIME

The future of facial recognition biometrics

POLMIL®

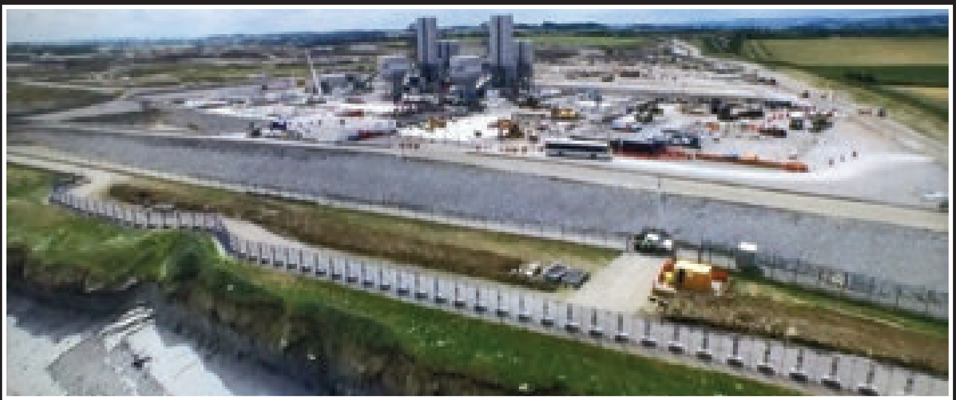
ON-GROUND RELOCATABLE SECURITY FENCING

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 5
May 2020

Cover photograph: Shutterstock.com

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

Three or four months ago hardly anyone had ever heard of digital conferencing tool Zoom, and yet now the video-call app is said to be worth in excess of $29-billion. It's funny how a global pandemic can change one's fortunes. But while the app that's enabled friends and families and work colleagues to try and maintain a semblance of normality during an extended period of lockdown has enjoyed an almost unprecedented increase in popularity, the cracks quickly began to show.

Firstly, there was the rather thorny subject of users' data. As is so often the case with such stories, whenever privacy and data are mentioned you can't pretty much guarantee that Facebook won't be far away. And so it proved when analysis by *Vice* discovered that the iOS app version of the tool was sending analytic data to Facebook, even if the user in question didn't have a Facebook account – in spite of the fact that this is not addressed in Zoom's privacy policy. In fairness to the company, it apologised when the issue was raised and promptly updated the app to right the wrong. But the problems didn't stop there.

Zoombombing entered the public lexicon not long after as trolls utilised weaknesses in the app to jump on board other people's conversations and then bombard them with anything from pornography to inappropriate images. Perhaps the most high-profile example being when The Verge's Casey Newton and investor Hunter Walk hosted their WFH Happy Hour public zoom call, only for trolls to bombard the unassuming participants and screenshare a series of offensive pornographic material. Attempts to curtail the attack were thwarted as the perpetrator simply re-entered the call under a new name and then screenshared more unwelcome material. In the end, the hosts were forced to abandon the call rather than subject viewers to more. The problem originated from Zoom's original policy that "The host does not need to grant screenshare access for another participant to share their screen". However, this option can easily be disabled in the settings or admin controls of a call.

And then there was the case of British Prime Minister and walking accident Boris Johnson who immediately undermined the historical significance of the very first virtual cabinet meeting by tweeting a screenshot with the entry code and password clearly legible so that anyone could join.

Obviously, considerable changes in circumstances such as those that we've all recently experienced thanks to COVID-19, mean that there are going to be teething problems and the odd stumble along the way. And perhaps Boris' blunder served as a timely reminder that properly looking into a video conferencing tool (or any other piece of software you intend to use for your organisation, in fact) and examining the implications of using it are absolutely vital. Going through the privacy policy of the provider, its third-party security certifications and terms, where it is based – and so what data jurisdiction it offers – and where the software was developed with a fine comb should be the bear minimum of requirements. You can read more about security during a crisis on page 16.

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: May 2020

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

May 2020
www.intersec.co.uk

intersec

Features

Regulars

8

12

16

22

28

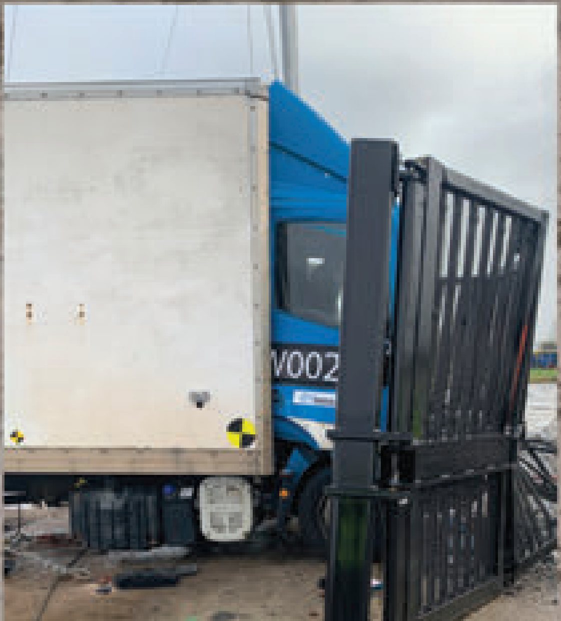
32

34

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

Trust China at your own cost

Major General Julian Thompson CB OBE Principal Consultant Editor

"Don't trust China. Ever." This is the advice given by a former senior diplomat in April. As further information about the source and spread of Coronavirus emerges, the more strongly I believe the blend of 'cock-up' and conspiracy that I wrote about last issue, is at the root of the current pandemic. It has all the hallmarks of 'cock-up' and conspiracy. The fate of several whistle blowers in China should be proof enough that there is a conspiracy of silence: if you do not play along you are for the chop. Here one is criticising the system of Government not the race of the population.

Not believing what you see or hear is often the result of 'mirror imaging'. Because you would not lie and dissemble, you cannot believe that anyone else would. History is littered with examples of democratic governments simply not believing what the evidence is telling them, because mirror imaging results in them being unable to grasp the extent of the ruthlessness and corruption at the heart of a regime such as the one that currently rules in China.

The decision to allow Huawei access to the UK's 5G network has its roots in mirror imaging on the part of those who authorised it, linked to Britain's extensive trade relationship with China, and increasing reliance on this relationship, which the Chinese are quick to use as a weapon. A recent example being the arrival of 300 ventilators from China, forcing a senior British minister to soften his earlier criticism of the Chinese role in the spread of Coronavirus. The mirror imager's reaction to the despatch of these ventilators is probably, 'How kind and generous'. The cynics among us are not taken in. Especially if some of the boxes in previous shipments of medical equipment have been incorrectly labelled or contained defective equipment; either through incompetence or as a deliberate snub.

A rethink of the UK's relationship with China is long overdue. The Chinese see themselves as being in competition with the UK, as part of the 'West', which includes the United States. In these circumstances it is important to bear in mind that the only thing a regime such as China's can do wrong is to lose. Nothing, but nothing – moral considerations, humanity, veracity – will be allowed to stand in the way of winning.

The downstream effect of China's duplicity has hit one of her close allies hard. Iran continued to allow flights to and from Wuhan long after the Chinese had admitted to the city being the source of the pandemic. The core of the epidemic in Iran appears to be the holy city of Qom. Twenty million Iranians and over two million foreign pilgrims visit every year. Several thousand Chinese share overcrowded accommodation with huge numbers of religious students from a range of countries. The Iranian Government delayed quarantining Qom until March. Meanwhile it accused the old enemies, the USA and Israel, for spreading the virus, while delaying closing religious shrines for weeks. Even now, people still visit. The Iranian Revolutionary Guard Corps has issued threats of dire retribution to those who query the statistics issued by the Ayatollahs.

Picture credit: Getty

COVID-19 has all the hallmarks of both cock-up and conspiracy as far as China's involvement is concerned

A round up of other Gulf States and the malevolent effect of the pandemic on their economies is revealing. The Iranians have exercised considerable influence in neighbouring Iraq ever since the US-led invasion in 2003, which toppled Saddam, thereby removing a much-needed brake on Iranian activities in the Gulf. Now Iranian 'influence' is not confined to propagating Shia terrorism across the porous border with Iraq, but includes the spread of Coronavirus to Iraq whose medical services are in an even worse state than Iran's. Both Iran and Iraq are badly hit by the steep drop in oil prices, and in the case of Iran by US sanctions.

Saudi Arabia is in a better position. With large financial reserves and other natural resources it can borrow. Saudi also has an excellent health infrastructure. The Saudis also learned the lesson of the Middle East Respiratory Syndrome (MERS) outbreak in 2012, and closed mosques and public places quickly. The cancellation of pilgrimages and imposition of curfews along with closure of borders had been followed by other Arab Gulf states.

The aftermath of the pandemic bodes ill for the Gulf Region, not least as the former senior diplomat quoted earlier has remarked: "The expectation of Gulf nationals that their governments would look after their needs from the cradle to the grave already looked out-dated. Now they seem delusional."

On doing business with China; continue to deal with them, if it is in our mutual interest, but in the words of the diplomat quoted earlier: "We need to make sure it really is [in our interest]. Meanwhile, distrust and verify."

Picture credit: Getty

FACING THE FUTURE

Timothy Compston *considers where facial recognition is heading.*

When it comes to biometrics for security there is little doubt that facial recognition is now at the forefront of 'frictionless' ways to authenticate the identity of individuals or to identify potential security threats. The speed of change here is breath-taking with a new report from The Carnegie Endowment for International Peace pointing out that at least 75 countries around the world are actively using AI tools like facial biometrics.

Putting specific figures on the dramatic upswing in the value of the global market for facial recognition, the research firm MarketsandMarkets is now forecasting a more than two-fold increase in value from $3.2-billion in 2019 to $7-billion by 2024 at a compound annual growth rate of 16.6 percent. MarketandMarkets points to the growing surveillance market, rising government and defence deployments and technological advances across various industry sectors as the key drivers for growth here. Recent analysis released by Adroit Market Research is even more bullish, predicting that the worldwide facial recognition market will exceed $12-billion by 2025. Where Adroit agrees with MarketsandMarkets is in the prediction that 3D facial recognition will have the largest slice of the market by the end of each forecast period. When touching on why 3D has the edge over 2D, MarketsandMarkets attributes this to the fact that this technique makes use of facial contours to identify and analyse various unique features in a human face. In addition, MarketsandMarkets notes the ease in detection of facial data from videos and 2D images and the way that 3D is least affected by illumination issues.

Authorities in San Francisco have said they will not allow facial recognition on their streets

Not surprisingly, there has been some push back in the UK, US and Europe by privacy campaigners with regards to facial recognition and some manufacturers of camera equipment have also been clarifying their positions on its roll-out. Interestingly the first report from the AI and Policing Technology Ethics Board set up by Axon – the body worn camera vendor – said that: "Face recognition technology is not currently reliable enough to ethically justify its use on body worn cameras. At the least, face recognition technology should not be deployed until the technology performs with far greater accuracy and performs equally well across races, ethnicities, genders and other identity groups." Beyond this some US cities – like San Francisco – have said they will not allow facial recognition on their streets and at one point the European Commission was even considering a ban on the use of facial recognition in public areas for up to five years, although this threat now seems to have receded.

Despite some reservations, as we head into a new decade we are seeing the latest generation of powerful facial recognition solutions being brought to market that offer higher speeds and a greater degree of accuracy than ever before, thanks to advances in computing power – AI and, specifically, a deep learning architecture – plus the move from 2D to 3D to cope with a wider range of viewing angles and lighting conditions. Crucially, this facial recognition revolution is helping to unlock a growing footprint of applications, whether it be to ramp up security for mobile banking; secure smartphones; control access at key facilities or, when combined with video surveillance footage, tackle crime in our smarter, safer cities. Perhaps a sign of things to come for facial recognition is the news that researchers in China have developed a 500-megapixel cloud camera that can collect detailed facial data of thousands of people in a crowd simultaneously and specific targets to be identified when integrated with AI and cloud computing technology for facial recognition.

Drilling down to specific applications, it is interesting to reflect on the announcement by Dubai Police that, under a new Artificial Intelligence (AI) network, thousands of video surveillance cameras from Dubai Government agencies are now going to provide a live feed to one central command centre. The Oyoon (eyes) initiative applies AI and facial recognition technologies to help spot crimes and incidents by analysing live video with no human intervention and enables the police to track criminals across the city by uploading their images into a database. Implemented over the past two years, the initiative is part of the Dubai 2021 Vision of a smart city and preparations for Expo 2020. The value of video surveillance cameras fitted with facial recognition technology and also vehicle licence plate readers in a city environment was underlined at the end of 2018 when it was reported that these type of cameras had helped Al Muraqqabat police station in Dubai to arrest 100 wanted people and 441 suspects that year.

Other police forces are keen to investigate the utility of facial recognition with London's Metropolitan Police Service confirming recently that it is to begin the operational use of Live Facial Recognition (LFR) technology from NEC. This, it points out, will be 'intelligence led' and deployed to specific locations in London to tackle serious crime like those involving guns and knives. There is also growing interest in investigating the practicalities of facial recognition to ramp up security for large-scale gatherings and last February software was piloted over two days during Carnival in Nice, France, a city which was the victim of a devastating terrorist attack back in 2016. For sporting events, Danish Superliga Football Club Brøndby IF, for example, has enhanced fan safety by using Panasonic's FacePRO facial recognition system (see *Intersec* March 2020) to prevent banned football hooligans from entering the stadium, while maintaining visitor privacy and complying with European Union General Data Protection Regulations.

An important development for facial recognition in recent times has been the advent of deep learning. With modern deep learning techniques, facial recognition engines such as SmartVis from Digital Barriers – that develops edge-intelligent solutions for the surveillance and security market – can identify users in most lighting conditions, even when they are not looking directly at the camera. As well as this, the company says that off-the-shelf cameras can be used, dramatically lowering the cost. The ability of solutions like these to leverage existing video surveillance cameras – and not have to rely on bespoke hardware or special calibration – opens up the potential, says the company, for facial recognition to be deployed on a much greater scale than before around areas like critical infrastructure and crowded places.

GATWICK AIRPORT WILL USE FACIAL RECOGNITION FOR ID CHECKS BEFORE PASSENGERS CAN BOARD

Another example of the additional intelligence and computer processing power now being applied to this form of biometrics for border control, access control and time and attendance comes in the shape of facial recognition innovator Aurora. The vendor has a proven track record when it comes to state-of-the-art biometrics having cut its teeth in applications like London Heathrow's Terminals 2 and 5 for airport passenger management. Specialising in identity verification for over a decade now, Aurora has moved from visible light systems through to pioneering the use of near infrared sensor technology to overcome the problems of varying ambient light conditions on a scene.

The application of deep learning-based artificial intelligence has proved to be a real game changer for Aurora's solutions. The key factor about deep learning in this field, according to Aurora is not just the scale of the performance enhancement but the speed at which it can be achieved. According to the vendor, the Neural Network it has developed to recognise faces has cut down the development time required to make significant performance gains from months to weeks.

With regards to banking, last September, Aion Digital, one of the fastest growing FinTech solution providers in the GCC, announced a partnership with Daon – a global leader in biometric identity technology – to introduce the IdentityX two-in-one platform for digital customer on-boarding. Rewinding to 2016 and Gulf Bank Kuwait asked Daon to provide biometric authentication within its mobile banking application via Daon's Identity Platform. By working with Daon the bank's customers were then able to login with biometrics using their fingerprint touch ID and 'Blinking to Bank' facial recognition, from anywhere in the world, to perform a wide array of banking transactions efficiently and securely.

In another step aimed at making ride-hailing a safe and secure experience for its users, in April 2017 we witnessed Dubai-based Careem, the Middle East's leading ride-hailing app, announce the integration of facial recognition technology into its technological framework. Powered by Digital Barriers, the back-end biometric identification system enables Careem to confirm its 'Captains' identity in real-time, eliminating all of the risks associated with fraudulent car ownership and possession.

THE WORLDWIDE FACIAL RECOGNITION MARKET IS PREDICTED TO EXCEED $12-BILLION BY 2025

Dubai International Airport (DXB) too has been leading the way for facial recognition with Princeton Identity's multi-modal biometric technology being deployed in the Emirates Airlines Terminals. This is in the form of its Access500e identity management kiosk module, a fast face and iris biometric capture device. Here in the UK, last September Gatwick Airport became the country's first to confirm that it would use facial recognition cameras on a permanent basis for ID checks before passengers can board planes.

Returning to the debate over the relative value of 2D or 3D facial recognition, advocates of 3D say that unlocking a third dimension in facial recognition means these solutions should be better able to cope with a range of viewing angles and even changes to people's appearance, from facial hair to sunglasses. A case in point is the approach taken by Artec ID – the 3D biometric division of Artec Group – and its Broadway 3D system, which provides a very accurate mesh (structured light pattern) to make high-speed recognition possible, against templates stored in a database, in less than a second. Developed for recognition on the move, according to Artec, the Broadway 3D system's ability to read information about face shape has been optimised for high throughput facilities like office buildings, factories and transport hubs where being non-contact makes it a 'very friendly' process.

Back on the streets, in the view of Dr Rustom Kanga, ceo at iOmniscient – a specialist in video content analysis – the true value of recognising faces in crowded urban areas is rarely achieved through deploying the technology on its own: "The value comes from being able to implement complex use cases with little effort. For instance, assume someone abandoned a bag in a crowded location. First, one has to detect the bag, then one has to know who left it there and to enrol them in the database. After that, this person needs to be tracked (across a city if necessary). Finally, when they are located the system needs to find the nearest police officer and tell them where to go, who to catch and why." In the end, Kanga believes that the ability to achieve such steps automatically underlines the fact that the recognition of faces is at its most powerful when it is employed alongside other technologies. In the end despite privacy concerns by some, the future for facial recognition is a bright one whether that be to make airports safer or to help secure our cities from criminal and terrorist elements ●

Timothy Compston is a journalist and PR professional who specialises in security and defence issues. He studied International Relations and Strategic Studies at Lancaster University, is PR Director at Compston PR and a previous Chairman of both the National PR Committee and CCTV Section PR Committee of the British Security Industry Association (BSIA).

It is predicted that by 2024 facial recognition will feature on 90 percent of smartphones

Kestrel TSCM ® Professional Software

Dynamic Trace Autonomous Platform (DTAP-GPS) ™ with Dimensional RF Geo-Location Propagation Modeling!

Signals Intelligence Support System ™

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

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

Kestrel TSCM ® Professional Software

A New Powerful Disruptive Technology Combination for the Modern Spectrum Warrior...

Placing the Technical Operator Decidedly Back in Command of the Analytical Process!

Introducing the new Signal Hound (SM200C) Spectrum Monitoring Receiver (20 GHz) with 10GbE SFP+ Connectivity that Supports a Wide Range of 10 GbE SFP+ Copper, Multi-Mode and Single-Mode Fiber-Optic Technology (up to 80 Kilometers) for Enhanced Network Reliability, Exceptional Deployment Platform Integrity, Security and Advanced Analytical Processing of Mission Critical Spectra Across a Global National Security Infrastructure.

The Signal Hound (SM200C) is Fully Supported by the Kestrel TSCM ® Professional Software for Mission Critical Technical Surveillance Countermeasures (TSCM), and Remote Spectrum Surveillance and Monitoring (RSSM) ™ Applications as Defined by the TSB 2000 (Technical) Standard ™ in Combination with a Suitable Laptop Computer Equipped with Thunderbolt ™ 3 Technology.

The Kestrel TSCM ® Professional Software in Combination with the Signal Hound (BB60C) and (SM200C) has become the Deployment Standard of the Modern Spectrum Warrior within the Private Sector, Government, Law-Enforcement, Military and National Security Infrastructure for enhanced TSCM, RSSM ™, SIGINT and ELINT Roles.

Actionable RF Intelligence at the Speed of Light!

Visit www.signalhound.com for Technical Specifications

Our Kestrel ® Certified Technical Operator (CTO) ™ Training is Available in Canada or Hosted at Your Facility!

100% Canadian Scientific Research and Software Engineering Development with Strictly Controlled Operator Centric Software Defined Radio (SDR) Source Code for Proven Radio-Frequency (RF) and Power Line (PL) Offensive and Defensive Monitoring and Surveillance Applications for Professional Technical Operators.

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: US Department of Defense

DEFENCE LOGISTICS

Graham Grose *considers three developments that will shape the strategy of military forces, original equipment manufacturers and in-service support providers in 2020*

In a setting where even gaining the smallest advantage can be the difference between mission success and failure, standing still has never been an option for military organisations and defence in-service support providers operating in this asset-intensive environment. From an asset and equipment perspective, military organisations have found themselves at an interesting crossroads: budgets have to be balanced between keeping older, but still vital assets in service and the attraction of shiny new investment in next-generation equipment; but this is set against a backdrop of a real shortage of personnel, particularly from a maintenance engineering point of view. As a result, the spotlight is falling directly on to military logistics and supply chain technology as a strategic enabler to deal with these issues.

Here I outline my three frontrunners for 2020 and beyond. As I put my predictions together, I realised that

The integration of AI will take centre stage in the development of aircraft

each development linked to the next in a positive way, to help defence forces looking to straddle both the past and present to maintain force readiness – a phrase we heard a lot about in 2019, and not always in a positive sense. Here is how they can turn the tables in the battle for readiness this year.

Artificial Intelligence (AI) is rapidly maturing to help improve the readiness of military equipment. Over the course of the last year or so, all of the US military services have launched predictive maintenance projects to help bridge the readiness gap. At the same time, some of the latest military assets in design are allowing for a whole new approach to mitigate the challenge of maintaining military assets through their service lives.

AI is expanding as a decision-making tool in the form of intelligent agents for data modelling and simulation. The arduous task of ingesting, aggregating and analysing raw data transmitted from aircraft is now being shortened as a result of this increased digitisation. As the F-35 Lightning II fighter jet continues to roll off production lines it is only natural that the industry will start to turn its attention to the sixth generation of fighter aircraft – the F-35 is just the beginning for high-tech stealth fighters. It is sustained by the Autonomic Logistics Information System (ALIS) – the most advanced sustainment solution currently in use for any military asset. ALIS provides a strong IT backbone, with the ability to turn data from multiple sources into actionable information.

At last year's IFS World Conference held in Boston USA, it was interesting to hear global security and aerospace company Lockheed Martin discuss the role of technology in the sustainment of advanced military platforms – in particular the length of time associated with the design of a 'next generation' military asset. In fact, IFS was involved in supporting the ALIS system as far back as 1999!

"If we were to do it all again, we would probably do something different, just like anything we're talking about and building today. If you were to roll the clock forward 15 years from now, it will be like: 'Why were they building those things like that?' It doesn't make any sense," explained Mark Adams, Logistics and Technology Development, Lockheed Martin, in his IFS World conference breakout session.

For the aircraft being developed into the new decade, given the long-term nature of designing, manufacturing and deploying complex new assets, it will be the integration of AI which will take centre stage in future sustainment software, from aircraft design, through to manufacturing and maintenance. Just look at the British-led Tempest and the Franco-German-Spanish Future Combat Air System or the UK Royal Navy's experimentation of an AI predictive maintenance system on its front-line Type 45 destroyers. AI is set to have a huge role in how those aircraft operate from both a maintenance and repair standpoint, but also operationally.

And it is fair to say AI is doing more than just helping sustain military equipment through secondary support and sustainment, it is already coming to the fore to actually operate military equipment too. Many predictions in recent years have focused on unmanned equipment, but the advancement a year on is in regard to the potential of grouping AI-controlled unmanned aerial vehicles (UAVs) together to provide a swarm – a development that is incredibly difficult to defend against from a military perspective.

We have seen the US military test simple Perdix drones dropped from F/A18 jets in the past, but the intention is that pilots will soon be able to leverage AI in the cockpit to control a small group of advanced drones flying nearby to perform sensing, reconnaissance and targeting functions. This takes control away from the ground, where drone operations are currently co-ordinated, and instead puts it in the hands of the warfighter themselves.

Drones in a military context have existed for a while, but a squadron of AI-controlled drones or drone wingmen is now a very real possibility. The Defense Advanced Research Projects Agency (DARPA) recently tested a swarm of autonomous drones and ground robots to assist with military missions, while the US Air Force has tested the XQ-58A Valkyrie 'Sidekick' drone, a robotic supersonic aircraft designed to be flown alongside a manned F-35. Alongside this, the US Air Force Research Laboratory's Skyborg programme is developing AI for a wider wingman-drone effort.

ONE MAJOR CHALLENGE IS PROLONGING THE LIFE OF OLDER ASSETS THAT ARE CURRENTLY IN SERVICE

The key benefits of this new age of warfare are, of course, tactical. The greatest advantage of a swarm of drones is the ability of these intelligent machines to work together – in numbers that would be simply impossible for humans – and when it comes to the battlefield, numbers matter. Most air defences are poorly prepared to deal with an aerial swarm, but simpler unmanned equipment can also be manufactured and maintained far more cost effectively. This not only reduces the logistics footprint of an aerial squadron, but also has the wider benefit of putting less servicemen at risk.

It is in the area of logistics footprint that I also expect to see further developments, maybe away from the frontline of operations, but with similar benefits of removing servicemen from harm's way. One of the most influential changes to keep a close eye out for is the introduction of electricity as a power source into the battlefield – or battlefield electrification – a development that was hot on the agenda when I attended the Defence and Security Equipment International arms fair in London at the latter end of last year.

The battlefield has been relatively immune to the wave of electrification hitting the civilian world, from cars to homes and public transport. When the concept of battlefield electrification first comes to mind it perhaps implies unrealistic visions of fully electrified ships, tanks and aircraft, built as now but without combustion engines, operating in combat environments. However, we are probably at least ten years or more away from this level of sophistication – as the same challenges of civil electrification of vehicles apply in terms of limited range, cost, weight and the fact battery technology has been slow in its evolution and has failed to keep up with aspirations. But irrespective of future hopes, change is on the horizon and this will be about so much more than simply 'green energy initiatives' – we are talking about delivering strategic benefits by introducing new ways to power military operations. In the long-term we may see full electrification of military vehicles – witness the US army's project to produce two prototype electric tanks by 2022 for example – but in the near term it will be electrification of secondary support which will hit the battlefield first.

Fossil fuels come at a significant cost to military forces in terms of logistics support – just look at the high number of supply casualties experienced in the fuel convoys of the Afghanistan war. Consider that forward operating bases consume vast volumes of electricity, often 1000s of kWh a day. This demand is currently met almost entirely by generators fuelled with diesel, which brings forward major supply chain concerns around efficiency and safety. Reducing the number of fossil-powered generators and replacing them with renewable alternatives such as solar and wind power vastly improves the logistics footprint of a forward-operating base. This helps to keep forces lean, minimises attack vulnerability and goes a long way to reduce supply chain casualties.

ARTIFICIAL INTELLIGENCE IS COMING TO THE FORE TO ACTUALLY OPERATE MILITARY EQUIPMENT

SUPPORTING AND PROLONGING

Throughout the rest of the year and beyond we will see developments on two fronts. On the one hand the challenge will be supporting and prolonging the life of older assets currently in service – it should not be forgotten that the average service life of USAF aircraft is currently over 20 years – but on the other hand, it must be recognised that new plans need to be put in place to support the assets of the future.

Of course, getting to grips with changing requirements and finding new ways to prolong asset life requires inherent organisational flexibility, something defence organisations have historically struggled with – and this applies all the way through to the software they use to manage operations and equipment. Previously, technologies such as AI and UAVs seemed to be banded about like buzzwords so organisations could demonstrate they are progressive and up to speed with the latest technological developments. But now these initiatives are beginning to prove themselves operationally – it will be the those who prepare and take action today that will set themselves up for a strong decade ●

Graham Grose, Vice President and Industry Director, IFS, Aerospace & Defence, is responsible for supporting all IFS business development within the A&D industry, together with associated industry marketing and overall product direction.

Grouping AI-controlled UAVs together to provide a swarm is incredibly difficult to defend against

Picture credit: US Department of Defense

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

Picture credit: Getty

PREPARING FOR A CRISIS

Gavin Wilson M.Sc *underlines the importance of having pre-defined emergency and business continuity plans in the event of a crisis*

Explanations of crisis can often differ, although the meaning usually remains the same. A good definition that seems to have been quoted many times is suggested by Rosenthal et al (1989) as "A serious threat to the basic structures or fundamental values and norms of an organisation, which – under time pressure and highly uncertain circumstances – necessitates making vital decisions". In this context the management of any crisis must necessitate the ability to make quick decisions that are essential in mitigating the impacts of the event. A phase often quoted within the crisis management arena is: "Making a bad decision during a crisis is better than making no decision at all". This is certainly true, but the consequences of bad decisions are also far reaching and certainly not desirable. Decisions need to be made and actions need to be acted upon. During a crisis the time to debate, test and exercise a decision to make sure that the right courses of action are effectuated is more often than not available. Time is after all a luxury in most circumstances, let alone during a crisis.

Failing to plan for crisis is a fundamental failing of any organisation in today's world. Although globalisation offers a multitude of opportunities and benefits, it also presents a myriad of risks that need to be carefully considered and planned for. Fortunately,

It's vital to be able to adapt quickly and operate fluidly within an unstable environment

most organisations that operate widely know this and have at least considered the basics in emergency and crisis preparedness. However, a question to ask is: are our traditional methods of managing crisis still relevant in the present day where these events seem to be more so frequent, aggressive and agile? Certainly, this seems to be true of the COVID-19 pandemic.

The speed of which COVID-19 has spread across the globe is unlikely to surprise many with the film industry dramatising mass infectious diseases on both the large and small screens for many years. Fortunately, at the time of writing our populace has not turned into zombies, although the scale of self-isolation witnessed across many regions that spans several weeks may give that impression when people eventually emerge from their dwellings.

While a widespread infection of any new disease is foreseeable, with records dating as far back as 200AD, occurrences do not seem to have been frequent until now. With ever increasing population growths and expanding urbanisation across communities that were previously separated by distance, the opportunity for disease to spread among inhabitants is apparent. Add to this the rise in global connections through air and sea travel that brings people together from across the globe, and the opportunity for new diseases to cause an epidemic and pandemic is evident.

In the past 20 years alone, we have seen the emergence of SARS, MERS, Swine Flu and COVID-19 affecting multiple countries, with Swine Flu (H1N1) causing the first pandemic of the 21st Century during 2009. Before that the 20th century witnessed three pandemics with the Spanish Flu being the most notable of that century emerging in 1918 that led to between 40-50 million deaths. A key denominator of that pandemic is thought to have been from infected soldiers returning from World War I back to their native countries. Indeed, history demonstrates the spread of disease is accelerated through the infected carriers travelling between populations. In regard to COVID-19, and at the time of writing, it's projected that the reproduction rate R0 is 2-2.5 from one infected person that would rapidly multiply; usually due to the carrier not knowing that they're infected leading them to unknowingly infect others.

Within a four-month period, the rate of COVID-19 global infections had spread to every continent but for Antarctica, with over a million confirmed infections and over 50,000 deaths reported; the figures of which are widely debated at the time with the overall amount of infections likely to be many more. The speed of which this widespread pandemic has spread among global populations, while alarming, is not necessarily unforeseen. After all, the Swine Flu pandemic lasted 18 months, is said to have infected over 1.5-million people and is estimated to have caused between 150,00- 575,000 deaths. Lessons have been learnt from previous disease outbreaks, especially in those countries most affected, with governing authorities responses seeming quick and to some extent affective in controlling and containing contaminated communities and regions. This is more so true of South Korea, which at the time of writing, has been widely praised in its ability to tackle high infection rates within communities by introducing strict measures early on, implementing effective responses, containment and communication measures, that seemingly led to a quick decline in recorded infection rates. Reports suggest that these measures were taken from lessons learned from the MERS outbreak during 2015 that widely affected that country, however, innovative adaptions to the COVID-19 situation were identified.

So, what did South Korea do to tackle this new crisis? It implemented a multi-level approach by adopting technology and innovating its usefulness in collecting, analysing and communicating data, ensuring open and transparent communications, developing public and private partnerships to enable a joint approach to tackling the problem where it arose, and mass testing the population whether they displayed symptoms or not that not only helped to identify and isolate those that were infected, but also impressed the seriousness of the situation on the nation. These measures resulted in half the number of new cases being reported within a week, half again over the next four days, and then again within a single day.

THE ABILITY TO BE ABLE TO ADJUST TO ANY GIVEN SITUATION IS KEY TO MANAGING UNCERTAINTY

Many crisis management and business continuity plans provide for an abundance of information, that in the usual sense, would greatly educate and transfer knowledge to the reader, but do these forward-planning preparations really enable an organisation to make the right decisions and enact the right actions quickly enough to avert their own crisis; regardless the external influences against them? In todays modernised world where technology enables many to work almost anywhere, but for those whose employment does not allow them the luxury of flexibility events alike the COVID-19 pandemic can have serious ramifications for the employee and employer alike. Indeed, the real crisis for many organisations may very likely be to prevent job losses, revenue losses and potentially closure. After all, financial and economic damage is usually guaranteed in any global crisis situation that in itself could lead to another crisis such as a recession.

International, national and industry related standards set out relative guidelines to encourage organisations to develop plans, procedures and practices that will enable them to operate accordingly to agreed best practice and, in some cases, to ensure compliance to laws. Most often these standards significantly improve how organisations operate within a defined framework that is frequently audited for both compliance and to also demonstrate how they are adapting and continually improving how they operate. Auditable frameworks that are designed to a pre-set compliance criteria may not enable the right amount of flexibility to encourage an organisation's agility within a changing and fast-paced environment. While standards are updated to necessary change, it could be questioned whether the frequency of change is relative to the needs of today's world that is evidencing far more and far consequential events;

such as economic uncertainties, natural disasters, regional conflicts, epidemics, pandemics etc. than ever before. In terms of emergency, crisis and business continuity management the success of these pre-defined plans, procedures and practices that have been developed to a pre-set compliance criteria can only be judged by those who use them. What has been evidenced in any recent crisis situation is the ability for those affected to adapt quickly and to be able to operate fluidly within an unstable environment. The ability to adjust to any given situation and circumstance seems to be key in managing uncertainty that is often a prime cause of a crisis. South Korea's ability to tackle COVID-19 at a time where infection rates were escalating is perhaps a good example of how the right and vital decisions were made to adapt responses to effectively mitigate an impending crisis.

DEVELOPING RESILIENCE TO A CRISIS DOES NOT NEED TO BE A BURDEN TO AN ORGANISATION

The relevance of pre-defined emergency, crisis and business continuity plans is evident in an organisation's preparedness for an event that would likely cause undesirable consequences for them. The key to enabling the success of any crisis pre-planning and preparations is to make them light enough to be enacted, to be adaptable enough to enable change and to action them fast enough to make relevant. Specifically, and perhaps most importantly, is the absolute necessity will inevitably be down to the capability and effectiveness of those persons directly and indirectly involved. The fluidity of change that we constantly evidence in today's world dictates that any plan can only be used to guide a crisis response, it will not in itself control the required outcomes to mitigate the consequences that is largely due to the agility of any situation, the operating environment and the external influencers that more often than not decide the level of impact imposed on the organisation; but not necessarily the overall consequences.

UNDERSTANDING RISK

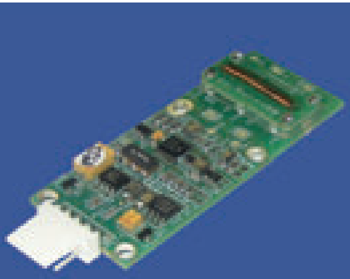
Developing resilience to a crisis does not need to be an overly encompassing burden to any organisation, it must however first and foremost understand the risks and those risk outcomes that would significantly impact the organisation's ability to operate. Understanding risk criticality ensures that the right level of focus and decision-making attention is given to those areas that will cause the most harm should they be adversely affected by the situation. Therefore, the significance of constant consultation through risk-based analysis to enable the continual development of crisis preparations is realisable in the enablement of quick decision making that would be essential in mitigating the impacts and overall consequences of an event. Making the right decisions quickly must, of course, be followed with decisive actions that are adaptable to change and that appropriately effectuate the desired outcomes. These are no easy tasks, but by adopting simpler processes into the crisis management preparations the ability to then adapt within an agile environment quickly will inevitably encourage more of the right decisions than the bad ones. Importantly, decisions will at least be made ●

Gavin Wilson M.Sc, Head of Risk Advisory Services at Wilson James, has over 20 years' experience in the security industry, with specific areas of interest in risk, crisis, and business continuity management, threat intelligence and security solutions design.

It is vital to regularly test and exercise any crisis response plan

Picture credit: Getty

FLUXGATES FOR MAGNETIC DETECTION



MAG646

- Single axis sensor
- For incorporation in door entry systems
- Low cost

MAG690

- Detection of magnetic materials
- Surveillance
- Low cost

Bartington™ Instruments

www.bartington.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

Police

Military

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

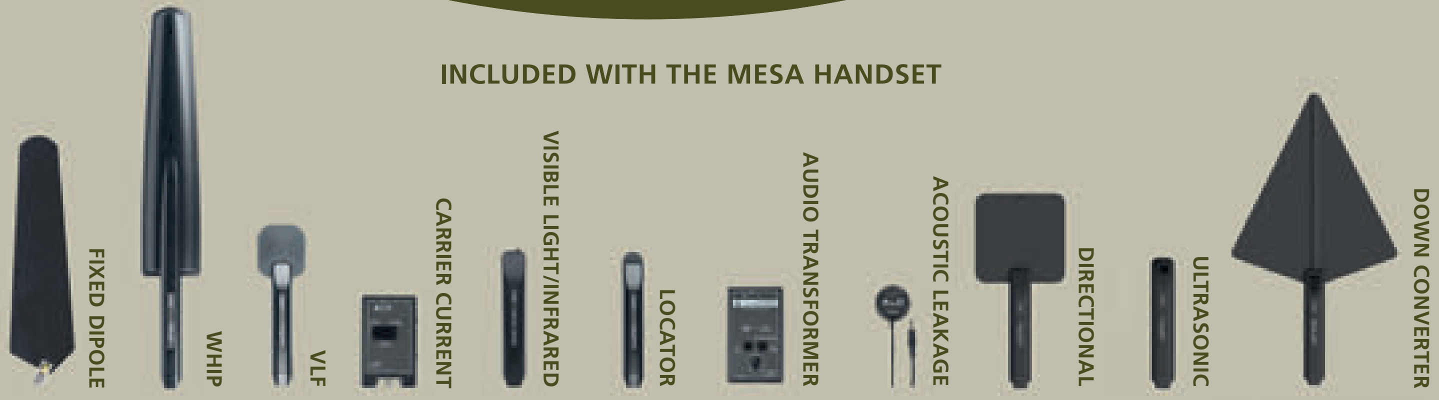
Introducing the new MESA...

Whether the security issue is in the UK or abroad, the new MESA has the power to tackle hidden state of the art bugging devices with the mobility to go anywhere to find them - single handed. With eleven separate probes it offers a versatility previously unseen in a handheld device.

The MESA (Mobility Enhanced Spectrum Analyzer) is the very latest product from REI, manufacturer of the world's leading counter surveillance equipment - only available in the UK from I.P.S.

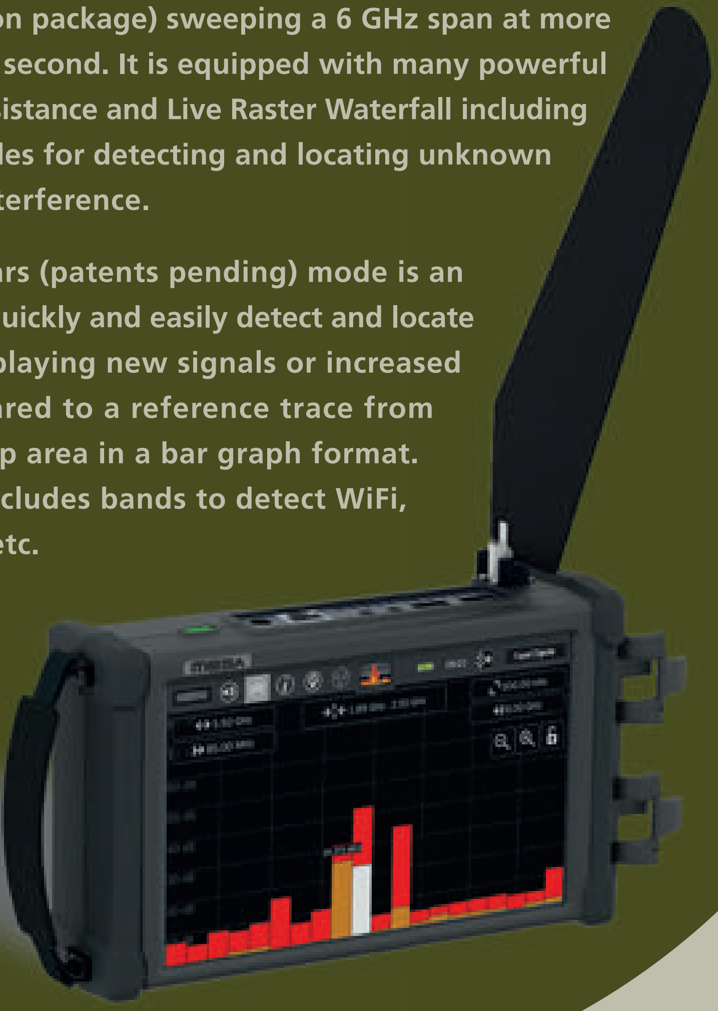
For more than twenty five years I.P.S. (Overseas) Ltd have been the first choice of governments and professional sweep teams around the globe to provide the world's leading equipment, manufactured by Research Electronics International (REI).

INCLUDED WITH THE MESA HANDSET



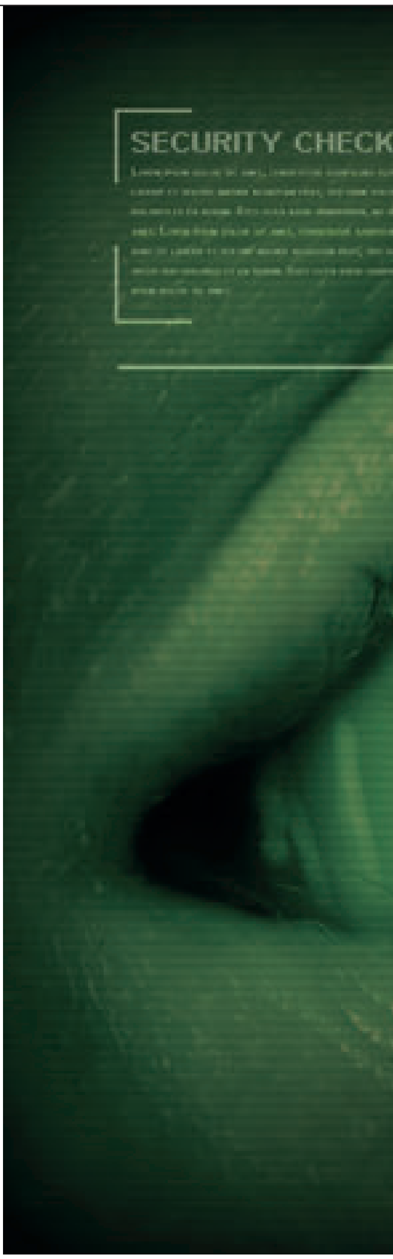
The MESA is a handheld spectrum analyzer covering up to 6 or 12 GHz (depending on package) sweeping a 6 GHz span at more than 100 GHz per second. It is equipped with many powerful functions like Persistance and Live Raster Waterfall including other unique modes for detecting and locating unknown RF signals and interference.

The new SmartBars (patents pending) mode is an effective way to quickly and easily detect and locate RF energy by displaying new signals or increased RF energy compared to a reference trace from outside the sweep area in a bar graph format. The MESA also includes bands to detect WiFi, Bluetooth, GSM etc.



SOURCE OF THE PROBLEM

Jeremy Praud *explains why tightened staff screening is vital to protect UK supply chains*



The Coronavirus pandemic has put the food industry under huge pressure to keep the shelves stocked during this global emergency, and the experience has brought home the tacit importance of the food supply chain. This should bring into sharp relief another ongoing threat to food supply chains – the risk of a deliberate terrorist attack.

Shortages and implications due to the reaction to the pandemic have been felt not just in the UK but across the world. The very short resupply time to keep the UK population fed is now evident to the whole population. It should highlight the concern felt for a long time by the leading UK intelligence providers that it is only a matter of time before a major attack is launched using the country's food supply chain by a terrorist group or a lone wolf pursuing a radicalised agenda. Unlike COVID-19, which has impacted the whole world, a premeditated contamination attack through the food supply chain has the potential to be limited to one country, but with similarly catastrophic economic damage.

Current business security in the UK tends to be reactive and therefore behind the curve, leaving significant risks unaddressed. Technology has made the security of physical buildings and systems relatively robust, but few people are looking at the changing face of risk that comes from malevolent insiders with their own agenda.

With the nation's attention diverted by Coronavirus, the guard might be down against other threats to business security especially following the announcement that thousands of new employees will be taken on by supermarkets and the pharmaceutical sector to keep items on the shelves during the pandemic. In April, screening requirements were loosened to ensure rapid recruitment of new employees into the food sector was possible. As an emergency measure that makes some sense, but it does not take long for those with a terrorist agenda to think of how to exploit an opportunity, and tightening up employee screening to protect operations from a potential enemy within has never been more important – especially new employees that are taken on and then become part of a stretched workforce.

What better scenario for a potential terrorist than to strike at the heart of the UK's supply chains during a recovery period from a national emergency? Because of its widespread delivery capabilities, the FMCG sector needs robust safeguards in place for all stakeholders including employment screening measures to protect against rogue employees, pressure groups and/or ideologically motivated individuals.

Companies in the sector need to now implement and maintain a comprehensive range of employee background checks, checks that go far beyond DBS (criminal records) and Right to Work. This forms a fundamental part of companies' Threat and Vulnerability mitigation (TACCP and VACCP compliance) using a simple traffic light system – red: do not proceed, amber: proceed with caution and green: no negative issues identified, proceed.

It was necessary to fast track the thousands of new workers being taken on by the food and pharmaceutical sectors to cope with the increased demand for their products due to the Coronavirus outbreak, with the minimum of fuss, but this necessary short-term relief must be followed up with future background checks to give lasting protection to the supply chain.

> EMPLOYEE SECURITY SOLUTIONS INSTILL CONFIDENCE IN THE LIKELY INTENTIONS OF RECRUITS

Standard DBS checks can only access 8 percent of an employee's background information, compared with checks such as FMCG Security's intelligence-led INSIGHT service, which evaluates 78 percent of data, the most important being verification of identity using highly advanced facial recognition technology. There are only three food security specialists in the world outside Government intelligence agencies, to offer this level of employee background checking service. The question is: would you choose to make informed decisions based on understanding only 8 percent of the potential problem, or would you prefer to have access to 78 percent of the data?

Workers are a company's most important asset, but that person walking through the door every day could also be one of the biggest risks if not appropriately vetted, and that applies to process operators and engineers as much or indeed even more than for finance directors and payroll staff.

The Government is enacting legislation to compel this work for key industries starting with the entertainment sector for large events, mainly in

Background security checks of staff in the food supply chain need to be more robust

response to the Manchester Arena bombing, but the food industry will be part of a second wave. Instead of waiting for imposed legal deadlines, those in the food industry who act now will avoid a more costly requirement later on, nevermind the peace of mind of protecting brands, public and country from the potentially devastating effects of a terrorist incident.

Increasingly stringent privacy and data security legislation has made employment screening compliance a challenge. The burden is on the employer to conduct risk-based screening to ensure a secure and compliant work environment by verifying movements, backgrounds and the right to work. Should someone get through the net, then management would be responsible if the available checks had not been carried out and product recall insurance may not cover costs if the attack is seen as an act of terrorism.

There have already been documented attempts to disrupt the UK's food supply chain, the most notorious being the case of Munir Mohammed and Rowaida El-Hassan, the couple convicted in 2018 of preparing for terrorism in a plot that could have attacked Derby or poisoned supermarket food.

Mohammed slipped under the radar by obtaining false EU documents which helped him secure work at Kerry Foods in Burton, a major manufacturer of ready meals where he cooked sauces for meals going to Tesco and Morrisons. Whereas the standard vetting tests were passed, INSIGHT vetting would have revealed he was using falsified ID, and also that he was a risk to the food supply chain. Kerry subsequently lost the Tesco contract, so closed the plant with the loss of 900 jobs.

REMOVING THE OPPORTUNITY

UK manufacturers can access the information they truly need to protect both their brands and the public in a way affordable for FMCG manufacturing. Safeguarding your workforce can lead to increased confidence across employees. Businesses, particularly those offering maximum opportunity to a lone wolf terrorist, need to understand the psychology of that type of individual in their sector. They must understand the motivation and the outcomes in play to close down the opportunity. The food industry can be viewed as a vast unprotected delivery system for a terrorist working inside with complete access. Food industry security tends to be focused on microbiological and health and safety, not crime and terrorism. However, radicalisation means that ordinary people can become terrorists and mass murderers. The food industry employs thousands of ordinary people in positions where terrorist actions could have staggering effects. The key is to know your people.

> IT IS ONLY A MATTER OF TIME BEFORE AN ATTACK IS LAUNCHED AGAINST THE UK'S FOOD SUPPLY CHAIN

Embedding counter measures and instilling formidable layers of security is a small price to pay against premeditated contamination to damage the UK economy, among other serious consequences. It is estimated that it cost the Russians less than £2,000 to mount a mainland attack on the UK, but the Skripal incident resulted in a £20-million clean-up bill, town centres closed, hospitals quarantined, transport and businesses affected, three people seriously ill and one fatality.

Now every terrorist in the world knows how to attack the UK for virtually no money. Nerve agents similar to Novichok are widely available. Other less exotic poisons more so. All that is needed is a delivery system and the food industry and water supplies provide an ideal route to potential havoc. How many food businesses can point to the critical control points they have implemented to control these vulnerabilities?

Just think of the consequences for an already weakened nation that an attack on the food or water supplies would have during the Coronavirus outbreak. To reduce this risk, employee security solutions are designed specifically to instill confidence in the status, background and likely intentions of existing employees or new recruits.

Some food manufacturers are already taking steps to beef up their security checks on staff. One convenience food manufacturer has already joined forces with FMCG Security to explore more stringent security measures that can help protect the UK food supply chain from a potential catastrophe. The food company, whose multiple food brands appear on many supermarket shelves, has successfully completed a pilot scheme and is looking at how robust safeguards can be implemented on a long-term basis by screening employees across its manufacturing sites.

A HOLISTIC VIEW

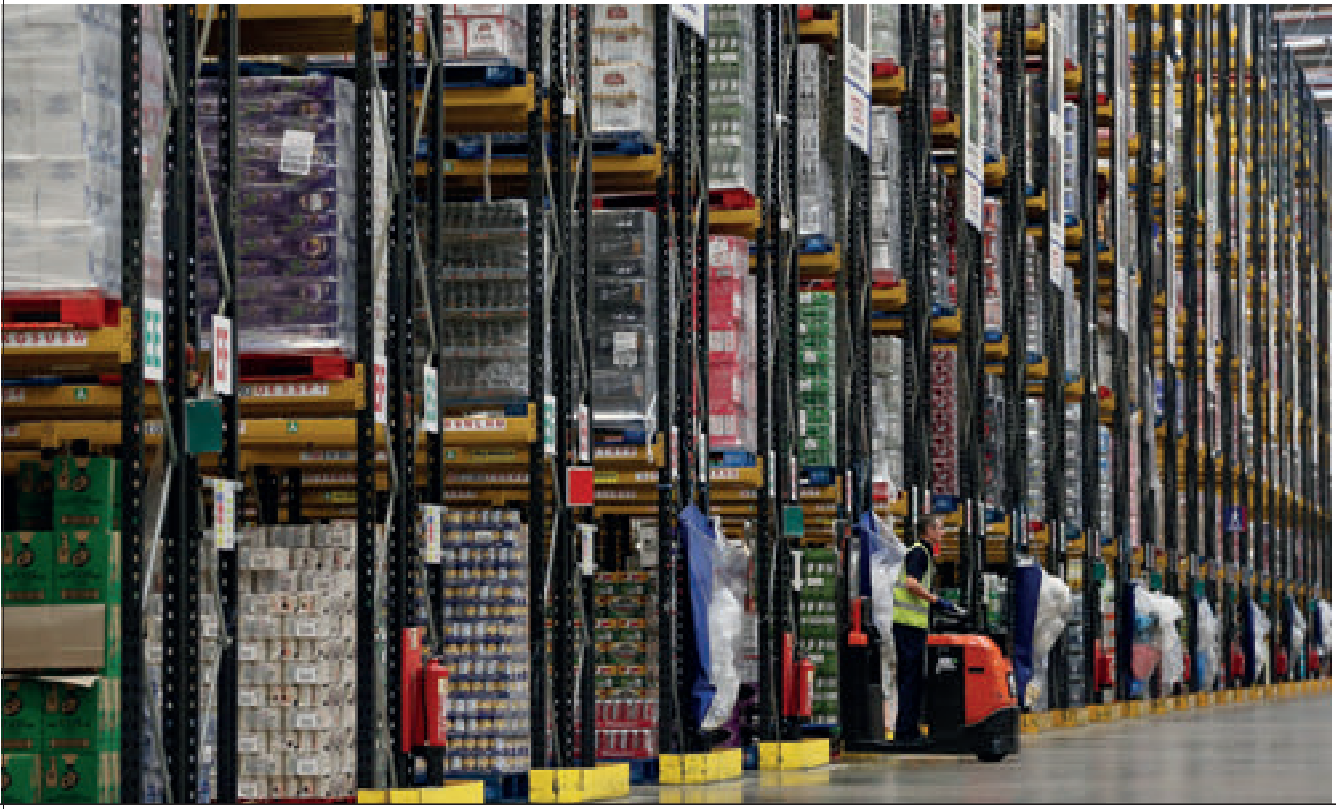
The specialist's Technical Director found that having a fully holistic view, which evaluates 78 percent of data – the most important being verification of identity using highly advanced facial recognition technology – does bring peace of mind.

Employers within the FMCG sector currently tend to rely on verification of identity simply by looking at employees' passport details and DBS checks, but documented attempts to disrupt the UK's food supply chain have shown that this is simply not sufficient any more.

Having a partner with a very strong background in intelligence and people assessment will give companies a real sense of reassurance for the future. Embedding new screening procedures enables access to the information that is really needed to protect brands and the public from malicious attacks with what should really be an industry-standard level of defence. Employee safeguarding solutions conducted by agents at the forefront of counter terrorism can be designed specifically for the food and drinks supply chains – after all, it's better to be safe than sorry ●

Jeremy Praud, FMCG Academy Chairman, has 20+ years' experience of working with manufacturers to improve productivity. Instrumental to the growth of LI Europe. He has a long track record of delivering successful improvement; above expectations both in terms of bottom-line results, and sustained change.

Background checks need to go beyond just DBS and Right to Work



Picture credit: Getty

GLOBAL QCC T.S.C.M

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?

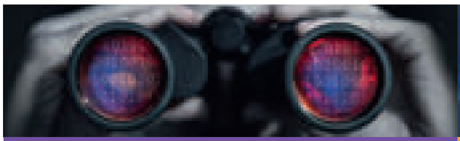
We don't just make and sell TSCM equipment, we use it & understand it.

QCC solutions include:

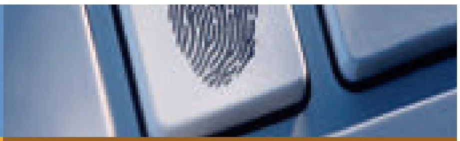
TSCM & Tactical IMSI Capture solutions - **SearchLight Plus** & the new **BlackLight**.

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

QCC's other proven and ISO certified services include:

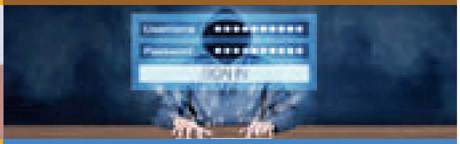

TSCM

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 !

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

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

DIGITAL DOCUMENTS

Ian Lancaster *considers the need for caution when it comes to the digital document revolution*

A revolution is underway in the secured document field. Society is migrating from using physical secured documents, such as bank notes and identity cards, to the use of smartphones and electronic payment cards for financial transactions and as carriers of our identity credentials.

The COVID-19 crisis has thrown this trend more sharply into focus in relation to payments. In just one week, cash usage halved in the UK and a similar story is playing out around the world, as more people turn to contactless payments to minimise the spread of the virus. Whether this is a temporary measure while the virus is active or another nail in the coffin of cash remains to be seen.

In the minds of many, this transition from physical to digital is inevitable, unstoppable and irrevocable, even though cash is still used for most retail purchases globally (COVID-19 influence aside) and passports are still required to enter a territory. Nonetheless, this transition is inevitable, so there is a need to consider the impact and implications of this change.

THERE'S A TENSION BETWEEN CONVENIENCE ON THE ONE HAND AND SECURITY ON THE OTHER

These considerations are the driving force behind Reconnaissance International's new White Paper, *Physical To Digital: A Revolution in Document Security* (pictured opposite), which looks at the implications of the current digital revolution in the areas of financial transactions and ID document security. The publication contrasts more than 1,000 years' experience in printing and examining security documents with the 30 years of digital experience and the use of smartphones in what has previously been the domain of secured printed documents.

In simple terms, is it a revolution that leaves us and our data safe? We are moving from a world in which people can examine and inspect a document to check its legitimacy (in order to be confident it can be trusted), to one in which we have to trust that a device, such as our smartphone, is doing what we think it's doing, that the data it's using is accurate and secure and the decision it makes – or leads us to make – is correct and appropriate.

Are we right to invest this much trust in these new methods of making payments and showing our identity? Or should we pay heed to the view that, in failing to question the algorithms that are doing this work for us, we open the door to hackers, fraudsters and other criminals?

In examining the transition in security documents from the physical to the digital, the white paper considers: How far has it gone and what is its future? What are its implications and – crucially – how safe is the data held and used in the digital world? Are we merely users of these systems, or is there a role for us in ensuring that they and the data they use are secure? What might that role be? Is anything needed to enhance the safety and security of these digital methods and if so – what?

The use of digital technologies has some way to go before replacing cash – most people in most countries continue to rely on money for retail transactions. Similarly, when it comes to ID documents, digital technologies, while attractive, remain for the time being some way short of being ubiquitous. It's clear that physical bank notes and ID credentials remain the norm, but why?

Physical documents are tangible, familiar, and with security and authentication features built in. Moreover, a key driver for specifiers and designers – honed over this 1,000 years of experience – is security and document protection. In this physical world, professional document examiners develop a sixth sense, a feeling for the document which comes with familiarity and practice.

The result is reflected in the low counterfeiting levels for bank notes and passports; for example, 0.003 percent of Euro bank notes in circulation and 2 percent of passports worldwide. This compares with, say, the World Health Organisation's estimate that 10 percent of medicines worldwide are fake.

As digital methods become more common, we need to question whether they match the security and detection built into the physical document world. If not, how can they be improved? Should we abandon the use of human inspection and, if not, how do we combine the best of both worlds?

These questions become more pertinent when we consider the significant number of data breaches, hacks and outages that occur in the digital world. There are numerous examples of online identity and financial theft, often serious enough that they are reported in the mass media, not just the specialist media. In addition, there have been many cases of systems crashing, making it impossible for people dependent on their credit cards or smartphones to conduct any financial transactions.

To give a few examples: In July 2019, Capital One bank suffered a data breach, which affected around

100 million US citizens. In 2019, 165-million records containing personally identifiable information (PII) were breached in the USA alone, according to the Identity Theft Resource Center. Following system crashes at TSB, NatWest and other UK banks, an October 2019 report by the House of Commons Treasury Committee said that customers were left "cashless and cut off" due to an unacceptable number of IT failures – some of which cut off customers from their bank for several days or longer

It is worth pointing out that these are thefts from or hacks of the places where our data is stored. Those promoting online systems refer to storage in the cloud, implying an ethereal, intangible entity that cannot be illicitly penetrated. But the reality is that our data is transmitted over the internet (via cables and satellites) to huge server farms, buildings that contain thousands or even hundreds of thousands of servers making and recording our transactions or our identity. These tangible resources are certainly well protected, with back-ups and redundancy built in, but they have been hacked, as have the internet network connections to them, as the previous examples reveal. So, for cloud read 'networked computers'.

These computers, data stores and the connecting networks operate numerous security features, including hash codes, two-factor sign-in and encrypted apps, but they all work within the digital domain; there is no interaction with human beings.

There are numerous collaborative development projects underway to establish standards and improved systems for data protection, including the EU-funded Olympus7 project and ISO's emerging mobile driving licence standard. These all show that there is recognition of the need for security within the digital domain, even though the original impetus may have been – and in hardware terms, still is – technology driven.

Nevertheless, current systems remain vulnerable and fallible – particularly so in the digital payments world. The

The transition from physical to digital payment methods is inevitable

difference in the rate of fraud between bank notes and payment cards in the Eurozone is stark. The European Central Bank reports that payment card fraud in the zone in 2016 totalled €1.8-billion, which is one-tenth of one percent of the total card transaction value of €1.8-trillion. This is over 300 times greater than the 0.003 percent of Euro banknote counterfeits, while Europol reports that cardholder not present (CNP) transactions accounts for 66 percent of card fraud.

WHEN IT COMES TO ID, DIGITAL TECHNOLOGIES REMAIN SOME WAY SHORT OF BEING UBIQUITOUS

In electronic transactions, whether card or app-based, the key challenge is identity. If you pay with cash, the cash is assumed to be yours and the physical exchange is straightforward. The link between value and the bearer is 'presence' and not 'identity'. A digital transaction is more complicated because there is no link between the value and the identity of the user.

The regulatory landscape is struggling to keep up and criminals are exploiting the new paradigm of payment being about value linked to identity rather than value linked to presence. This brings us back, of course, to how governments and businesses can secure identity with confidence, what is the proof of identity and how it can be proved at the point of transaction.

In general, digital identity has its benefits – notably, convenience and in some cases, reduced cost. Every day, millions of travellers get home faster because they can move quickly through ports of entry and exit using their digital ID. Tens of millions of patients get better treatments because their doctors can gain access to their digital medical records and billions of consumers can buy goods from around the world with a username and password.

However, there's a very real tension between efficiency and convenience on the one hand and security on the other. While a machine is highly efficient at confirming the truth or otherwise of a user's credentials, it is not so good at determining the provenance of those credentials. It may also be vulnerable to the theft of this digitised personal data.

While the switch to digital systems is undoubtedly gathering pace and there is widespread recognition that society cannot turn back the clock, there is also a need to change the mindset of people working in digital finance and ID, to encourage them to put data and personal security at the heart of this new world.

Improving data and cyber security should be a top priority for all of us. Perhaps there needs to be a greater realisation that physical and digital documentation can co-exist; a way forward in this inevitable transition to digital could be to seek ways of drawing on the best of both worlds. Can the commitment to security and protection that drives the physical secured document field be inculcated among digital system developers and adopters – and if so, how?

The primary purpose of creating, recording and storing personal data digitally is to improve convenience for service users and providers – a trend that seems likely to continue. Equally, card and contactless payments are set to become even more common. But there is a risk that further adoption of digital identity and digital payments may be greeted with pushback until key issues of trust, privacy and security can be addressed.

Could this be an opportunity for commercial entities with know-how and experience in the security arena to guide users in the proper balance between physical and digital safeguards to ensure that security is built-in and not merely a bolt on?

While the White Paper (available free to download at digitaldocumentsecurity.com) is an important contribution to this debate, clarifying the current position and the critical issues, it doesn't have all of the answers. Hopefully, however, it facilitates the asking of the questions and exploring of the issues ●

Ian Lancaster has many years' experience in security and authentication. Founder and former MD of Reconnaissance International, he is a specialist analyst of and consultant in holography and anti-counterfeiting and is lead author and editor of *Physical to Digital: A Revolution In Document Security*

COVID-19 saw the use of cash half in just one week in the UK

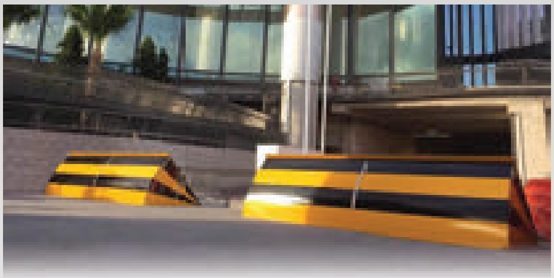
HEALD®

INNOVATORS, MANUFACTURERS AND INSTALLERS OF AWARD-WINNING PERIMETER SECURITY PRODUCTS

Heald's Patent Protected Sliding Bollard System: The Matador!

THE EVO BOLLARD

THE VIPER



THE RAPTOR

@healduk

Heald Ltd

www.heald.uk.com

Secured by Design SBD Police Preferred Specification

MADE IN BRITAIN

MADE IN YORKSHIRE

PSSA

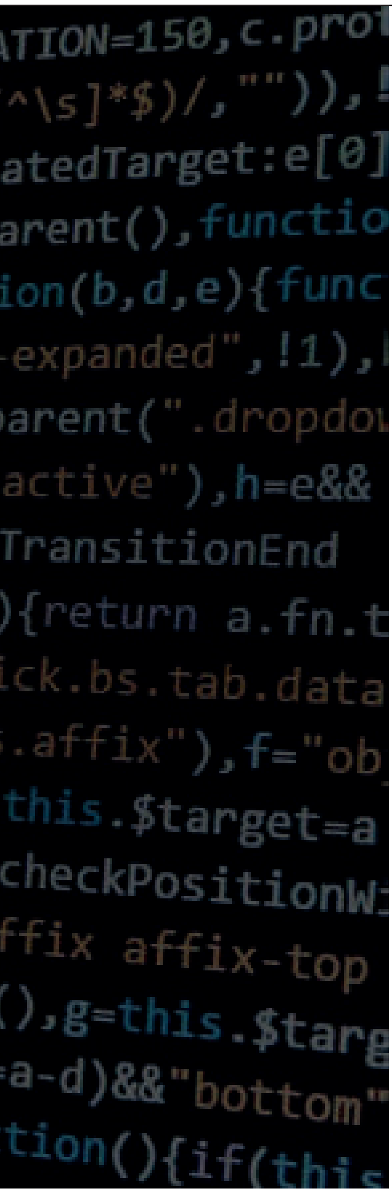
A SAFE HARBOUR

Colin Tankard *explains how encryption has become the building block for data security*

Encryption, whereby information is converted from a readable format into one that obscures its meaning from those without the authorisation or ability to decipher it, has long been used to protect sensitive information from prying eyes. Ever since the end of the Second World War, as the use of computers has become widespread, algorithms for encrypting data have become increasingly common, enabling vast swathes of information to be encrypted both quickly and efficiently.

Encryption is invaluable for ensuring that sensitive information that falls into the wrong hands, if it is lost or stolen, is prevented from being of use to anyone without the ability to decrypt that information. It satisfies requirements for data confidentiality and integrity by ensuring that information has not been tampered with.

In recent years, ensuring the security, confidentiality and integrity of data has become an ever more pressing concern. Information and data produced and collected by organisations, including intellectual property and personally identifiable information related to



65 percent of large firms reported having suffered a data breach in the past year

customers, employees and business partners, is valuable not just to the organisation concerned, but also to criminals who can use it for financial gain.

According to recent research by Thales, 91 percent of IT executives state that they feel vulnerable to data security threats. A recent government survey found that while 65 percent of large firms reported having suffered a data breach in the past year, more than half of medium-sized firms and one third of small organisations had been breached, showing that no one is immune.

In the Breach Level Index 2019, almost five billion data records had been lost or stolen since 2013, but only 4 percent of those records were encrypted. Any data breach can cost the organisation involved dearly, both in terms of lost revenues and damage to its brand and reputation.

According to IT Governance, in their data breaches and cyber attacks report, in February 2020, 623 million records were breached, but this doesn't tell the full story, as there were a whopping 105 incidents, making February 2020 the second leakiest month it had ever recorded.

Encryption has a vital role to play in keeping sensitive and confidential information safe from prying eyes. The use of encryption is the best strategy for any organisation for maintaining security of data when it is in storage or is being transmitted, such as over the internet. Initially considered to be a complex technology to deploy and manage, it has now moved on and can easily be used by anyone.

SAFEGUARDING DATA

But it is not just a good strategy to choose to encrypt sensitive data; it may also be required. Organisations face a wide range of regulations and industry standards that they must adhere to. In the US, the majority of states have laws regarding data breach notification and those doing business in Europe have similar pressures from the General Data Protection Regulation (GDPR), which specifically 'calls out' encryption and pseudonymisation as suitable, appropriate safeguards for protecting data.

What many of these regulations and industry standards, such as PCI-DSS for protecting payment card information, have in common, is that they provide a safe harbour when encryption has been implemented. For example, the majority of laws that mandate data breach notification contain clauses whereby notification is not required when data that has been lost or stolen has been encrypted, since the data cannot be compromised, unless the encryption code or method is also compromised.

When it comes to ensuring that data is properly secure, there are four critical questions that need to be asked: Who has access? It is not a lot of use locking up the family silver if everybody in town has a key to the strong room! The absolute minimum number of people must have the keys to the encryption and they must never pass them on without clear, documented permission.

When has the data been accessed? For the reassurance of the business and its prospective clients, as well as to ensure corrections can be made if data does leak, all access to encrypted material must be effectively logged. Not difficult to do, but crucial.

Is the data secure in the first place? If there is a flaw in your systems already, then your encryption processes may be worthless. You can only build on secure foundations and essential secondary controls will establish if those foundations are compromised.

When does complacency set in? A few years ago operators bought off-the-shelf firewall software for their PCs and considered themselves to be safe for all time. As we know, they were wrong. Basic computer security has had to be improved and updated on an almost daily basis. The people who are trying to get past your security are continually improving their attacking systems; your encryption needs to be dynamic and proactive. Beware a false sense of security!

Encryption by itself is not the only technology that organisations should have in place to protect sensitive data, but should be a strategic part of the entire security system, alongside complementary technologies such as access controls, monitoring systems, auditing and reporting capabilities.

ALL SENSITIVE DATA SHOULD BE ENCRYPTED BEFORE IT IS UPLOADED TO CLOUD SERVICES

The tight control of the actions of privileged users is of particular importance, in terms of what they can access and what they do with the information. This is necessary owing to the need to counter insider threats, which are estimated to account for 43 percent of all breaches, many of which are attributed to actions by privileged users. Not all insider threats are caused by malicious intentions, as accidents can occur, such as inadvertently sending information to a recipient other than was intended, but insider threats can be the most damaging, since internal users can have access to the most sensitive and valuable information that an organisation possesses. These controls should be tightly integrated so that there are no security gaps that could be exploited, so that organisations are better able to both ward off advanced threats while meeting their compliance objectives.

The increasing use of cloud-based services is another complication for effective data protection. Some cloud services support the use of encryption and other methods of data protection, but many people use cloud-based file-sharing services, many of which were originally developed for consumer use and for which security controls are variable. According to Box, file sharing services account for 39 percent of all company data that is uploaded to cloud services and 34 percent of users admit that they have uploaded sensitive and confidential information to file sharing services. The same survey looked at the encryption practices of cloud service providers, finding that while 82 percent encrypt data in transit, just 9 percent encrypt data at rest in the cloud. Meanwhile, just 1 percent of providers offer encryption services where the customer retains control of the encryption keys, which could lead to data being inappropriately accessed.

Because of factors such as these, organisations should ensure that all sensitive data is encrypted before it is uploaded to cloud services and that it remains encrypted when in storage. They should use a service that guarantees the retention of control of all encryption keys, which should then be stored securely and with tightly controlled access.

While encryption is seen as a best practice for data control and protection, it cannot be used in all circumstances, such as when data is in use for processing purposes. This is where the use of technologies such as tokenisation and data masking – referred to as pseudonymisation in GDPR – come into play. The difference between encryption and pseudonymisation is primarily the way that data is handled. Encryption uses an algorithm to scramble data so that it is unreadable, whereas pseudonymisation techniques substitute data with random codes or tokens.

With tokenisation, applications can still operate using tokens so that sensitive data is hidden, reducing any risk of exposure. An example of where it would be used is for medical research purposes, where large sets of data relating to people is analysed but sensitive data, that could be used to identify a person, is replaced with tokens.

As with encryption, data masking scrambles information, but it is often done more selectively than encrypting, such as for whole databases. An example of where it is particularly useful is in redacting sensitive data in documents such as emails and office productivity documents, so that they can be sent largely in plain text, but with sensitive information such as credit card numbers hidden or masked.

Both data masking and encryption are suitable technologies for protecting communications, especially via email, which remains the most prevalent mechanism in use. The entire contents of emails and their attachments can be encrypted so that nothing can be read by those without the appropriate authorisation. However, this can be considered to be overkill if used across the board, since many communications are fairly general in nature and encrypting every message adds to the burdens of users and increases time lags. Data masking provides an alternative by redacting sensitive information, similarly to how paper documents containing sensitive information have critical details redacted by hand.

Another core capability to add is cryptographic key management. This is the mechanism which stores and changes encryption keys as required, which should be centralised to ensure that policies can be consistently applied across all data, both when in transit and when at rest. Efficient key management can be achieved through use of a physical or virtual appliance or, increasingly can be provided as a service, especially for cloud applications.

In conclusion, encryption as a technology is versatile, robust and easy to deploy. The myth of it having performance issues when used has long gone and where needed, can be totally transparent to the user or application. It requires no modifications to applications or additional training of staff in its use. There are some challenges, especially where Data Leakage Protection (DLP) is deployed on endpoints or servers, as DLPs can't read encrypted data and will block it. This may lead to some organisations allowing encrypted data to pass through a firewall, which obviously defeats the objective, as users exfiltrating data from the organisation will encrypt it first.

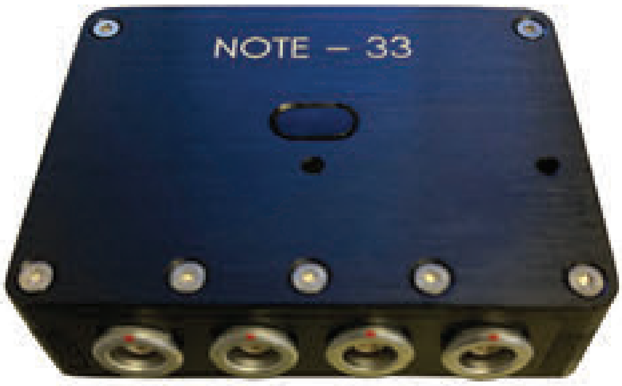
An encryption solution, once deployed, works with both the existing infrastructure, as well as future growth or strategies. It is an important part of any organisation's data security landscape and should always be the starting point for new data deployments and be considered a core part of any data security strategy that organisations develop. For both data security needs and for achieving regulatory compliance, encryption should be considered to be the baseline ●

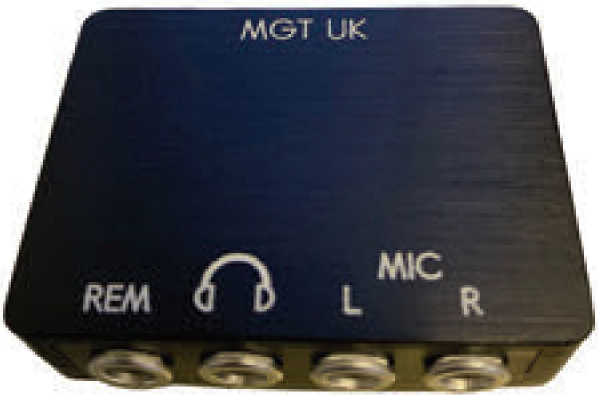
Colin Tankard is Managing Director of cyber security and data management company Digital Pathways, specialist in the design, implementation and management of systems that ensure the security of all data whether at rest within the network, mobile device, in storage or data in transit across public or private networks.

Pseudonymisation techniques substitute data with random codes or tokens

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).*

GDPR TWO YEARS ON

Reza Nezam *reflects on the changes brought about by the General Data Protection Regulations and reveals there is still much work to be done*

It has been two years since GDPR was introduced in the UK and the EU to give people more control over their personal data and how it is used. Any company that stores or processes personal information about EU citizens within EU states must comply with GDPR, even if they do not have a business presence within the EU.

Law firm Gibson & Associates Solicitors conducted a survey of more than 1,000 people in the UK and Ireland to gauge whether the general public understand their rights under the legislation. The results revealed that as many as one in five people have fallen victim to a data breach, while one in four are unaware as to whether they have had their personal data illegally accessed.

Of those who said that they had been the victim of a breach, only seven percent made a claim. When asked why they did not make a claim, 37 percent said they were not aware that they could do so, while 24 percent didn't think it was a big enough concern to bother trying.

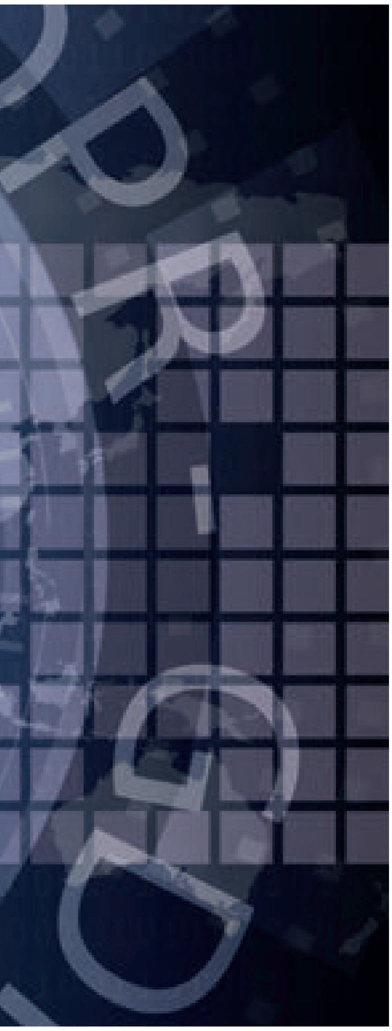
Personal data breaches can include: access by an unauthorised third party; deliberate or accidental

action (or inaction) by those responsible for your data; sending personal data to an incorrect recipient; computing devices containing personal data being lost or stolen; alteration of personal data without permission; or loss of availability of personal data.

The GDPR places a duty on all organisations to report certain types of personal data breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach. If a breach poses a high risk to individuals' rights, they must be informed without undue delay. Organisations are required to provide the following in clear and plain language: the nature of the personal data breach; the name and contact details of the organisation's data protection officer or another point of contact; a description of the likely consequences of the personal data breach; and a description of the measures taken, or proposed to be taken, to deal with the breach, including, where appropriate, measures taken to mitigate any possible adverse effects.

Any organisation that collects personal data has a legal duty of care to make sure every individual's information is protected. Anyone who has their data leaked due to the irresponsibility of a company is vulnerable to suffering financial losses. Regardless of how big or small these are, companies should be held accountable for their mistreatment of this often very sensitive data, which is why victims have the legal right to make a claim.

GDPR places a duty on organisations to report data breaches within 72 hours of becoming aware of them



While it may not seem like a big deal to make a claim if you haven't suffered significant financial losses, individuals shouldn't be worried about whether they are going to have their personal information used without their knowledge. Making a claim isn't just about reimbursing the victim's financial loss, it can be used to recompense any emotional distress and ensure that the responsible organisation has suitable security methods in place to protect data against any future breaches.

Despite 80 percent of survey participants confirming they know what GDPR is , respondents showed significant gaps in knowledge when asked about the guidelines. Only 28 percent understood what personal information could be legally kept by an organisation, while 15 percent wrongly said that companies were not able to keep any personal data at all.

The full list of personal information that an organisation can keep on an individual under GDPR includes: your name; date of birth; address or mobile phone GPS; telephone number; an online identifier, such as IP address or email address; the job you do; your racial or ethnic origin; identification numbers, such as National Insurance and passport; items you view or buy online; your bank details, including credit cards; the school you went to; information on your health; biometric data, such as photos and fingerprints; details about your partner/family; membership of any Trade Union; religious or philosophical beliefs; political opinions; passwords; or details concerning your sex life and sexuality

There was also a significant lack of knowledge when respondents were asked what companies can legally do with personal data, with only 26 percent correctly identifying that organisations are able to do the following: use it to provide a service; make a recommendation; decide what you see online; directly sell to you; or sell the data to third parties. Some 14 percent incorrectly said that companies were not able to do any of the above with personal data.

GDPR was introduced to allow people to take back control of their personal information and make informed decisions about how it is used. While it falls to a company to responsibly handle someone's personal data, individuals need to be aware of what information is being stored about them and what can be done with it.

Despite 62 percent of respondents saying they do not trust companies to use their data responsibly, and 72 percent being greatly or somewhat concerned about organisations misusing their data, it is surprising to see that more than half (55 percent) of UK and Irish residents were not familiar with the means to request access to their data.

IF YOU ARE USING THE INTERNET OUTSIDE OF THE EU GDPR'S PROTECTION NO LONGER APPLIES

A subject access is a written or verbal request asking for access to personal information that an organisation holds or processes on you. You are able to make a subject access request (SAR) whenever you want to know about what personal data any company stores about you.

Following the changes made when GDPR was introduced, individuals can now make an SAR for free. If a request is considered to be "manifestly unfounded or excessive", a reasonable admin fee may be applied to a request. Using an SAR, individuals can request: a copy of their data; the reason why their data is being processed; what type of data is stored and processed; who receives the data; how long it is stored for; and how the data was collected.

To make a subject access request, you should find out which department and person you need to send the request to. Write to the organisation by recorded delivery or email, including your full name, address, contact telephone number, any account numbers, unique IDs and other information to distinguish who you are. You should also include specific details of the information you require and any relevant dates.

You may be charged an admin fee if your request isn't specific enough. For example, when making a request to see CCTV footage it would be reasonable to specify a location, date and time instead of asking for a month's worth of footage. In the request, you should also make reference to your right to make an SAR for free and the one-month deadline, which applies to the time period a company has to respond to a request. Finally, it is important to keep a copy of the SAR and any other correspondence. This will be useful if you need to make a complaint against an organisation that hasn't fulfilled a request.

An organisation is required to reply to an SAR within one month from the date it receives the request. This period can be extended by two months if a request is complex or there are multiple SARs made, but the company must get in touch during the first to explain why an extension is necessary. All

SARs must be completed free of charge; however, a reasonable fee can be requested if an SAR is unfounded or excessive, or additional copies of the personal data are requested.

Organisations should provide data in a commonly used electronic format unless this is not possible or it takes "disproportionate effort". Information should be provided in a concise, transparent and easily accessible form that is written in plain English and is capable of being understood by an average person.

GDPR WAS INTRODUCED TO ALLOW PEOPLE TO TAKE BACK CONTROL OF THEIR PERSONAL INFORMATION

Companies are allowed to withhold certain information if it could identify someone else and it is not reasonable to disclose that information. Also, if somebody making an SAR is being investigated for a crime or in connection with taxes and the investigation would be prejudiced if access to the data was granted.

GDPR is an EU law, which means that the benefits are focused on protecting the privacy of citizens of the European Union. Although some organisations have stated that they will roll out similar protections for users worldwide, currently, the legislation only applies to people who are browsing in the EU region.

This means that if you are outside of the EU, even temporarily, the same protections do not apply because websites determine the geographical location of their visitors based on their IP address. However, it is possible to change the IP address by using a VPN, meaning if you're travelling outside of the EU, you can still connect to an EU server and be treated as an EU citizen by websites.

To ensure you are protected under GDPR, you will need to sign up with a trusted VPN service; download the VPN and launch the application on your computer or mobile device; select a server to connect to – this can be anywhere across the globe, but will need to be in the EU in order to take advantage of GDPR protection; connect to a server in order to be assigned a new IP address; and then browse the internet at your leisure with added protections.

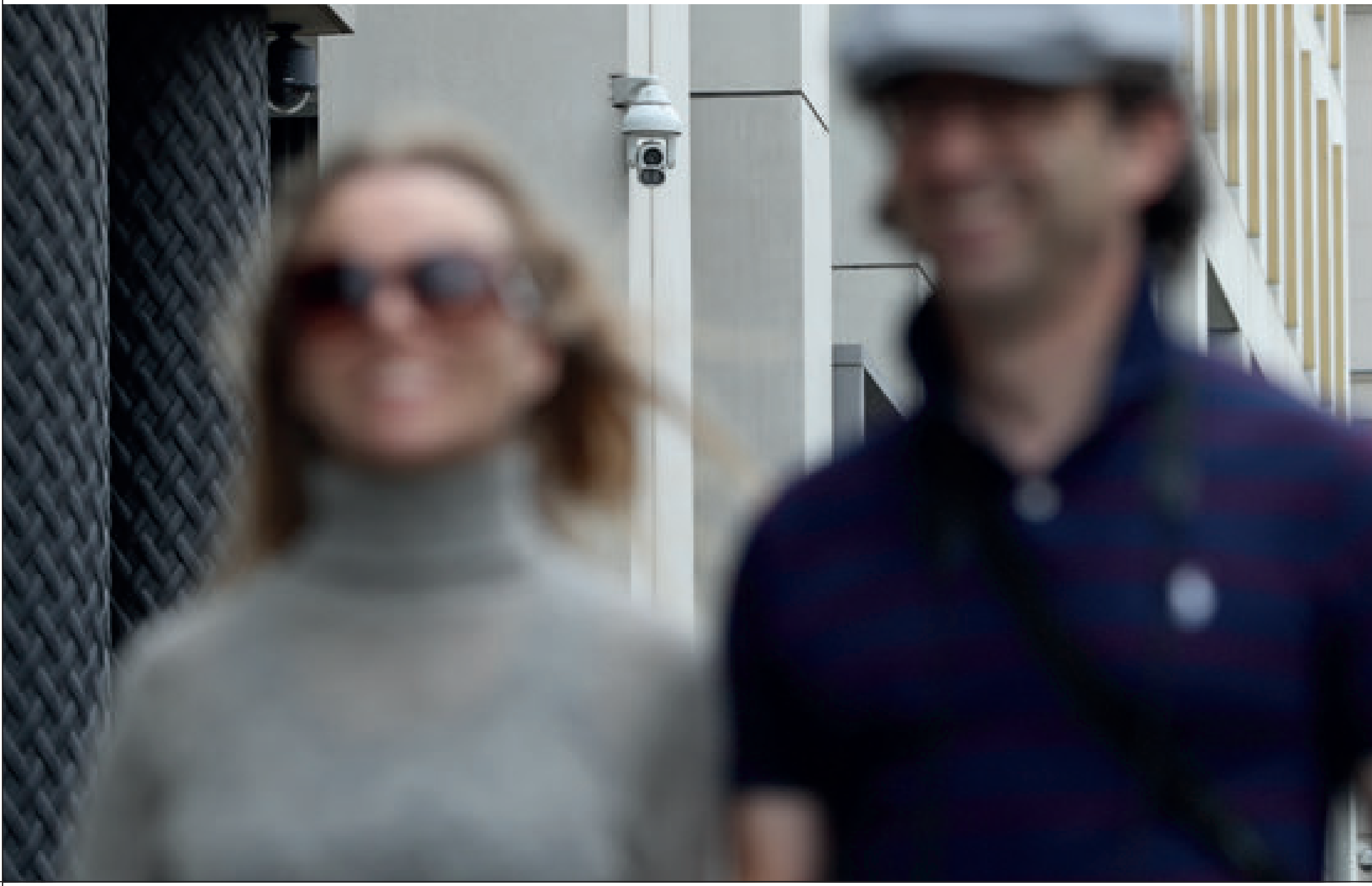
Using a VPN can also have numerous additional benefits, including encrypting your web connection and hiding your web traffic data. This means a VPN can provide protection by blocking websites and ISPs that collect your data.

In addition, you will also be able to browse websites that were previously blocked in a country outside of the EU. VPN tools are also considered to be extremely effective in keeping malware off mobile devices.

In the digital era, is it essential that data is protected. Misuse of data can result in discriminatory decisions, violation of privacy rights, identify theft, fraud, and much more. This is why you must be in control of your information. Now that the law has changed to strengthen what were once weak enforcement mechanisms, you have a responsibility to keep data secure and hold any organisations that infringe your rights to account ●

Reza Nezam is a data protection solicitor at Gibson & Associates, qualified as a solicitor in 2016 and has professional certification in data protection law.

When requesting CCTV footage it is prudent to provide details of specific location, date and time



Picture credit: Getty

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

Police

Military

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

INCIDENT BRIEF

Europe

4 April, Romans-sur-Isère – France

Two people were killed and five others injured in a stabbing attack. An asylum seeker was arrested and French counter-terrorism police are investigating the incident.

9 April, Angarsk, Siberia – Russia

A fire broke out in a high-security prison after a riot by inmates who accused guards of mistreatment.

15 April, Western Germany – Germany

Raids were carried out on six locations, resulting in the arrest of five Tajik nationals on the suspicion that they were members of an Islamic State cell planning attacks on US forces stationed in Germany.

27 April, Colombes – France

An Islamic State fanatic seriously injured two police officers when he rammed his vehicle into them.

29 April, Vienna – Austria

The Austrian President's office was evacuated after receiving a bomb threat. The building was searched and the area surrounding the office was sealed off.

6 May, Sittingbourne, Kent – United Kingdom

After receiving a threat that an armed man was heading to Sittingbourne Memorial Hospital, the whole building was locked down and police were informed.

Americas

8 April, Monroe Correctional Complex, Washington – United States

More than 100 inmates rioted, sparked by reports of a COVID-19 outbreak in a prison wing.

9-10 April, Lansing Correctional Facility, Kansas – United States

Up to 150 inmates rioted at a Kansas prison after several prisoners refused a lockdown order. Fires were lit and offices and equipment were destroyed.

19 April, Portapique, Nova Scotia – Canada

A gunman posing as a police officer shot and killed 16 people in a 12-hour rampage. The shooter died in a police standoff.

24 April, country-wide – El Salvador

The Savadorian President ordered a 24-hour "maximum emergency" lockdown of prisons confining gang members after 22 murders in a single day.

29 April, Miguel Castro, Castro prison, Lima – Peru

Nine inmates were killed in a riot, which left two other prisoners wounded. Five police officers and 60 guards were also injured.

2 May, Los Llanos prison, Western Guanare city – Venezuela

At least 46 people died in a riot in a penitentiary in the Venezuelan state of Portuguesa. Prison staff, including the governor, were among the 60 injured.

Asia

9 April, Bagram Air Base, Kabul – Afghanistan

Islamic State claimed responsibility for a five-rocket attack on the air base, the United States' largest in the country. There were no casualties or injuries.

10 April, Northern Badakhshan province – Afghanistan

At least 27 Taliban insurgents were killed in offensives in Warduj and Nusay districts. Nine others were injured. No civilians were harmed.

11 April, Manado – Indonesia

Inmates set fire to an overcrowded prison during a riot over measures to contain COVID-19. Hundreds of soldiers and police were sent in to take control of the situation.

13 April, Mansuriyah al-Jabal – Iraq

Islamic State terrorists targeted a federal police observation post in Southern Kirkuk, killing a police officer.

15 April, Mahibadhoo harbour – Maldives

Islamic State claimed responsibility for an incendiary attack on boats, including a sea ambulance, in the harbour.

17 April, Sulu – Philippines

Abu Sayyaf is suspected of being responsible for an attack on an island in the South of the country which killed 11 soldiers and injured 14 others.

21 April, Rakhine State – Myanmar

A WHO worker collecting Coronavirus samples was shot and killed during an attack on his vehicle. Rakhine Nationalists are suspected.

28 April, Afrin – Syria

A suicide bombing near a market killed at least 53 people and injured more than 50 others. YPG is suspected of being behind the attack.

29 April, Char Asiab District – Afghanistan

A suicide bomb detonation killed three and injured 15 other civilians in Kabul Province. At the time of writing, no terror group has claimed responsibility.

Africa

2 April, Jilib – Somalia

Five terrorists were killed in an airstrike on Jibil, one of six undertaken by AFRICOM in early April.

5 April, Amchide – Cameroon

Boko Haram is suspected of being behind a suicide bomb attack in the Far North Region of Cameroon which killed at least 10 and injured 14 others.

6 April, Bamba – Mali

Jama'a Nusrat ul-Islam wa al-Muslimin' (JNIM) terrorists attacked a military base in Gao Region, killing 20 soldiers.

11 April, Achigachia – Cameroon

Three people were killed and one was injured in a suicide attack on the village in the Far North Region. Boko Haram is suspected.

12 April, Maiduguri – Nigeria

At least seven people were killed when suspected Boko Haram fighters attacked vehicles near a village 20km from the capital.

14 April, Cairo – Egypt

A policeman and seven suspected terrorists were killed in a gunfire-exchange in the al-Amiyira district. Three other policemen were wounded.

16 April, N'Djamena – Chad

Forty-four suspected Boko Haram members were found dead in their prison cell. Autopsies indicated they had been poisoned.

21 April, Bulawa – Nigeria

According to the Defence Media Operations, high-ranking Boko Haram commanders were killed in a raid conducted by NAF jets, destroying terrorist compounds.

24 April, Virunga National Park – Democratic Republic of the Congo

Democratic Forces for the Liberation of Rwanda are suspected to be responsible for an attack, which left 17 people dead.

NEWS

Europe

New support for traumatised security staff

In response to additional pressures on security guards from the COVID-19 pandemic – and with lockdown prohibiting training events – charity PTSD Resolution has launched an online interactive version of its Trauma Awareness Training for Employers (TATE) course. TATE is designed to enable staff to recognise post-traumatic symptoms among security guards and other staff; understand the most common observable effects of trauma on behaviour; know how to engage with traumatised staff and when to signpost them to further support; and formulate, through discussion, clear routes to resolve specific workplace difficulties caused by trauma. The course is for security line managers, counterterror operatives and resilience planners among other work roles. Treatment options can include therapy delivered online by TATE organisers PTSD Resolution, which operates a network of 200 therapists. According to research from University of Portsmouth, thousands of security guards are being left traumatised after facing a constant tirade of abuse and violence while on duty. In what is believed to be the biggest study of UK security personnel, city researchers interviewed 750 workers and found almost 40 percent of them were showing symptoms of PTSD.

Additional DASA funding for cyber attack prediction

To further develop technology that predicts and counters cyberattacks, three lead organisations have been awarded nearly £1-million in Defence and Security Accelerator (DASA) funding in the second phase of DASA's Predictive Cyber Analytics competition. The latest recipients are Bristol-based RiskAware Ltd. (awarded around £450,000 in collaboration with the University of Southampton), Vauxhall-based decisionLab (awarded nearly £240,000 in collaboration with DIEM Analytics and Actica) and Gloucestershire-based Montvieux Limited (awarded nearly £250,000). Seven proposals received nearly £1-million in funding during the first phase, bringing the total funding to around £2-million.

Schiphol Airport cybersecurity judged inadequate

An audit by the Netherlands Court of Audit has revealed that the cybersecurity of the border controls operated by Dutch border guards at Amsterdam Schiphol Airport – which handles almost 80-million passengers per year– is not only inadequate, but also far from futureproofed. According to the sobering findings of the audit, few – if any – security tests are performed on IT systems, the software currently used for two of the IT systems has not passed requisite approval procedures and the systems are not linked up to the detection capacity of the Dutch Ministry of Defence. It adds that there is a risk of cyberattacks directed at the three IT systems used for border controls either not being detected or not being detected in time. "As the three IT systems used for the border controls are not linked directly to the detection capacity of a Security Operations Centre, only a certain proportion of any cyber attacks mounted against the border controls are open to immediate detection," the report says. "Our audit of the cybersecurity of the border controls showed that, despite the availability of the requisite expertise and procedures, the cybersecurity procedures adopted are not as effective in practice as they could be," runs the conclusion.

Virtual cybersecurity school for UK teens launches

Thousands of young people in the UK are being offered the chance to join a virtual cybersecurity school as part of plans to nurture the next generation of professional cyberdefenders. Online initiative Cyber Discovery – which offers from-home-access to over 200 free cybersecurity challenges and the opportunity to learn from industry experts at the Virtual Cyber School – aims to inspire future talent to work in the cybersecurity sector. Teens can learn how to crack codes, fix security flaws and dissect criminals' digital trails while progressing through the game. This will help them develop important skills needed for future jobs – particularly in the growing cybersecurity sector. The school – which opens its doors as the National Cyber Security Centre (NCSC) also launches its CyberFirst summer courses online – provides free weekly webinars run by industry experts teaching fundamental security disciplines such as digital forensics, cryptography and operating systems. "We have a world-leading cyber sector which plays a crucial role protecting the country and our digital economy, so it is vital we continue to inspire the next generation of tech talent to help maintain the UK's strong position," said digital infrastructure minister Matt Warman.

WHO reports dramatic increase in cyberattacks

The World Health Organisation (WHO), headquartered in Geneva, Switzerland, has reported a five-fold increase in cyberattacks directed at its staff and email scams targeting the public since the onset of the COVID-19 pandemic. Working with the private sector to strengthen security measures and educate staff on cybersecurity risks, the WHO also asks the public to remain vigilant against fraudulent emails. "We are grateful for the alerts we receive from Member States and the private sector," said Bernardo Mariano, WHO's chief information officer. "We are all in this fight together." In late April, 450 active WHO email addresses and passwords were leaked online along with thousands belonging to others working on the Coronavirus response. The leaked credentials did not put WHO systems at risk because the data was not recent, but the attack did impact an older extranet system used by current and retired staff and partners. The WHO is now migrating affected systems to a more secure authentication system. Scammers impersonating WHO in emails have also increasingly targeted the public in order to channel donations to a fictitious fund.

Americas NEWS

Survey shines light on poor passwords

Ahead of Clario's jargonless privacy and security app launching this summer, a new study by the London-based cybersecurity company and OnePoll has revealed eyebrow-raising stats about American millennials' password practices. Clario and OnePoll conducted an online survey of 2,000 people aged 18-55+ across the United States. The survey found that more than 75 percent of millennials use the same password for more than 10 different devices, apps and accounts, with some confessing to using the same password in more than 50 different places. Also, over 80 percent of Americans (25-35 years old) are concerned about mobile device security – yet 44 percent use password autofill. "Using multifactor authentication, a secured password manager, VPN and staying up to date on data breaches is a good way of protecting yourself from unwanted hacks," commented Alun Baker, CEO at Clario. "However, most people don't follow these recommendations daily."

SecurityScorecard partners with GM Sectec

New York-based cybersecurity ratings provider SecurityScorecard has partnered with digital risk manager GM Sectec. The partnership aims to deliver products and services to the latter's customers in Latin America and the Caribbean. The first phase of the partnership will see the inclusion of SecurityScorecard in GM Sectec's Cyber Essentials toolkit – a portfolio of products and services GM Sectec distributes to its 52,000 customers in Latin America and the Caribbean. The second phase will deliver innovative PCI (Payment Card industry) and MSSP (Managed Security Service Provider) offerings to drive value to customers and help maintain compliance. The partnership will also support GM Sectec in its delivery of managed self-monitoring and vendor risk management (VRM) across the region. "In a fast-moving global economy, businesses in the Latin American and Caribbean regions have a critical need for cybersecurity tools that help protect their data. We are excited to provide that by adding SecurityScorecard to our toolkit of cybersecurity essentials," said Héctor Guillermo Martínez, president of GM Sectec. "We strive to work with the leading tools and services in the world to help organisations understand their true cyber risk and we believe this partnership is an essential step in that direction."

VPN demand rises by more than 40 percent during pandemic

According to data gathered by LearnBonds, demand for commercial virtual private networks (VPN) in the US jumped by 41 percent between 13 March and 23 March. Privacy and security are the main reasons for VPN use. Before the Coronavirus outbreak, the global VPN market was forecast to generate $70-billion profit by 2026, growing 13 percent year-on-year, according to the Global Market Insights 2020 survey. North America was forecast to remain the leading region in VPN usage, with around 30 percent market share. The Global VPN Usage Report 2020 showed that 51 percent of people in the US and the UK use VPN to protect their privacy on public Wi-Fi networks. Another 44 percent of respondents named browsing the web anonymously as the main reason for using the VPN. Secure communication was the third most common reason, among 37 percent of users. Statistics showed that more than 20 percent of Americans and UK residents use virtual private networks to access better entertainment content or restricted download, stream, and torrent sites. However, the increased online traffic caused by the Coronavirus lockdown is expected to significantly boost these numbers by the end of the year.

OSP tackles pandemic-related security threats

The US Department of Homeland Security launched Operation Stolen Promise (OSP) in mid-April to address COVID-19-related security threats and criminal activity. Raising awareness around fraud, the recent OSP initiative combines Homeland Security Investigations' (HSI) expertise in cyber-investigations with private and public partnerships to fight criminal activity and strengthen global supply-chain security. The plan is built around four central pillars – Partnership, Investigation, Disruption and Education – each of which represent a core element of the HSI approach. The OSP website also provides guidance on how the American public can recognise potential fraud, protect themselves online and report suspicious activity to the relevant authorities. At the time of writing, the initiative had resulted in 11 criminal arrests, disrupted 127 instances of illicit activity and analysed more than 21,000 COVID-19-related domains. The HSI is also collaborating with law enforcement partners to identify and investigate financial fraud schemes and target online platforms and Dark Web sites that enable the sale and distribution of illicit materials related to COVID-19 and facilitate financial crime.

MediaPRO chief strategist joins NCSA board

MediaPRO's chief strategist Lisa Plaggemier has joined the US's National Cyber Security Alliance (NCSA) – a leading nonprofit, public-private partnership keeping individuals and organisations safe online by promoting a culture of cybersecurity through education and awareness – board of directors. NCSA's primary partners are DHS and NCSA's Board of Directors, which includes representatives from Cisco, Google and Microsoft Corporation, among others. The NCSA's core efforts include National Cybersecurity Awareness Month (October), Data Privacy Day (28 January), Stop Think Connect (a global online safety awareness and education campaign co-founded by NCSA and the Anti-Phishing Working Group) and CyberSecure My Business (which offers webinars, web resources and workshops to help businesses be resistant to and resilient from cyberattacks). "The NCSA understands that tackling online safety and security today means more than just having the right technology in place – it means ensuring that every person is cyber-savvy," Plaggemier said. "The NCSA has an impressive resume of bringing together public and private efforts to focus on programs aimed at creating individual behaviour change. MediaPRO's mission aligns perfectly with the NCSA's efforts and we look forward to contributing to the mission."

NEWS

Asia

BIMP hits South-East Asian terrorist routes

An INTERPOL-led operation saw law enforcement from Brunei, Indonesia, Malaysia and the Philippines (BIMP) deploy to strategic points along known terrorist transit routes in South-East Asia in a series of simultaneous law enforcement and border control actions in March. Codenamed Maharlika III, the coordinated move resulted in the arrest of more than 180 individuals, including one suspected member of the terrorist organisation Abu Sayyaf Group. The operation saw 82 victims of human trafficking, mainly young women, rescued by Philippine authorities. Firearms, illegally assembled explosives made of ammonium nitrate and other illicit goods and substances worth more than £873,000 were also seized. The World Customs Organisation also partnered in the operation, coordinating the role of customs agents and reporting seizures to INTERPOL National Central Bureaus in each of the countries.

Elbit bags two major defence contracts

Israel-headquartered Elbit Systems has been awarded two multi-million dollar contracts. The first is a $15-million contract from the Swiss Federal Office for Defense Procurement to provide Command and Control (C2) systems for the Tactical Reconnaissance System (TASYS) of the Swiss Armed Forces. The contract will be performed over a three-year period and Elbit will provide reconnaissance battalions and forward observers of the Swiss Army with C2 systems to improve target acquisition, facilitating rapid decision making and engagement. The second is a $103-million contract to supply comprehensive Electronic Warfare (EW) suites for an air force of an unspecified Asian country. Performed over a three-year period, the contract includes long-term integrated logistic support. Elbit will fit the country's helicopters with complete EW suites, including countermeasure systems, providing them with advanced protection.

ACSC issues new cyber-scam threat warning

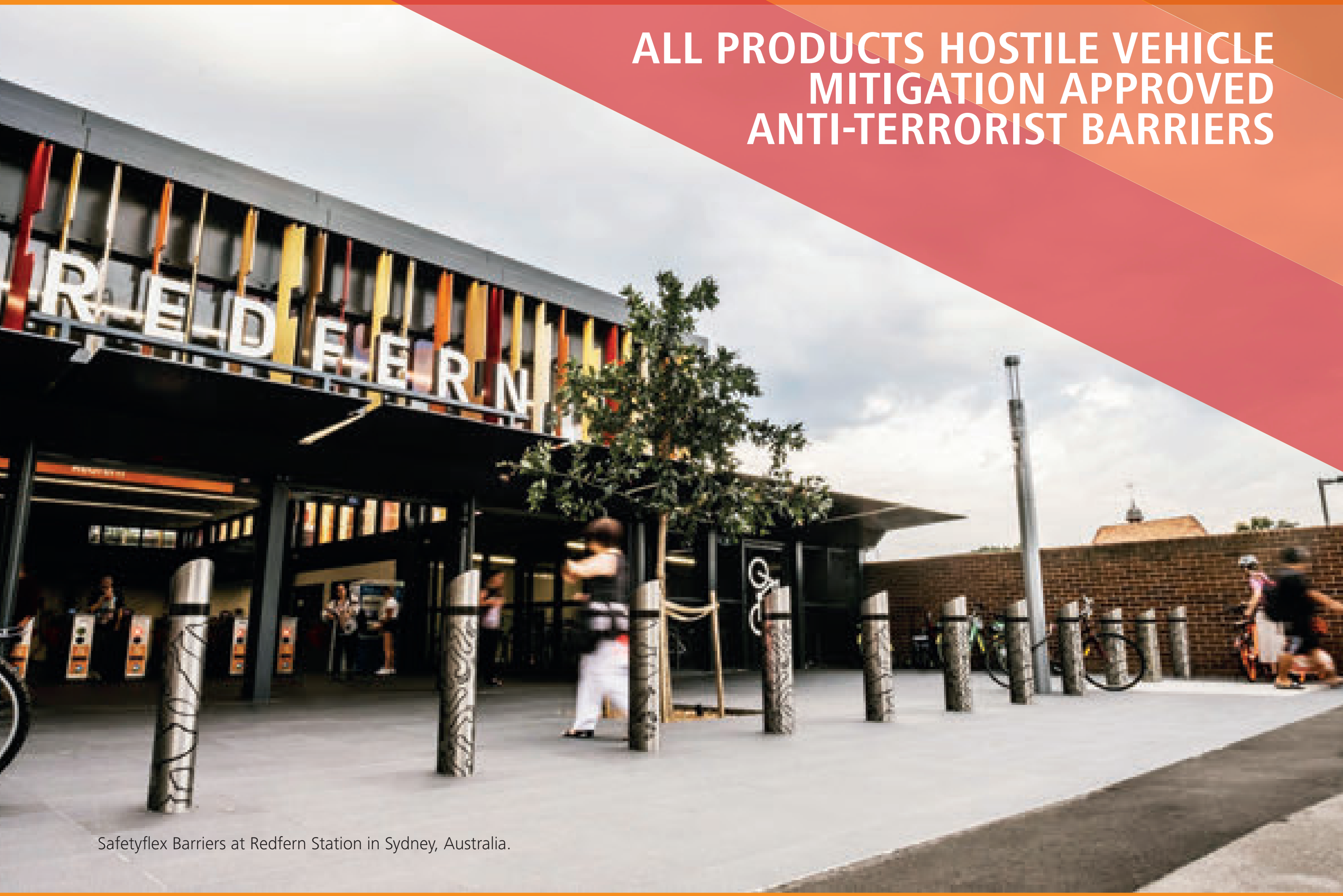
In a new threat update, the Australian Cyber Security Centre (ACSC) has warned that cybercriminals are targeting citizens with an ever-evolving range of COVID-19-themed scams, fraud attempts and deceptive email schemes. Urging vigilance, ACSC head Abigail Bradshaw said that the ACSC had observed cybercriminals adapting their techniques within days – sometimes even hours – of Government announcements, such as relief payments or public health guidance. "The ACSC is focused on protecting Australian families and businesses against cyber-scams and compromises during the COVID-19 pandemic, and helping them to stay safe online," Bradshaw added. "The Australian Signals Directorate has also used its offensive cyber-capabilities to disrupt foreign cybercriminals responsible for malicious cyber-activities exploiting the pandemic. We have stopped them from accessing their own systems and prevented them from accessing information they stole." Since March 2020, the ACSC has received more than 95 cybercrime reports about Australians losing money or personal information to COVID-19-themed scams and online frauds. It has also responded to 20 cybersecurity incidents affecting response services and disrupted over 150 malicious COVID-19 themed websites.

US considers banning China Telecom

The US Departments of Justice and Homeland Security have recommended that the Federal Communications Commission (FCC) revoke and terminate China Telecom's – the US subsidiary of a People's Republic of China (PRC) state-owned telecommunications company – authorisations to provide international telecommunications services to and from the United States. "Today, more than ever, the life of the nation and its people runs on our telecommunications networks," said John Demers, assistant attorney general for national security. "The security of our Government and professional communications, as well as of our most private data, depends on our use of trusted partners from nations that share our values and our aspirations for humanity. Today's action is but our next step in ensuring the integrity of America's telecommunications systems." In its recommendation, several Executive Branch agencies identified "substantial and unacceptable" national security and law enforcement risks associated with China Telecom's operations, which "render the FCC authorisations inconsistent with the public interest". More specifically, the recommendation was based on claimed increased knowledge of the PRC's role in malicious cyberactivity targeting the US and concerns that China Telecom is vulnerable to exploitation, influence and control by the PRC Government.

Cyberattack fears delaying APAC digitalisation

A recent report from Deloitte, commissioned by VMware, analyses cyber-exposure, preparedness and economic opportunity across 12 economies in the region, and reveals that as many as three-in-five businesses in the Asia Pacific (APAC) region have put off digitalisation plans out of fear of cyberattacks. According to the report (entitled *Cyber Smart: Enabling APAC Businesses*), 48 percent of businesses in the region have experienced security attacks in the past 12 months while 63 percent reported interruption due to a security breach. What's more, it finds that large organisations with more than 500 employees in the APAC region may stand to lose as much as US$30-million in the event of a cyber breach. Threats can also flow beyond individual organisations affected to broader business networks using island hopping attack methods. "As the digital economy continues to grow in each country, so does the exposure to cyberattacks," said Duncan Hewett, senior VP and general manager of APAC and Japan at VMware. "Being appropriately prepared can mitigate the risks to organisations and minimise the potential costs of an attack," he added.



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

NEWS

Africa

Kaspersky reveals African corporate sector Trojan attacks

According to the company's recent threat analysis findings, nearly 774,000 users of Kaspersky solutions were attacked by banking Trojans in 2019 – a third of which were in the corporate sector – and almost every hundredth user in South Africa, Ethiopia, Nigeria and Kenya was attacked at least once during the past year. The data shows that Ethiopia has the largest share of corporate users among those who are targeted by banking malware in African regions: it reached 71 percent in 2019, meaning that almost two thirds of banking malware attacks in the country were aimed at the corporate sector. In South Africa, this figure is significantly smaller and can be compared with the global number, reaching 30 percent. Kenya and Nigeria, however, saw this parameter being lower than average, with approximately a fifth of banking malware attacks in Kenya targeting corporate devices, compared with 13 percent in Nigeria.

EU €194-million aid for G5 Sahel

The EU has announced €194-million in additional support to the G5 Sahel countries – Burkina Faso, Chad, Mali, Mauritania and Niger – to help strengthen their security and defence capabilities. Breaking down the package, €112-million is allocated for security and defence, while ensuring respect for human rights and international humanitarian law, as well as re-establishing basic services throughout the territory. The remaining €82-million will be used to intensify development efforts and help improve living conditions of vulnerable populations. "The situation in the Sahel keeps deteriorating and the Coronavirus pandemic cannot make us forget how serious the situation is in a region whose challenges are our challenges as well," VP Josep Borrell explained, adding that the Sahel must remain on top of the international agenda. "I am pleased to see the support from the African Union, including with the upcoming adoption of a stabilisation strategy for the region and the operationalisation of the African Peace and Security Architecture" he noted.

New INTERPOL-Afripol alliance

An online ceremony in April launched INTERPOL's operational working relationship with Afripol, the African Union (AU) Mechanism for Police Cooperation. The two organisations will now implement their joint action plan to position Afripol as a strategic Pan-African policing partner and strengthen the continent's fight against terrorism, organised and emerging crime and cybercrime. The ceremony follows an agreement signed between INTERPOL and the AU early last year to work together in tackling serious global crime. "With region-specific capabilities an essential part of INTERPOL's global police response, this new working relationship is the natural continuation of our longstanding work with African law enforcement… we look forward to tackling Pan-African crime holistically, effectively and together," said INTERPOL secretary general Jürgen Stock. Afripol will now have access to INTERPOL's extensive global criminal databases and secure police communications network, enabling it to work directly with law enforcement in each of INTERPOL's 194 member countries.

Prisons could be epicentres of Cameroon COVID-19 outbreak

Amnesty International has warned that prisons in Cameroon are at risk of becoming epicentres of the current pandemic and called for the release of prisoners of conscience. "As COVID-19 spreads in Cameroon, it is essential that detainees and their families have access to accurate information about the virus. The poor conditions in detention centres mean they risk becoming epicentres of the pandemic unless urgent action is taken," said Fabien Offner, Amnesty International West and Central Africa researcher. "Authorities must take all necessary measures to allow those in prison to enjoy standard healthcare services free of charge and without discrimination, and to urgently reduce the overall number of people in detention." According to the National Commission On Human Rights And Freedoms, the occupancy rate was already extremely high in many prisons in Cameroon, reaching 432 percent in Kondengui and 729 percent in Bertoua prison, for example. Following a Presidential decree on 15 April commuting and remitting sentences, hundreds of prisoners have been released in all of Cameroon's regions. In the Far North, 831 prisoners were released, and the number of detainees fell from 3,370 to 2,547, according to state media.

Great Lakes' security compromised by pandemic

According to the UN secretary-general's special envoy, the onset of COVID-19 is hampering efforts to implement the Peace, Security and Cooperation Framework for the Great Lakes region, and already taking a significant economic toll on countries still working to emerge from years of conflict. Calling for greater international support to consolidate gains, Huang Xia said: "Countries of the region, some of which are emerging from decades of conflict, will need steadfast and resolute support." COVID-19 has forced countries to redirect their priorities, resulting in the postponement of two major events in March: the Great Lakes Investment and Trade Conference, Rwanda, and the tenth Summit of the Regional Oversight Mechanism, Democratic Republic of the Congo. However, signatory countries and guarantor institutions – the African Union, International Conference on the Great Lakes Region and the Southern African Development Community (SADC) – are working together to advance the Peace, Security and Cooperation Framework, Xia explained. Gains have also been made in combating armed groups in Eastern Democratic Republic of the Congo, he noted, pointing to greater coordination and exchange of information among the armed forces of the Democratic Republic of the Congo, Burundi, Rwanda and Uganda.

DIARY DATES

2020 Conference and Exhibition planner

6-8 July SECON 2020

KINTEX, Korea
Organiser: UBM BN Co. Ltd.
Tel: +82 2 6715 5400
Email: global@seconexpo.com
www.seconexpo.com

8-10 September IFSEC International 2020

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

8-10 September 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

22-23 September The Emergency Services Show 2020

Birmingham NEC, UK
Organiser: Broden Media Ltd.
Tel: +44 (0)1737 824010
Email: emmanicholls@brodenmedia.com
www.emergencyuk.com

6-8 October itsa IT Security Expo 2020

Nuremberg, Germany
Organiser: NürnbergMesse GmbH
Tel: +49 9 11 86 06-49 26
www.it-sa.de/en

20-22 October IFSEC South East Asia 2020

Kuala Lumpa, Malaysia
Organiser: IFSEC
Tel: +44 (0)20 7921 8063
Email: ifseccustomerservice@ubm.com
www.ifsec.events/kl/

9-11 November MAST 2020/ Japan Defense 2020

Sheraton Miyako, Tokyo, Japan
Organiser: MAST Communications Ltd.
Tel: +44 (0) 7411 732978
Email: paul.hunt@mastconfex.org
www.mastconfex.com

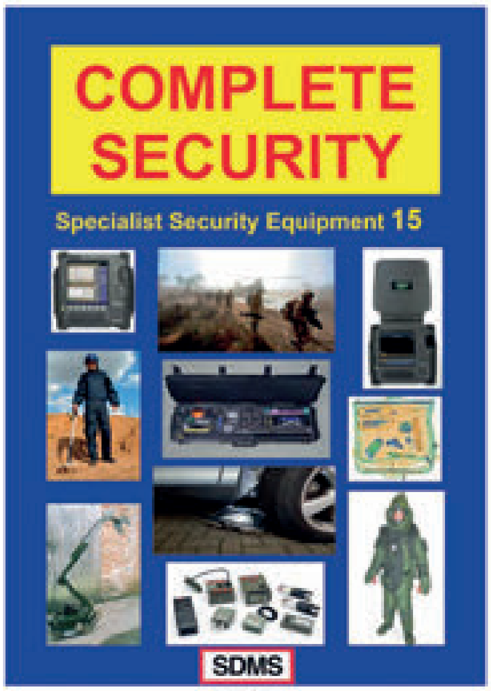
10 November Global MSC Security 2020

Bristol, UK
Organiser: Global MSC.
Tel: +44 (0) 1275 332288
Email: info@globalmsc.net
www.globalmsc.net

17-19 November Global Sicurezza International Security & Fire Exhibition 2020

Milan, Italy
Organiser: Fiera Milano.
Tel: +39 02.4997.1
www.sicurezza.it

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

SAVE THE DATE
2-3 December 2020

INTERNATIONAL SECURITY EXPO 2020

EVOLVING SECURITY THROUGH INNOVATION

OLYMPIA LONDON, 2 – 3 DECEMBER 2020

International Security Expo (ISE) is the only flagship event bringing Government, Industry, Academia and the entire end-user community in charge of regulation & procurement together under one roof to debate current challenges and to source the latest security technologies and services.

400+ Exhibitors

14,000+ Vetted Visitors

THE WORLD'S PREMIER GOVERNMENT & END USER EVENT

50+ Officially Hosted Country Delegations

37% of our audience have a yearly security spend budget of £5M+

76% of visitors have purchasing power or are a direct influencer

79% of visitors in 2019 said sourcing new products was main reason for visiting

NEW FOR 2020:

INTERNATIONAL CYBER EXPO 2020
OLYMPIA LONDON, 2-3 DECEMBER

In association with

techUK

ADS

BIGGER THAN EVER BEFORE

BOOK A STAND NOW –
www.internationalsecurityexpo.com

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**
- Blast threat? **Shock mitigation**

TSS International official distributor for:

RODGARD
HUTCHINSON®
TSS HEAVY DUTY® WHEELS
SEMA WORLD ANTI-TERRORISM SAFETY FEATURES
Téléflow
MOV'IT®
ProtecTank® TSS
B&G electronics
SKYDEX®

TSS®

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

NEW TECHNOLOGY SHOWCASE

Saab's early warning airborne system

Saab has delivered it first GlobalEye Swing Role Surveillance system to the United Arab Emirates. The UAE ordered three GlobalEye aircraft on 29 April, following an original contract that was signed in late 2015, and in November of last year the country additionally announced that it intends to complete the contract amendment for the purchase of an additional two systems. GlobalEye is Saab's new airborne early warning system and control solution. It combines the company's latest Erieye Extended Range Radar along with a range of additional advanced sensors and the ultra-long range Global 6000 aircraft from Bombardier. Commenting on the announcement, Micael Johansson, President and CEO of Saab, noted: "The delivery of the first GlobalEye is a major milestone for Saab, but also an important step in the history of airborne early warning and control. We have set a new standard for the market and I am proud to say that we have delivered the most advanced airborne surveillance solution in the world to the United Arab Emirates."

Introducing the ExMesh Securilath range

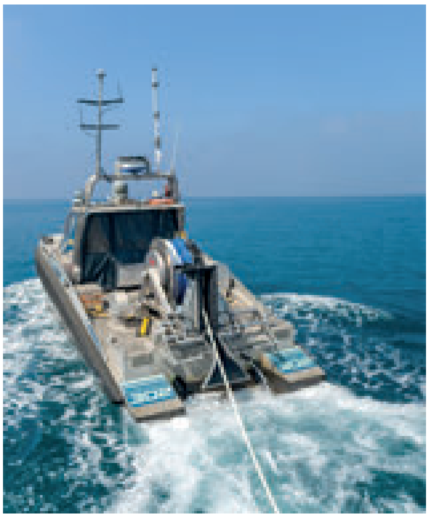
The Expanded Metal Company has achieved new certification for its ExMesh Securilath range. Securilath is now the only security mesh range to be certified by the Loss Prevention Certification Board (LPCB) when applied to metal stud, timber stud and block walls. The enhancements were made in response to the increasing use of metal stud wall systems in construction and is designed to help contractors and end users meet insurance and security requirements. Originally developed in the nineties as a discreet method to protect critical areas, it delays determined intruders from creating an aperture large enough to gain entry to a building and can be situated within internal and external walls, ceilings, roofs and windows. It can be easily fitted during construction or retro-fit and is used by worldwide financial institutions and retailers and at many high-risk sites. After extensive testing, ExMesh Securilath MD1 now holds LPCB Loss Prevention Standard (LPS) Security Rating (SR) 1 certification for metal stud, Securilath HD1 holds LPCB LPS SR1, SR2 and SR3 certification for metal stud and Securilath HDR holds LPCB LPS SR3 certification when applied to block wall.

ASL Group's blast containment

Air Sea Land Group has revealed details of its latest security solutions. The Folding Blast Container is a lightweight, easy to assemble and store containment vessel. The foldable container enables the user to contain a suspect explosive device while awaiting the arrival of a bomb disposal team. Designed to withstand and contain blast and fragments from an explosive device containing up to 200g of PE4, it is said to be flexible and considerably lighter than a standard blast containment bin. When folded up it will fit in the spare tyre compartment of any vehicle, making it ideal for the emergency services, security and defence units or large capacity venues. Following feedback from private and commercial companies, it is also launching its new Flexible Anti-Cut Armour, manufactured using bespoke Legion Flexi-Armour. The soft armour is constructed to significantly increase protection time against hand-held power cutting blades, offering a lightweight and agile alternative to other rigid, flat armours. It can be tailored to fit into spaces where a flat panel armour maybe more difficult to store.

Industry-first super hi-res 8K camera

Security personnel responsible for the safety of visitors at airports, sports stadiums and other wide open environments can now rely on a new high-performance Wisenet video surveillance camera manufactured by Hanwha Techwin, to help detect and forensically analyse suspicious activity. The H.265 Wisenet TNB-9000 has a full-size 43.3mm CMOS sensor to capture true 8K images at 15 frames per second and is equipped with deep learning-based video analytics to detect and classify various object types, including people, vehicles, faces and license plates. The video analytics tool is also able to ignore video noise, waving trees, moving clouds and animals, all of which might normally be the cause of false alarms. Built-in Intelligent Video Analytics include tampering, loitering, directional detection, defocus detection, virtual line, enter/exit, appear/disappear, audio detection and motion detection. There is additionally an audio feature that recognises critical sounds such as raised voices, screams, broken glass, gunshots and explosions, and generates an alert to enable security personnel to quickly react to any incidents.



Elbit's integrated active towed array sonar

Elbit Systems Ltd. has announced the integration of the Towed Reelable Active Passive Sonar (TRAPS) for Unmanned Surface Vessels (TRAPS-USV) onboard its Seagull USV. The sea trials included multiple deployment and recovery cycles, towing at different speeds and transmission at various power levels. Integration of the TRAPS-USV enables the Seagull USV to perform Anti-Submarine Warfare (ASW) operations on the move, substantially extending its operative range and further enhancing its flexibility. TRAPS-USV is a compact low-frequency towed sonar intended for detection, classification, localisation, and tracking of submarines in ASW operations. TRAPS versions are containerised or permanent-fit for any size, diverse purpose vessel. The TRAPS-USV variant is lighter weight but maintains all acoustic active sonar capabilities of the regular TRAPS. The Seagull autonomous multi-mission USV features plug and play, modular mission payload suites and can perform, in addition to ASW, mine countermeasure missions, electronic warfare, maritime security, underwater surveys and other missions using the same vessel, mission control system and data links.

3DX-RAY

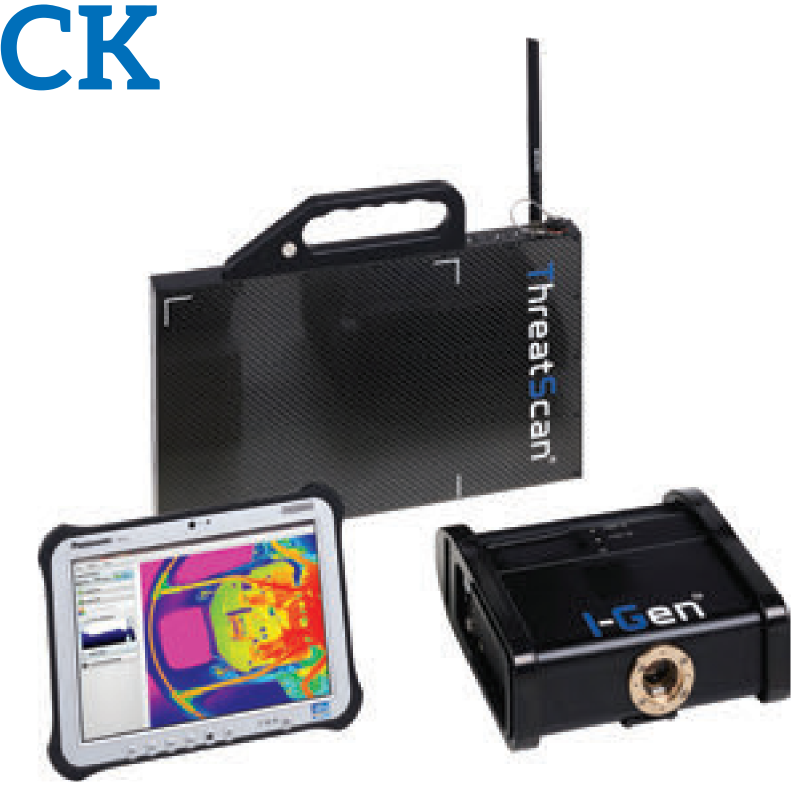
INSIGHT WHERE IT MATTERS

SECURITY IN A BACKPACK

Rapid deployment.
High quality images.
Fast decisions.

Introducing the new, robust and powerful **ThreatScan®-LS3**. Designed in collaboration with first responders, this is a small, lightweight and compact unit that's designed to be rapidly deployed.

High quality, real-time X-ray images (305 x 256mm), materials discrimination, pan, zoom, DeepFocus™, 3D Emboss, measurement and annotation all enable rapid and accurate decision-making.



Optional tablet PC shown.

The complete system fits in a backpack.

www.3dx-ray.com

An **IMAGE SCAN** company

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