www.intersec.co.uk

intersec

The Journal of International Security

May 2021

Hope for the future

How ARIA will benefit UK security technology

RESTORING TRUST

And why national security depends on it

intersec

Volume 31 Issue 5
May 2021

Cover photograph: Getty

Editor
Jacob Charles

Principal Consultant Editor
Maj. Gen.
Julian Thompson CB OBE

Design & Production
jellymediauk.com

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

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

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

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

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

EDITORIAL COMMENT

In scenes more reminiscent of a post-apocalyptic movie, the US public was given a first-hand experience of precisely why cyber security matters at the start of May. Colonial Pipeline – one of the largest fuel suppliers in the United States – was forced to shut down its 5,500 miles of pipeline responsible for carrying and delivering 45 percent of the east coast's fuel after its computer networks were breached and attackers took over control of its pumping operation. The pipeline transports gasoline, diesel and jet fuel (according to Colonial's website, approximately 100-million gallons of the stuff everyday) and services seven different airports in the region. Within days of the announcement, tens of thousands of Americans began panic-buying gas for their cars, leading to queues in petrol stations and further exacerbating the problem.

With almost precision timing, the attack came within days of President Biden's 100-day plan to protect the nation's critical infrastructure against cybersecurity threats. According to the plan, the US Department of Energy, the Cybersecurity and Infrastructure Security Agency and the electrical industry were coming together to: "confront cyber threats from adversaries who seek to compromise critical systems that are essential to US national and economic security".

As reminders go to push this further up the agenda, Colonial couldn't have been much more graphic. While ordinarily ransomware can completely disable the victim's computer or mobile device, locking the hard drive and blocking access to files and data, for an enterprise it can be devastating for productivity, profits and reputation. And that's before you even consider the lives that are potentially put at risk.

For its part Colonial was able to initiate the restart of its operations the following Wednesday after reportedly paying a $5-million ransom to a group called Darkside, which is understood to be made up of criminals based in Russia.

Commenting on the events, UK Home Secretary Priti Patel (who was speaking at the National Cyber Security Centre's CYBERUK 2021 virtual conference) warned that the British government does not support victims of ransomware attacks paying up, noting: "Government has a strong position against paying ransoms to criminals, including when targeted by ransomware. Paying a ransom… does not guarantee a successful outcome, will not protect networks from future attacks, nor will it prevent the possibility of future data leaks. In fact, paying a ransom is likely to encourage criminality to continue to use this approach."

However, doubters need only look to Baltimore for an alternative take on this. When the city was attacked with ransomware in May 2019, it refused to bow down to criminals and opted not to pay the 13 bitcoin ransom (approximately $91,000). Noble though the move was, the city is understood to have spent more than $18-million on its subsequent recovery…

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 2021

CONTENTS

May 2021

www.intersec.co.uk

intersec

Features

Regulars

8

12

16

22
GDPR

28
HEDDLU
POLICE

32

36

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

West prepares for new cold war

Major General Julian Thompson CB OBE Principal Consultant Editor

Recent Chinese pronouncements amounting to 'hands off' warnings to the United States over support for Taiwan are further indications that the West is already engaged in a new 'cold war'. Whereas in the previous version, from 1945 to 1989, the most dangerous adversary was the Soviet Union, it is now China. The latter's aggressive intent was summed up by Admiral John Aquilino the Commander of the US Indo-Pacific Command, when he appeared in front of the Senate Armed Services Committee recently and stated that China considers taking control of Taiwan as: "Number one priority". The Chinese President Xi Jinping's announcement that Taiwan must and will be unified with China by force if necessary gives credence to Admiral Aquilino's views.

Credit: US Dept of Defense

US hunter-killer nuclear submarines have been sent to shadow any Chinese subs shadowing American warships

Whether we like it or not, we need to recognise that we are in a similar situation to the Thirties. In the not too distant future we will be faced with the same temptation to back down in the face of aggression that many succumbed to in the UK back then. There will be those who will view Taiwan in the same way as the 'appeasers' of the Thirties who applauded the British Prime Minister, Neville Chamberlain when he described Czechoslovakia as: "a far away country of which we know nothing". This was the prelude to Hitler taking over.

It is arguable that the potential for trouble today is far more menacing than it was nearly 100 years ago. There are two powerful opponents, plus an array of others, less powerful in conventional terms, but dangerous nevertheless. To use a football analogy, China and Russia are Premier League teams. In a lower league are militant Islamist groups, of which the Taliban is currently the most active. Also in this league are Iran and Pakistan.

How is the US reacting? Leaving China aside for the moment, not too well. President Biden has justified the forthcoming withdrawal of US troops from Afghanistan by citing the need to counter challenges from China and Russia. How resolute he has been in countering the Russians can be judged by his cancellation of a planned transit of the Black Sea by US warships when President Putin of Russia warned Biden off. As for the withdrawal of troops from Afghanistan, the predictions are that like hyenas smelling blood, Pakistan, Iran, China and Russia will move in on the Afghan carcass. The Taliban is the creation of the Pakistan Inter-Services Intelligence Directorate following the 1979 invasion of Afghanistan by the Soviet Union. Pakistan supported the Taliban throughout the Soviet and the US led coalition campaigns in Afghanistan, and still does – for over 40 years. China has also supported the Taliban, and intends continuing to do to maintain influence in Afghanistan as a means of confronting India. Russia, sometimes in collaboration with Iran, has funded and supplied arms to the Taliban in order to challenge the United States and kill and maim US soldiers.

US reactions to Chinese threats to Taiwan have so far been more positive than Biden's to Afghanistan. It is important to remember that democratic and self-governing Taiwan broke from China in 1949, following the take over of China by the Chinese Communist Party. Ever since then Taiwan has been an ally of the US. Allowing China to seize Taiwan would give the Chinese the opportunity to cut off the considerable flow of seaborne trade that passes the island. Furthermore it would severely damage the credibility of the US with its Asian and Pacific allies: Japan, South Korea, the Philippines, Malaysia, Singapore, Australia and New Zealand.

The United States has deployed a carrier strike group and an amphibious ready group with marines embarked to the South China Sea. There are also indications that United States hunter-killer nuclear submarines (SSNs) have been sent to shadow and 'mark' Chinese submarines that might be shadowing American warships. These are thought to be in addition to the normal SSN escorts that accompany a carrier strike group.

The UK plans to send a carrier strike group to the South China Sea. As well as escorts, the group will include Royal Marines from 42 Commando RM. There has been talk in some circles about not sailing the UK group through the Taiwan Strait. This strait – also known as the Formosa Strait – is an international waterway, 81 miles wide at its narrowest part. If British ships did not exercise what is a perfectly legal right to transit the Strait, it would signal lack of resolve. Some British politicians and commentators are suggesting that the UK carrier strike group should not pass through the Strait on the grounds that Britain has no significant Asian interests. Apart from being questionable, such a view is uncomfortably like Chamberlain's: "a far off country of which we know nothing," and we know how that episode ended…

SECURITY AND PUBLIC TRUST

Picture credit: Axis Communications

Dr Frens Kroeger *on why national security depends on solving the public trust crisis*

The UK government needs to get a handle on the crisis of public trust it is facing – and fast. Otherwise we will be increasingly likely to face the challenges of deepening polarisation and home-grown terrorism.

Trust is an indispensable ingredient to security. I have studied its central role both within security agencies – how can they strike the right balance of trust and distrust? – and between agencies and their external networks – how can they manage trust relations with partners and key audiences? Beyond this, however, our national security will be crucially affected by the degree of trust that the public holds – or does not hold – in the government.

Speaking at the Cabinet Office in 2018, I warned that the UK was facing a trust crisis of historic proportions. While met with interest at the time, it appears that trust fell off the agenda again quite quickly afterwards. That is not unusual. While most of us are broadly aware of low trust in government, we tend to focus in on the issue only when it makes the news – recent coverage of David Cameron's conduct in the Greensill lobbying affair springs to mind. Once the turbulence has passed, we direct our attention back to (supposedly) 'harder' realities and forget about trust and trustworthiness again, until the next scandal erupts.

This pattern cannot be allowed to continue for much longer. We finally need to give our undivided attention to the bigger picture of trust or suffer the consequences. This becomes readily visible when considering the numerous anti-lockdown protests around the country or the violence that recently erupted on the streets of Bristol in response to the Police, Crime, Sentencing and Courts Bill: they

The main thing that unites dissatisfied groups is their distrust of the status quo

are merely symptoms of a much wider problem, namely flagrant distrust of the public in the British government and politicians more generally. This level of distrust has been bubbling away for decades and the pandemic has merely brought these feelings to the surface.

But is this really new? While it may be true that there has always been a degree of suspicion in politics and politicians, there are a number of alarming trends that show that the trust crisis we are facing now is one of a kind. It is not just that all surveys and other research indicators consistently show that trust decline in the UK is accelerating; not just that the crisis is expanding, increasingly pertaining not only to trust in government but also in once-resistant institutions like courts or the police. This crisis is historical in nature because it is of a new quality: the public no longer merely distrusts *this* government, but more and more people are beginning to harbour a deep distrust of *all* government, of politics, increasingly even of democracy itself. The new quality of this crisis is that it questions not just the individuals involved or their decisions, but increasingly the system as a whole, the mutual consensus that forms the foundation of co-existence in our communities.

As a result, in the UK, as in many other countries, we are seeing new and unprecedented coalitions in the streets: business owners protesting alongside left-wing conspiracy buffs, suburban anti-vaxxer mums shoulder-to-shoulder with hardened anti-establishment activists from the far right. We need to acknowledge these new realities and confront them head-on; and trust needs to be foremost among our concerns, because the only thing that unites these seemingly so disparate groups is their distrust of the status quo.

So how did it come to this? I would argue that the government's trust problem is homemade. Like many other governments, it has made the grave mistake of regarding trust purely as a communication issue. That is, at regular intervals (usually triggered by one of the abovementioned scandals) they turn their attention to existing trust problems and ask: "What do we have to say so people will trust us?" That is the wrong question to ask. Really, what they would need to ask is: "What do we need to do in order to earn people's trust?" or perhaps even more fundamentally: "Who do we need to be, and what does our internal culture need to be, so that people will trust us?"

Instead we have been caught in a vicious cycle of communication for years. Most governments still choose to ask the simple question ("What do we have to say?"), hiring spin doctors, communication professionals and the big four consultancies to answer it. Inevitably, the PR professionals devise a new communication strategy or slogan, which will often even create some trust in the short term because it *sounds* trustworthy. However, as long as trust and trustworthiness are regarded purely as communication issues, this same strategy will produce long-term distrust. If no substantive actions follow to back up the communication, people tire very quickly of what they perceive as mere lip service. For trust, more than anywhere else, actions speak louder than words, and words on their own are perceived as 'cheap talk'.

This is precisely how we got into the mess we find ourselves in today. Once this cycle has been repeated enough times, even those who were ready to invest trust on the basis of polished government communications are likely to become increasingly cynical. This is where true distrust dynamics kick in. Importantly, distrust is much more than mere lack of trust – it is the active assumption that whatever the distrusted entity says is likely to be a lie. This means that no communication, however cleverly honed and professionally polished, can reach these people and pull them back from the brink. They are likely to immediately discount what you say and, more often than not, retreat deeply into their echo chambers on social media instead. There, driven by algorithms that favour tight-knit groups, their distrust of government, politics and even democracy is likely to deepen further. Polarisation and radicalisation are known to find fertile ground under these conditions.

MORE PEOPLE ARE BEGINNING TO HARBOUR A DEEP DISTRUST OF ALL GOVERNMENT

Considering this dire state of affairs and the self-reinforcing nature of these dynamics, what – if anything – can be done to start rebuilding public trust? Two approaches promise to begin mending the deep rifts between the government and the public, as well as between different factions within the public itself, but both are big undertakings that require stamina.

The first task is to break the vicious communication cycle just described; it could be called an 'anti-communication' approach to trust. This involves shifting the focus from *sounding* trustworthy to actually *being* trustworthy, from lip service (however professional and/or highly priced) to putting your money where your mouth is. That is, rather than hiring the same spin doctors and consultancies over and over, governments need to make trustworthiness a part of everything they do, to build it into the DNA of how government operates.

Because the public can trust or distrust government in so many different respects – from racial equality over climate change to vaccinations – rather than planning 99 important things to do and scheduling another communication initiative to address trust problems as the 100th, this would mean that a real commitment to trustworthiness will need to pervade each of the other 99 as well. What is 'trustworthy' in each context needs to be defined in a process that combines listening to the public with a systematic comparison against the values that the government has defined for itself. In this, the latter values need to be broken down so that they are not mere commonplaces that no-one could ever seriously object to (would anyone disagree with 'doing what's best for the country'?), but instead feature value choices: no-one would speak out against either keeping the public safe and healthy or keeping the economy running – but what if the two are at odds and you have to make a choice?

One could even imagine a National Office for Integrity to do this job; but it would be imperative that any office or ombudsman entrusted with this function be *inward* facing, communicating to everyone within government, not trying to extol the government's newly found virtues to the public. Truly committing to trustworthiness, *being* trustworthy, produces trust on its own – more slowly perhaps (which is unnerving to

▶

politicians who may be thinking in five-year terms at best), but more steadily and lastingly. Once such trust has been built, it remains stable even in the face of bigger challenges.

The second task is an equally big but necessary one. It is to change our electoral system. Why? Because in its present form it facilitates polarisation and distrust and can ultimately provide fertile ground for extremism and violence.

It is important to acknowledge that at its heart, the logic of a first-past-the-post system like the one in the UK, which favours two dominant parties, allows candidates to aim for the support of 51 percent of the population, with little thought or worry given to the remaining 49 percent, even if they are deeply unhappy or violently opposed. In the US with its similar voting system, this was clearly Trump's logic; it led to deeper polarisation than ever before, and ultimately to the storming of the Capitol. It is also reminiscent of the Brexit referendum, whose narrow result of 52 percent to 48 percent divides the country to this day. Wherever the '51 percent logic' is pursued, it drives polarisation and radicalisation because it makes it unnecessary, and therefore over time increasingly unlikely, for the opposing camps to find common ground and engage with each other productively.

NATIONAL SECURITY IS AFFECTED BY THE TRUST THE PUBLIC HOLDS IN THE GOVERNMENT

In a system of proportional representation, such tactics tend to be much less valid. In such electoral systems, a party that lets itself be dominated by extreme views will struggle to find coalition partners needed to form a government. Parties thus typically remain more within a frame that is acceptable to bigger majorities within the public – at least to a degree that allows for productive debate and compromise with political opponents. In addition, votes for parties other than the two dominant ones have a much higher likelihood of actually counting, reducing feelings of being 'left out' and remaining unheard among their supporters and increasing their trust in the political process. Polarisation and radicalisation are much less favoured by such an electoral system.

Both of these approaches are big endeavours that require commitment and stamina, and it is questionable whether this or any other government will want to commit to the risk of undertaking such Herculean tasks. However, doing nothing at all seems the bigger risk now. If we do not break the vicious cycle of distrust that we have been caught in for decades, we can clearly see ahead of us a path that parallels that of the US: one of worsening polarisation, deepening distrust, increasing radicalisation and a growing danger of homegrown terrorism. Our own storming of the Capitol may be less far off than many of us would like to believe. We have arrived at a watershed moment, and we need to act now to address the historic crisis of trust that we are facing if we don't want to frivolously gamble away the security and liberty we value so much ●

Dr Frens Kroeger has studied the causes and effects of trust and distrust for over 15 years. He currently holds a research professorship at Coventry University.

We need to give our undivided attention to the bigger picture of trust or suffer the consequences

Picture credit: TapTheForwardAssist

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

Powerful New Disruptive SDR Technology for the Modern Spectrum Warrior...

RF Geo-Location Heat Mapping is as we say, "Just the Beginning", we have now added a Powerful algorithmic Power Line (PL) Analytical Heat Mapping Capability Supported by the Kestrel ® 3D Energy Probe (3DEP-10) Technology

he Kestrel TSCM ® Professional Software is by Definition and Reputation the Leadin ext Generation, Mission Critical TSCM | SIGINT Technology for Scalability, Flexibilit ase of Use, Low Procurement Cost and Powerful Near Real-Time Deployment Read Software that Address Today's and Tomorrow's Emerging Threat Technology.

The Kestrel TSCM ® Professional Software in Combination with Supported SDR Hardware is the Deployment Standard of the Modern Spectrum Warrior within the Private Sector Corporate and for Public Sector Government, Law-Enforcement, Milita and National Security Infrastructure utilized for enhanced TSCM, RSSM ™, SIGINT an ELINT Roles Worldwide.

Statistical Threat Modelling, Remote Radio Management (RRM) and Digital Demodulation is coming s

AINING: Our Kestrel ® Certified Technical Operator (CTO) ™ Training is Available in Canada or Hosted at Your Own Facility Worldwide. sponse the on-going Pandemic and High Demand for Technical Operator Certification Training, we have the means to deliver the CTO and CGTO ™ program content via our Remote Virtual Classroom (RVC) | Classroom Management System (CMS) Technology.

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 Spectrum Surveillance Requirements.

Kestrel-net ™

Actionable **RF** Intelligen

Professional Development ***TSCM*** Group Inc.

"Innovation is Simply the Beginning..."

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

Picture credit: US Dept of Defense

A NEW HOPE

Arnab Basu *considers ways in which ARIA will benefit the UK – and what makes it distinctive*

Britain needs to be "match-fit for a more competitive world" said Boris Johnson following publication of the Integrated Review of Security, Defence Development and Foreign Policy in March. The country had to be willing to change its approach and adapt to "a new world emerging around us". The Prime Minister's comments reflected wider perceptions of a more perilous landscape at home and abroad. In the February edition of Intersec Jules Werner of QinetiQ outlined the increasing complexity of the security and defence threats to the UK and the democratic world. And amid the turmoil, it makes sense the Government should see science and technology – and new ways of facilitating it – as one of the key solutions to evolving threats ranging from security and terrorism to climate change and pandemics. In addition, Britain, particularly, faces new economic challenges and opportunities from its recent departure from the EU. Science and tech may well be a game-changer in the global dog fight of 21st Century economic competition as well as a source of cooperation.

A new Bill to create the Advanced Research and Invention Agency (ARIA) was introduced to Parliament last month. A potentially pivotal step in establishing the UK as a front runner in scientific and technological innovation, the plans were afoot for some time. In 2019 in its briefings

ARIA unlocks new ways to tackle a range of security issues while invigorating UK industry

for the Queen's Speech, the Government declared a new approach for long-term funding to support visionary high-risk, high pay-off scientific, engineering and technology ideas to complement the country's existing world-class research system. Then, in the July 2020 R&D Roadmap, it put its money where its mouth was, pledging £800 million to develop an independent body focusing on high-level research. ARIA was born.

The new agency will fund, commission and conduct research in core sectors including defence and security. It will identify and support transformational areas of research, empowering some of the world's most exceptional scientists and researchers. ARIA is expected to be fully operational by 2022. But what makes it distinct from research agencies that are currently active and how might it operate?

Existing infrastructure already supports basic and applied research in the sciences and technology. Innovate UK, for example, a non-departmental public body, has invested £2.5 billion since 2007 to aid business and research collaborations, accelerate innovation and drive business investment into R&D. However, existing agencies' speed and responsiveness is often compromised by bureaucratic and other institutional constraints. Such constraints can restrict the ability of agencies to quickly and responsively invest in creation of cutting-edge military, commercial and civil products. What sets ARIA apart from pre-existing agencies is its flexibility and, arguably, tolerance of failure as an essential part of technological discovery. It will be equipped with unprecedented powers to develop ambitious research at previously unseen speeds. Matching this, is an innovative funding approach – including seed grants and prize incentives – and the ability to start and stop projects based on success.

"To rise to the challenges of the 21st century we need to equip our R&D community with a new scientific engine – one that embraces the idea that truly great successes come from taking great leaps into the unknown," said Science and Innovation Minister Amanda Solloway prior to the Bill's introduction.

ARIA IS PIVOTAL IN ESTABLISHING THE UK AS A FRONT RUNNER IN SCIENTIFIC INNOVATION

ARIA is broadly but explicitly modelled on the US DARPA project, which has driven military capabilities and security innovations since the Cold War. This was originally founded by Eisenhower in the Fifties as the Advanced Research Projects Agency (ARPA) after the Soviet launch of Sputnik. The technological sophistication of the launch in 1957 took the West by surprise. Following this momentous event, ARPA orchestrated competing American missile and space projects, allowing the US to catch up and get ahead in the space race. Though the US agency was created specifically to enable research with potential military applications, many of ARPA/DARPA's projects have also had great influence in the civilian sphere. For example, DARPA could be described as the father of Silicon Valley for its work provided the basis for the modern internet. For over 60 years since its foundation, DARPA has worked with innovators and manufacturers inside and outside government. Fruits include ground-breaking military advances – precision weapons, research on antiballistic missiles, nuclear test detection, radar, high-energy beams, computer science and advanced materials. Projects on 'stealth' compounds have rendered US F-22 fighters and B-2 bombers 'invisible' to enemy radar. New battlefield sensors, blue-green lasers and non-acoustic submarine detection are also among its achievements.

Importantly, DARPA comprises experts at the top of their fields in both academia and industry, who are looking to push the limits of their discipline. They generally serve the agency for only three to five years, fuelling a unique urgency to achieve success in less time. ARIA is expected to emulate key features of the US model including significant autonomy for its project managers and the tolerance for failure in pursuit of transformational defence. Crucially, ARIA will not be subject to Public Contract Regulations or the Freedom of Information Act. This will drastically reduce time spent processing FOI requests and protect Britain's competitive advantage, while allowing the agency to run an extremely lean and agile operating mode. Recognising high-risk research requires patience. The ARIA Bill confers the necessary long-term security, with a 10-year grace period before ARIA's potential dissolution can be triggered.

Ramping up national security has been a key component of the UK Government's agenda in recent times in response to organised crime and evolving terrorism. It recently announced some £340 million towards further enhancing the UK's nuclear detection capability over the next five years. In November 2020, the PM declared the largest military investment in 30 years. ARIA therefore seems the next logical step as the UK bolsters its defence prowess.

But leanness alone will not guarantee success. If it is to closely resemble DARPA, the agency must also foster dynamic relationships between various players and businesses within the security and defence sectors, developing and exploiting the results of their research.

British-based Kromek has worked with DARPA for many years and so appreciates first-hand the value of such an agency. The company's high-performance security screening and nuclear radiation detection equipment is deployed in 25 countries including the US. The nuclear detection products it develops and supplies have been integrated by DARPA for use by the US Department of Defense. One of Kromek's radiation detection solutions currently protects critical infrastructure in New York, and the company is collaborating with DARPA on a system to detect viruses, including SARS-CoV-2, in open spaces.

Naturally, Kromek welcomes introduction of the ARIA Bill and believes freeing the agency from administrative constraints such a FOI requests will enable concentration of resources into streamlining transformation projects, bolstering Britain's competitive advantage.

Paul Howell MP for Sedgefield told Parliament: "Innovation-led funding that accepts a higher risk can be the key that opens scientific advances quicker. It also provides better opportunities for such companies to develop production and supply chains in the UK."

ARIA is not the first agency to model itself on DARPA. Germany's Federal Agency for Disruptive Innovation known as SPRIN-D was created in 2019 to discover highly innovative research projects, support their development and help them break into the market. SPRIN-D has a budget of approximately $1 billion to 2029 and is designed to allow innovative entrepreneurs to advance ideas with as much flexibility as possible. Similarly, Japan's Moonshot R&D programme collaborates across various governmental departments and with academia and industry to develop scientific solutions for a plethora of needs such as sustainable care systems for major diseases and sustainable global food supply.

With ARIA support and funding, stories like Kromek's could become commonplace in the UK, generating job opportunities and addressing the specific needs of the UK's security and research and development landscape. An agency actively looking to collaborate with industry leaders regionally would also fulfil the Government's levelling up agenda and help stop the brain drain, Paul Howell said.

However, despite ARIA's flexibility, it will still have administrative and legal obligations. ARIA will be required to proactively share information on its activities. It will also be subject to the usual National Audit Office oversight of public bodies and Parliament will scrutinise its annual report. Furthermore, the Business Secretary will have power to intervene in the interests of national security, including directing the agency to cease collaboration with hostile actors or end a particular programme.

By greenlighting ARIA, the UK Government has made a clear move to align itself with other world nations that currently deploy DARPA-inspired agencies like Germany and Japan. The initiative will open the door to partnerships with multiple government department customers, unlocking new ways to tackle a range of security and societal problems while invigorating UK industry. Most of all, it will cement the United Kingdom as a scientific and technological powerhouse in the wake of Brexit and the COVID-19 pandemic ●

Doctor Arnab Basu is the founding chief executive of Kromek Group, a spin-out from Durham University. It supplies cutting-edge radiation detection technology for Homeland Security, medical, industrial and laboratory applications.

Kromek's bio-threat detector developed under a DARPA project

Picture credit: Kromek Group plc

MESA™

A new spectrum analyzer with Broadband Utility.

Detecting and locating illicit transmitters requires an agile, portable, handheld spectrum analyzer to measure power and frequency of unknown transmissions. The new MESA™ (Mobility Enhanced Spectrum Analyzer) delivers precision, high performance, and versatility for assessing RF energy in a variety of environments. The MESA™ is a handheld RF receiver that detects and locates illegal, disruptive, or interfering transmissions throughout wide frequency spans up to 6GHz, or 12GHz with the Down Converter Antenna.

International Procurement Services (Overseas) Ltd

sales@intpro.co.uk
118 Piccadilly London W1J7NW
phone: +44 (0)207 258 3771
fax: +44 (0)207 569 6767

- **Portable**
- **Efficient**
- **Full touch screen control**
- **Full complement of antennas/probes**
- **Sweep modes:**
  Spectrum View
  SmartBars™ (Patented)
  Mobile Bands
  Wifi
  Bluetooth®
- **Sweep Speed**
  >200 GHz/second
- **Operating Freq. Range**
  10 kHz - 6 GHz /*12 GHz
- **Variable Resolution Bandwidth**
  0.0380 kHz to 312.5 kHz
- **Instantaneous Bandwidth**
  25 MHz
- **DANL - Noise Floor**
  500 kHz RBW
  with Pre-amp:-102 dBm
- **Detection**
  RF, Carrier Current, Acoustic Leakage, IR/Visible Light, Ultrasonic
- **Spurious Free Dynamic Range**
  81.6 dB
- **AM/FM Audio Demodulation with filter options**
  Auto, 200kHz, 20 kHz, 5 kHz
- **Case/Contents Weight**
  15lbs. / 6.8kg

*Down Converter Antenna

REI®

reiusa.net

A LAYERED SECURITY APPROACH

Tony Kingham *discusses the role of low dosage Through Body X-Ray Scanners in airports, prisons, VIP Protection, government and commercial security.*

Bad actors, whether they are terrorists, drug traffickers, smugglers or thieves, always have one advantage and that is, surprise. They can choose the time, the place and modus operandi for their nefarious activity, which they can change at a moment's notice.

They can turn up at an intended target one day, notice unexpected security measures and simply change their mind. They can change the day or even the target. If you are a terrorist and you are planning to blow up an aircraft or a drugs trafficker running mules, there are 117 international and 558 regional airports in the US alone. It is what the military would call, a target-rich environment. That means that the security community has the unenviable task of being ready everywhere, for all eventualities, all of the time!

Unfortunately, all too often, security measures are based on historical events, especially at airports where security is largely in the hands of airport operators. For instance, after several high-profile attempts to destroy aircraft by smuggling explosives on board, such as the 'shoe bomber' Richard Reid in 2001 and the 'underpants bomber' on Christmas day 2009, millimetre wave scanners were introduced in airports worldwide.

Millimetre wave scanners are a vital part of any layered security system and after some initial public concerns about privacy and safety, they are now accepted as routine. However, millimetre wave scanners are only able to detect items carried on the body, not in it. Which leaves aircraft vulnerable to attack from an IED carried inside a body cavity. Until the day we develop a safe standoff explosive detection technology, airliners will remain vulnerable. This might seem far fetched to some, but this method of attack has been used in the past. But more of that later.

The bizarre thing is that a technology to identify substances, organic and non-organic, hidden inside the body may well already be in use at the airport, but in arrivals, not departures. Customs officials have been using full body X-Ray scanners in arrivals for years, to find drug capsules ingested or inserted in body cavities by drug mules. Of course, these machines are not for mass scanning of passengers, but are a tool that is both quick and safe to be used when a trained customs official is suspicious of a particular passenger. So, why are they not available to security teams in departures as well?

Customs officials have been using full body X-Ray scanners in arrivals for years, but why not departures?

The real growth area for use of full body X-Ray scanners has been in prisons, custodial facilities, and detention centres. The escalation of drug use in prisons worldwide has reached epidemic proportions and has prompted the roll out of X-Ray scanners, as the only fool proof method of detecting contraband smuggled in body cavities without employing degrading body cavity searches. This technology enables the basic human rights of inmates (and visitors and staff) under the United Nations' Mandela rules, to be observed and their dignity preserved in what in the past has been an unpleasant and invasive process.

X-Ray scanners are equally effective in detecting mobile phones, sim cards, weapons and anything else that can possibly be inserted where it should not be. But there are other areas where this technology could prove invaluable and VIP Protection is one.

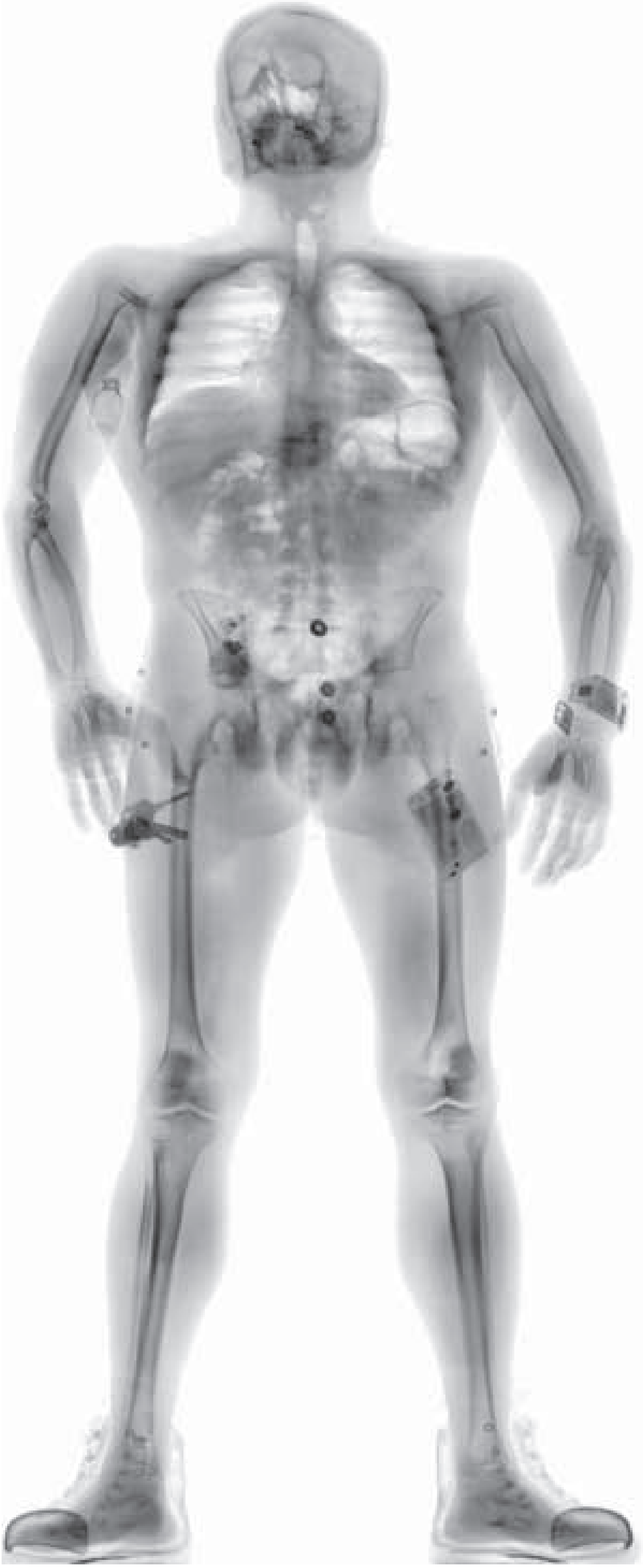
Back in 2009, a suicide bomber attempted to assassinate the Saudi Interior Minister, Prince Mohammed Bin Nayef. The bomb hidden in a body cavity was detonated by remote control, while the perpetrator was in a meeting with the Prince. The same method again in 2012 in an attempt to kill the Afghan Intelligence chief, Asadullah Khalid, resulting in Mr Khalid being seriously injured. On both occasions the would-be assassins passed through extensive security screening, but the IED's were carried internally and were not detected.

Through body X-Ray scanners would have easily identified an IED carried in body cavities, as well as any other weapons or objects carried on the body, making them far more effective than millimetre wave scanners for VIP protection.

State and corporate espionage is another critical area of concern that has been making headlines in recent years. Whether it is state actors like China, Russia or North Korea attempting to breach national security organisations or state and non-state actors attempting to steal commercial information or intellectual property.

Recent focus has been on cyber vulnerabilities, and many organisations have now created an air gap between their critical data and the internet as probably the only fool

Picture credit: OD Security



proof way to protect their secrets from cyber hackers. But insider threat remains a major concern for national security secrets and intellectual property for western governments and the commercial and industrial complex.

In 2013, Edward Snowden a computer intelligence consultant, copied and leaked highly classified information from the National Security Agency, when he was a Central Intelligence Agency employee and subcontractor. He stole thousands of documents using a USB flash drive. Given that you can buy drives with 1TB of capacity, if a foreign agent or disgruntled or criminal employee gained access to your system, that is an awful lot of data stolen.

Post Snowden, many government agencies have forbidden the use of USB drives and even banned them from being taken into a building (the NSA had all USB ports filled with liquid concrete). Less radically and more likely however is that IT departments will use IT solutions to block unauthorised human interface devices (HID's) such as flash drives, mice, *etc*. from the network. But there are other devices that can be used to steal data from computers with blocked HID's, such as USB drives that imitate an Ethernet adapter to gain access to the network.

Given the capacity of these drives and their small size, only by ring fencing critical data with an air gap and physically enforcing a "no unauthorised device" policy, can data ever really be secure. By way of experiment, I had a conversation with a colleague with a USB drive in the cheek of my mouth and they were none the wiser.

MILLIMETRE WAVE SCANNERS ARE ONLY ABLE TO DETECT ITEMS CARRIED ON THE BODY, NOT IN IT

An X-Ray scanner is the only way of enforcing a "no unauthorised device" policy. Instead of taking data out, critical infrastructure is vulnerable to insiders, visitors and contractors taking damaging data in, such as malware or introducing systems sabotage programmes. Even with an air gap and enforcing a no unauthorised device policy, the damage that could be done to the power grid or nuclear power station can be imagined! Once again, an X-Ray scanner is the only practical way of enforcing a "no unauthorised device" policy.

Finally, we come on to property theft. The great South African diamond house De Beers was the pioneer in the introduction of low dosage X-Ray scanners to prevent miners from going home at the end of a shift with more than they arrived with. Virtually anything small and valuable can be hidden in a body cavity. The higher the value, the more likely that a small number of staff members will be tempted to see theft as an easy opportunity to make big money and diamonds are worth big money.

Criminal gangs may also coerce staff through entrapment or threats to them or their families. Physical searches of hundreds of miners everyday was simply not a practical way of dealing with a problem that could have been costing the company millions. So, with local manufacturer Lodox Systems, they developed the first low dosage through body X-Ray scanner and deployed them at their mines with great success. Of course,

▶

diamonds are not the only small, high-value items. There are all sorts of other precious stones mined, traded, and manufactured worldwide.

In addition, as more and more manufactured goods such as MEMS sensors (micro-electro-mechanical systems) are miniaturised for the transport and space industries, the more potential there is for this type of crime in other markets. This brings us full circle back to drugs and drug smuggling.

Not all drugs smuggled are illegal substances. The pharmaceutical industry is one the world's biggest industries, and produces manufactured drugs that are worth more than the illegal kind. Zolgensma, a treatment for spinal muscular atrophy is priced at a hefty $2.1 million per dose. Actimmune is $57,310 per 6ml vial. Acthar is $40,000 per 5ml vial. Ravicti is $5,017 for one bottle of 25ml. I could go on, but you get the point.

And that brings us right up to date and the COVID-19 vaccine. The United Nations Office on Drugs and Crime, UNODC issued a document entitled *COVID-19 Vaccines And Corruptions Risks: Preventing Corruption in the Manufacture, Allocation and Distribution of Vaccines*, which noted that secure storage and distributions systems are critical for the safe delivery of COVID-19 vaccines and the mitigation of the risk of vaccines being diverted from public supply to black markets.

In any crisis, there is opportunity for those unscrupulous enough to exploit it, and the Coronavirus pandemic is no exception. So inevitably COVID-19 vaccines have become a target for criminal gangs and individuals seeking to make a quick buck.

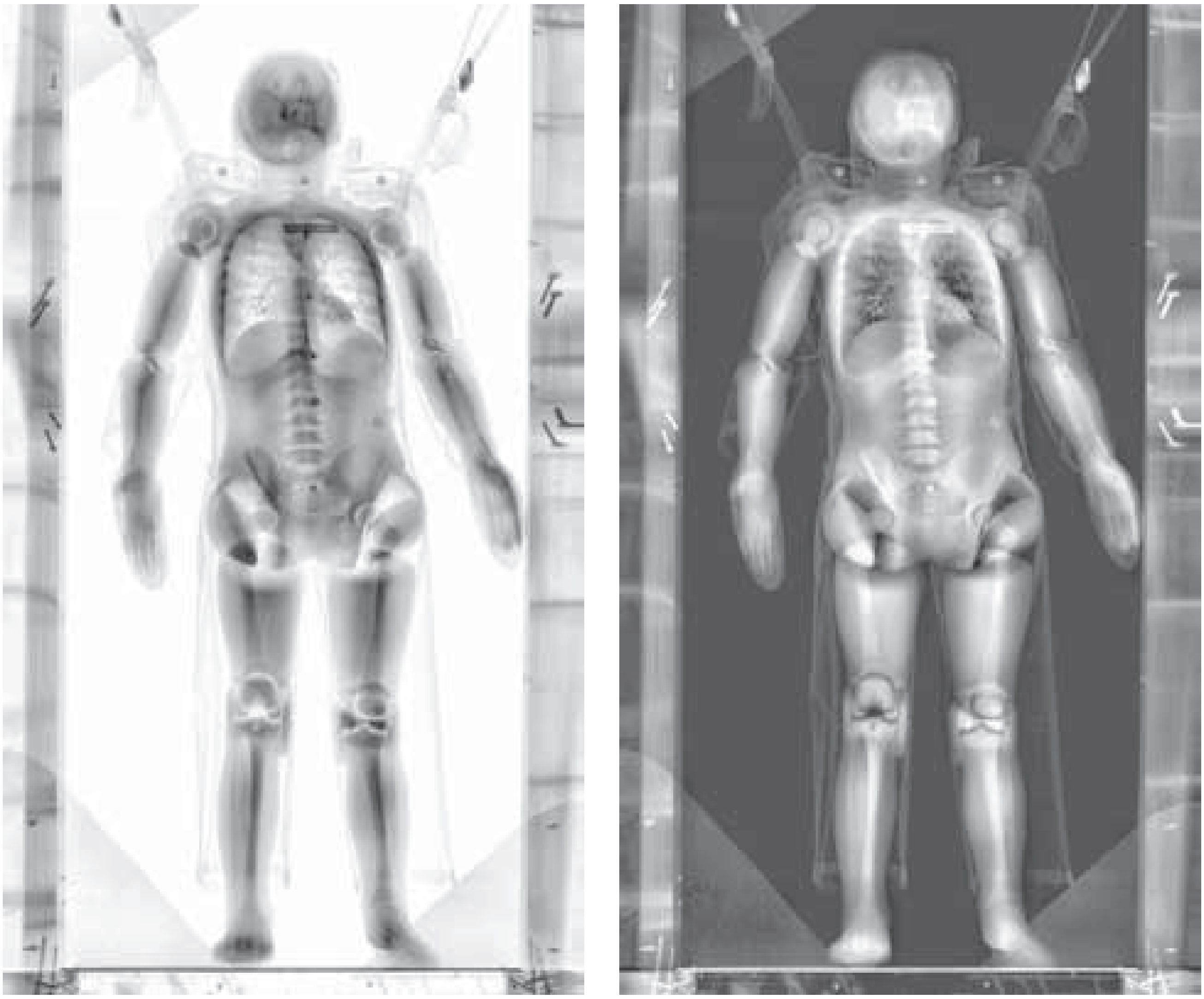
Manufacturer of Through Body X-Ray Scanners ODSecurity sells its systems primarily to the prison and airport markets and was recently contacted by a pharmaceutical company to investigate the possibility that its scanner – the Soter – could detect glass vials. The trial was highly successful.

Mr van der Veen of ODSecurity picks up the story: "We were recently contacted by a pharmaceutical company and tasked with investigating the possibility of installing a body scanner in their warehouse. We ran tests of various glass vials hidden within the body and on the body – full and empty. In each case the results were amazing. The scans showed 100 percent clarity of the glass vials shown on all scans taken by the Soter RS Full Body Scanner."

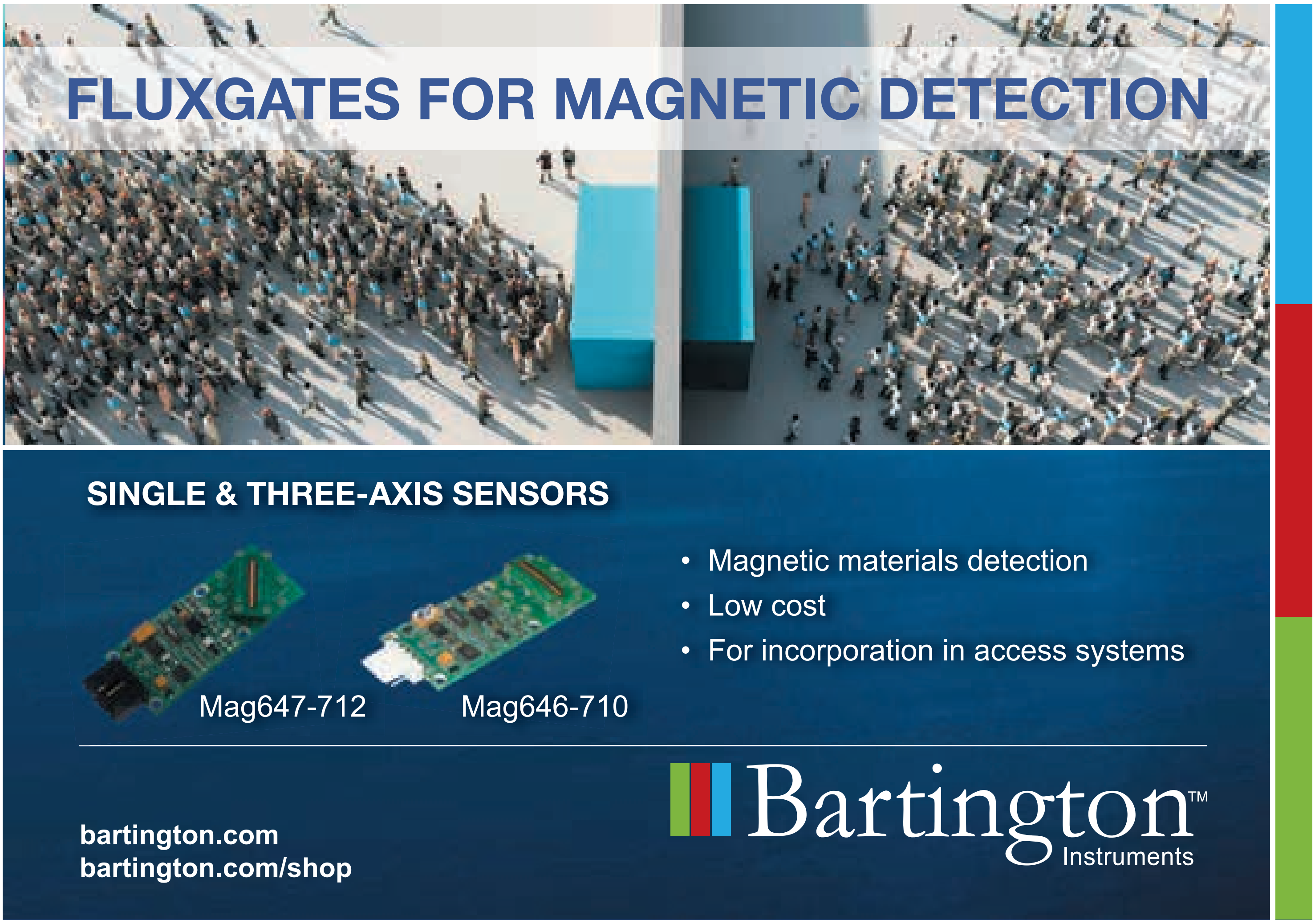
Sadly, the world we live in has plenty of people that do not share the values of you and I, and are prepared to go to any lengths to get what they want, whether that is in pursuit of their political aims by violence or profit from crime. There is no 'silver bullet' security technology, but Through Body X-Ray Scanners are key technology that address a range of security vulnerabilities and should be considered as a part of any effective layered security approach ●

Tony Kingham is a freelance journalist and publisher of www.WorldSecurity-index.com, specialising in information and public relations within the defence and security markets. He is also Communications Director for BORDERPOL.

X-Ray scanners are the only fool proof method of detecting contraband smuggled in body cavities aside from invasive body searches



Picture credit: ODSecurity



ELECTRONIC COUNTERMEASURES

IPS EQUIPMENT & SWEEP TEAM SERVICES

NEW REI MESA MOBILITY
ENHANCED SPECTRUM ANALYZER

NEW ANDRE DELUXE 12GHZ
WITH ULTRASONIC PROBE

VIDEO POLE CAMERA
2.0 INSPECTION TOOL

EDD-24T NON LINEAR
JUNCTION DETECTOR (HANDHELD)

TSCM TRAINING
COURSES &
CERTIFICATION
UK/US/GLOBAL

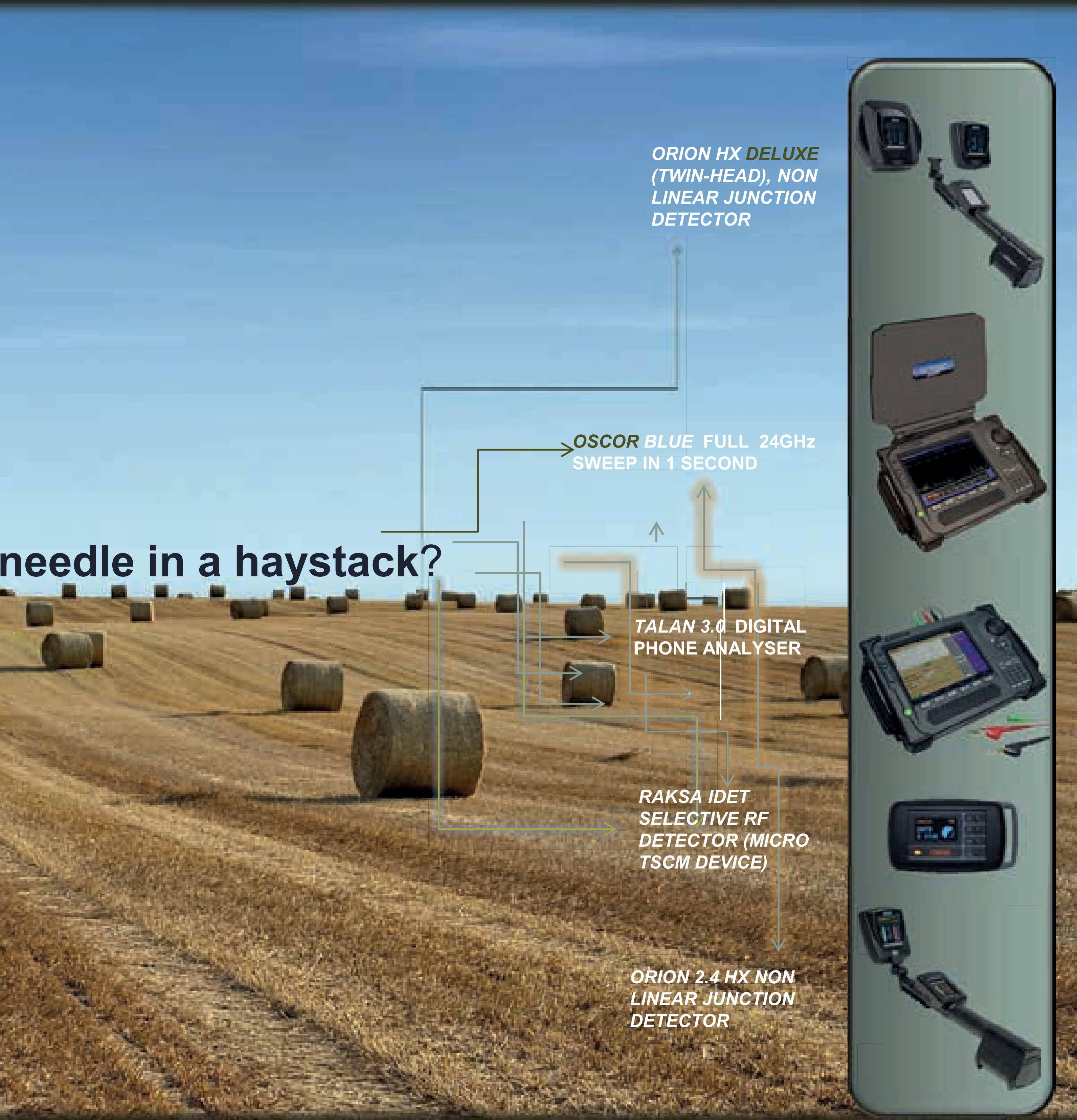
Looking for a

For details, demonstrations, sales and 24/7 response, contact:

International Procurement Services (Overseas) Ltd,
118 Piccadilly, London, W1J 7NW Email: sales@intpro.com
Phone +44 (0)207 258 3771 FAX +44 (0)207 724 7925

Rapid Quote:

Photograph or scan this image with your smart mobile to automatically request info / call back.



needle in a haystack?

ORION HX DELUXE (TWIN-HEAD), NON LINEAR JUNCTION DETECTOR

OSCOR BLUE FULL 24GHz SWEEP IN 1 SECOND

TALAN 3.0 DIGITAL PHONE ANALYSER

RAKSA IDET SELECTIVE RF DETECTOR (MICRO TSCM DEVICE)

ORION 2.4 HX NON LINEAR JUNCTION DETECTOR

TSCM Equipment supply, training and de-bugging services

The preferred choice of Government & Law Enforcement Agencies worldwide.

Web: **www.intpro.com**

GDPR: THREE YEARS ON

Nicola Howell *explains why the General Data Protection Regulations are more important in 2021 than ever*

GDPR. Four letters that send shivers down the spine of businesses large and small. While 2018 feels like an age ago, the scramble to prepare for the General Data Protection Regulations feels like yesterday. The new processes, the HR meetings, the flurry of emails updating customers on the business' updated data policies – who could forget them?

Thankfully, things have calmed down in the last few years. Most businesses are 'over the hump' as it were, having successfully put in place policies and procedures that make them compliant. Indeed, many are discovering that GDPR compliance has more utility than simply avoiding a nasty fine. The regulations encourage best practise for maintaining data health, ensuring businesses have data that is accurate, up-to-date and fully secure. That's not to mention deeper bonds with customers who feel more confident that their data is being properly looked after.

And yet, 2018 was a long time ago. Times change – even without Brexit and a global pandemic. As the world moves inexorably on, so does businesses' relationship with GDPR as data becomes ever more integral to operations.

NOW THE DUST HAS SETTLED

In this article, I want to give a bit of a GDPR update. Now the dust from that initial scramble has settled, how are businesses faring? How has and will Brexit impact them? And as we emerge into a post-COVID-19 world, how will the rules evolve to account for a business landscape that, more than ever, has data at its very heart?

One of the strange dichotomies of 2018 was that, as businesses were shaping themselves to comply with GDPR, they were also acutely aware that the UK was leaving the EU. However, at the time the exact shape of that exit was uncertain to say the least, and questions were asked about whether the EU's shiny new regulations would be preserved in UK law.

We do now have some clarity on that. As you may know, GDPR has been transposed into UK law almost exactly, which of course is good news for those worrying about having to repivot their organisation to match a new set of regulations.

While there is no action to take immediately, businesses should be aware things will change in the future. The UK and the EU have set themselves on divergent tracks that will only become more pronounced over time. Inevitably, GDPR will be changed, moulded and evolved to suit the individual needs of the UK as it seeks its new place in the world. Eventually EU and UK GDPR regulations may indeed look very different – and businesses must be prepared to adapt accordingly.

On the subject of Brexit, there has been one very good piece of news: the UK data protection policies have been awarded 'adequate status' by the EU. This means that, from the EU's perspective, the UK is able to adequately handle the data of EU member states. UK businesses can therefore freely continue to receive and process EU data, making it much easier to do business in Europe. This is critical for those who actively depend on their European channels. It means they have a pre-existing data transfer mechanism in place and don't need to enter into a new contract to maintain data standards.

It is worth mentioning that, as good as having adequate status is, it does represent a significant reduction compared with what the UK had before. The UK will not be invited to the table when it comes to making amendments to the regulations. If the UK wishes to keep its adequacy status, it must continue to align to European regulations – which is of course counterintuitive to the UK forging its own path.

> THERE IS NO EXCUSE NOT TO BE COMPLIANT. IF YOU'RE NOT, YOU RISK A HEFTY FINANCIAL PENALTY.

Furthermore, having EU adequate status doesn't benefit UK organisations when it comes to dealing with businesses further afield. America and China for example – two countries the UK hopes to trade more with in the future – may have different conditions that UK businesses will need to satisfy. Overall, in the short term, businesses are in a good place and the status quo has been maintained. But from a long-term perspective, the future cannot be predicted – and businesses must be prepared.

Brexit is only one major event that has had an impact on GDPR. The more pressing concern is of course COVID-19. The first point to make is the most obvious one: now that many of us are working from home (and that working remotely is likely to be a major trend in the future), the way we physically stay compliant will change.

Organisations will need to update their policies to cover those small-but-important processes. Now there

If businesses have relevant, accurate and up-to-date data, they will have keener insights and will be able to make smarter decisions

is no office shredder, how should employees dispose of sensitive documents? How should employees conduct meetings when there may be others within hearing distance? And when BYOD (bring your own device) is more common than ever, what measures should employees take to ensure a family member doesn't accidently access documents on a shared computer? These though are minor hurdles that can be overcome with training and a cultural shift. What is more important is ensuring infrastructure is up to scratch.

EMBRACING REMOTE WORKING

Data needs to be secure in order to be GDPR compliant. But the move to remote working is effectively widening businesses' security perimeter from a single building to potentially the entire globe. It's one thing to ensure only a certain type of computer in a single location can access data. But when a multitude of devices in multiple regions or even countries need to access it, keeping out bad actors while ensuring a smooth experience for employees is a big hurdle. This is of course not just a GDPR challenge. It falls into the wider bucket of security and is doubtlessly an issue businesses are grappling with now as they are forced to embrace remote working.

As technologies like the cloud become more commonplace and remote working becomes a staple of working life, questions about where data is stored and how it is kept secure will become even more important.

But remote working won't be the only lasting impact of COVID-19. The pandemic has turned the economy on its head: shop doors have been closed, high streets have been emptied and countless businesses have shut down. As it stands UK, 97 percent of businesses in the UK have already been disrupted as a result of the pandemic, as revealed by Dun & Bradstreet's COVID-19 Commerce Disruption Tracker.

The downtick in the economy could very well trigger a recession, which after a year of turmoil is exactly what businesses don't want. If this were to happen, it would be the second recession since the 2008 financial crash. Those in business back then will remember how during those hard times it was vital to migrate risk as much as possible. By having the right insights, businesses can make smarter decisions and weather hard times. And that brings us to data.

Data is crucial for providing these insights. If businesses have relevant, accurate and up-to-date data, they will have keener insights and will be able to make smarter decisions. For this reason, GDPR is vital. Failure to comply won't just result in fines, but will mean businesses won't have access to the best data possible – thus harming their decision making.

Another point to make is that many businesses, in the absence of having their own first-party data, will use a data supplier to get those market insights. This is a wise choice for many, but businesses must remember to check the data suppliers' GDPR practises. If they buy data from a company that doesn't comply with GDPR, then vicariously they won't comply either.

And this is true from a wider partner perspective too. On the brink of hard economic times where businesses will be using data more than ever before, they must be sure to step back and do their due diligence. The need to make sure any data you process – which has been sourced by a supplier or partner – is fully compliant and won't land them in trouble.

> GDPR WILL BE CHANGED, MOULDED AND EVOLVED IN THE FUTURE TO SUIT THE NEEDS OF THE UK

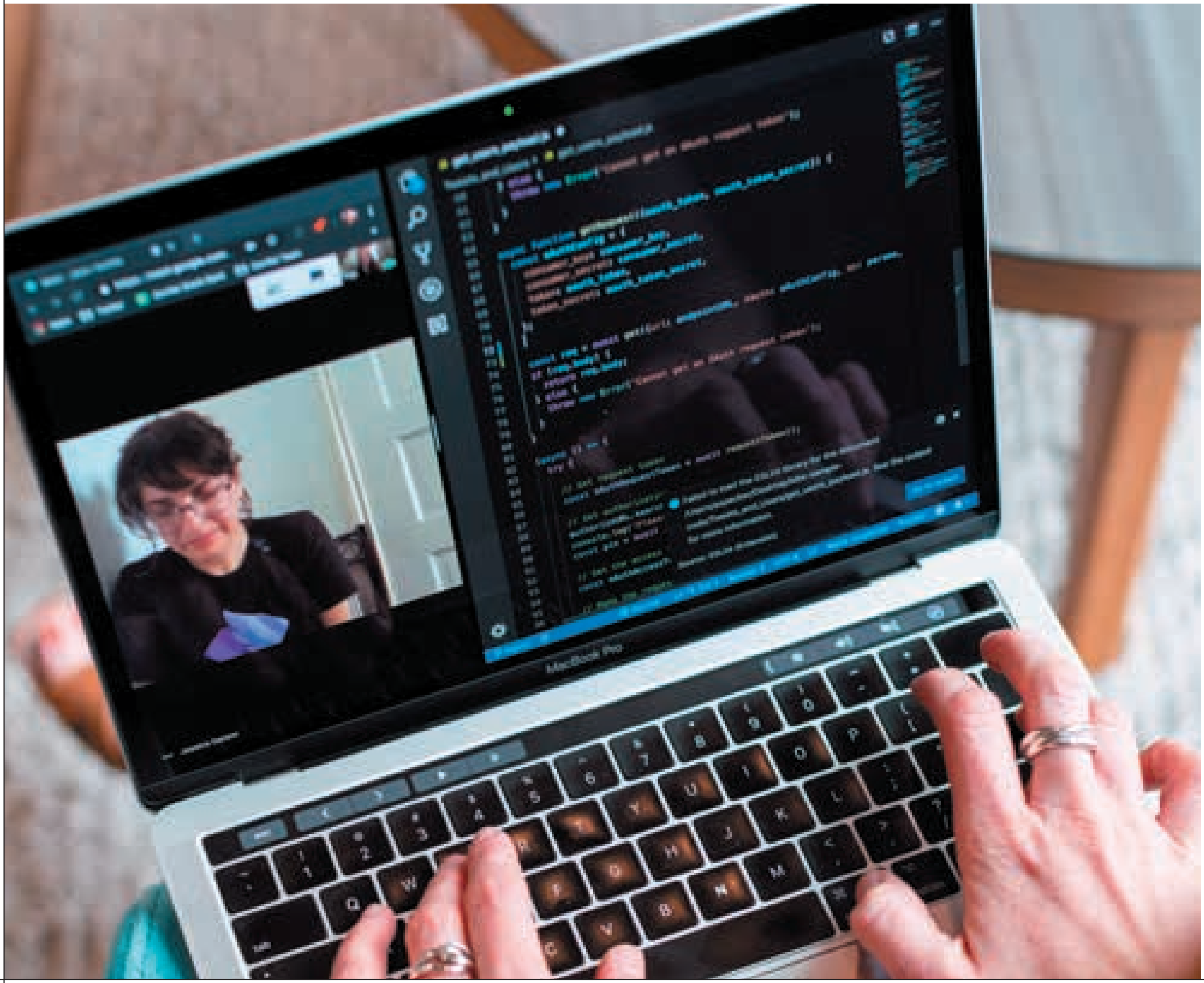
GDPR is as relevant in 2021 as ever, and as we head into a data-driven future, it's vital organisations stay updated with the latest policies. The cost of not complying is starker than ever. That's partly because fines are so high. Whatever period of grace authorities gave when GDPR first came into force is now gone – in 2021, there is no excuse not to be compliant. If you're not, you risk a hefty financial penalty.

But the financial damage of a fine could pale in comparison to reputational damage. The public has never been more tuned into issues of the usage and mishandling of data. The collective consciousness has an innate suspicion of businesses using their data in nefarious ways. Being seen to not comply with GDPR could confirm their worst fears and make them hesitant to do with business with a company.

But I don't want to end this piece on such a negative note. While the motivation behind compliance is partly fear, I feel businesses are increasingly seeing GDPR as an opportunity. It's certainly true in the conversations with people I've been having. The questions customers ask me today are light years away from what I was being asked in 2018 as their data maturity has moved on. In my experience, businesses want to comply. They want to earn the trust of their customers. And importantly, they want to have healthy, clean data that's going to add real value to the business. This is the attitude we should all adopt. Particularly as that second recession looms on the horizon and the quality of our data is put in the spotlight.

Now isn't the time to do the bare minimum to simply avoid fines. Instead, businesses need to rethink how they gather, store and draw insights from data. They should be securing their infrastructure, shifting their work culture, putting in place new processes and ensuring they are working with established, credible data suppliers who are fully compliant. But most importantly, they need to ensure they are fully leveraging their data and are unlocking its true potential. And that can only happen by putting in place a robust, GDPR-compliant foundation on which to build ●

Nicola Howell, Compliance & Privacy Attorney, leads Dun & Bradstreet's European privacy team which provides oversight and guidance on privacy issues to help ensure businesses are in compliance with privacy and data protection legislation.

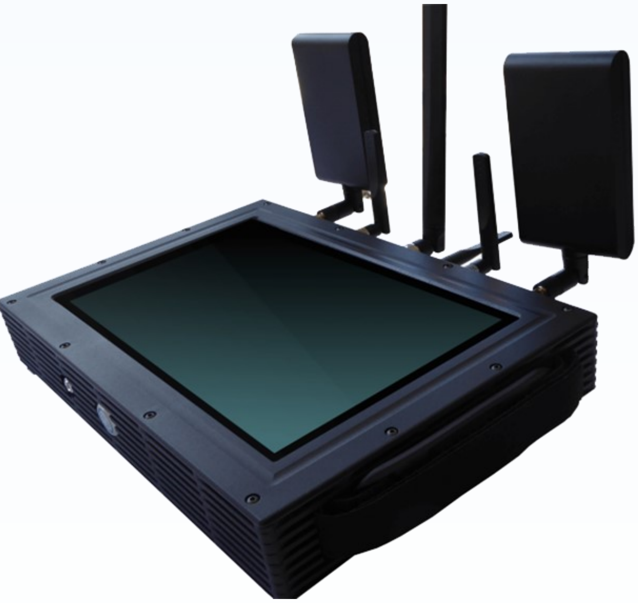


Organisations need to update their policies to cover the issues caused by working from home

GLOBAL QCC T.S.C.M

Sentinel

A TSCM BREAKTHROUGH



QCC Sentinel is the most advanced TSCM portable system for the detection & location of Wi-Fi 2.4GHz - 5GHz Devices & APs. Also with detection & location of all Bluetooth devices with full direction-finding. Software for TSCM & Tactical use.

Detect, analyse and locate all Wi-Fi & Bluetooth threats. (Discoverable, Hidden, Connected & Unconnected)

Designed for TSCM Engineers by TSCM Engineers.

FEATURES

- Display relationship between AP & device
- Packet Count & Activity Meter
- Identifies Wi-Fi Store & Forward devices
- Fully Flexible Display Parameters
- Create Wi-Fi / Bluetooth target lists
- Mission Correlation for Intel operations
- Comms with Wi-Fi devices to aid location
- Offline desktop app supplied
- Force disconnect of Wi-Fi enabled devices
- Ethernet for remote operation/reporting
- Windows/Mac OS Software
- Capacitive touch screen control

SENTINEL KIT INCLUDES

Omni & directional antennas, removable 98Wh battery, external power supply all in a rugged carry case. Optional extras include a 3G / 4G modem module (excluding SIM card).

For further details: contact@qccglobal.com

"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*

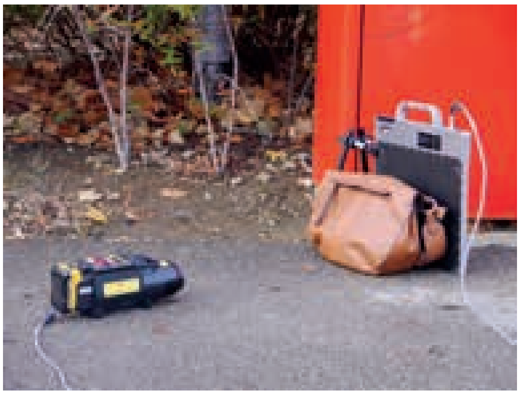
MGT Europe www.mgteurope.com

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

MOVING FORWARD

Simon Hall *reports on the dawning of a new era in frontline police technology*

Picture credit: Crown Copyright

In the past few years, the approaches to delivering front line software have changed with blistering speed. Systems that were state of the art just two to three years ago now lack the required flexibility moving forward. The demands arising from COVID-19 and Brexit have only accelerated the pace, with forces needing high agility to meet rapidly changing requirements. Policing is now much better prepared to adapt and deploy new technology when the time calls for it. But this more agile approach did not happen overnight; a number of factors converged to reach this tipping point.

We now have a new generation of officers and new cloud-based services to help them. The traditional but inflexible technology investments of the past are giving way to a new breed of cloud-first, Software-as-a-Service (SaaS) solutions that can deliver change at a significantly greater pace and at lower cost while giving forces more control over their own destiny.

While this transition was already in motion prior to the pandemic, it was undoubtedly accelerated by COVID-19. The switch to virtual meetings over Microsoft Teams almost overnight is a good example of this. Such an achievement would have been almost impossible if it wasn't for the adoption of cloud technology by Forces beforehand, led by the National Enabling Programmes (NEP).

Frontline officers are also benefitting indirectly from the consumer technology revolution of the last few decades, with devices and services that can support advanced innovations such as artificial intelligence, augmented reality and natural language processing.

This new combination of cloud-based services with cutting-edge devices brings new found freedoms to our forces. The question now is, how do they harness these freedoms without creating new problems and bottlenecks that will slow down the pace of change, or inadvertently repeat the mistakes of the past by swapping the 'Big Consultancy' of yesteryear with the 'Big Tech Company' of today?

Technology has become a bit of a sore point for officers, with some citing it as a contributing factor to early retirement. To quote directly from Andy Rhodes, Lancashire's chief constable at the 2021 UK Police Digital Summit, one officer told him: "I'm actually leaving the police earlier than I should have been doing because of the technology. I can't cope with it. It's not me doing my job, doing the thing I know."

Senior Officers and Ministers have been aware of these issue for some time and have put a strategy and initiatives in place to address them. The Policing Vision 2025 and the National Digital Policing Strategy 2020-2030 both recognise the need for greater interoperability between police and other related systems, uniform data standards and better data quality, for example. This new era is being led from the top and needs to filter down through the policing organisations and hopefully into procurement too, so that more innovative and agile SMEs can play a greater part in delivering this vision.

The success of the National Enabling Programmes (NEP) has demonstrated how the cloud can deliver meaningful business change to forces in a short timeframe and with minimal disruption. This lesson is also being applied to other projects run by the Home Office, most notably with the recent announcement of the evolution of the Police ICT Company into Police Digital Services (PoDS).

> THE SAAS-FIRST APPROACH WILL ALLOW FORCES TO DEVELOP AND INTEGRATE THEIR OWN PROCESSES

The Police ICT Company – along with the success of the NEP – has played a significant role in shifting the mindset of policing around technology in advance of its vision of: "Supporting UK policing to keep people safe, get more from technology investments and make better use of public money". Police Digital Services, which has been up and running since April this year, and will replace the Police ICT Company, will pick up the mantle with a bigger budget and more resources. With a focus on delivering outcomes rather than specific technologies, Police Digital Services has a broad range of objectives; these range from providing a seamless experience for citizens when they engage with the police, to the digital enablement of officers and staff through digital while empowering the private sector to play a key role in the delivery of innovative and cost-effective solutions. Police Digital Services has an important role to play in maintaining the current momentum towards more SaaS-first, cloud-based technology deployments across police forces in the UK.

One of the key sessions from the recent Police Digital Summit was delivered and demonstrated by Philip Bartholomew, Digital Transformation Programme Manager, Essex Police. He showcased a solution that was developed using an in-house team, using Microsoft Power

Solutions must be fit for purpose and flexible enough to meet likely future requirements

Apps and the Power Platform to provide a quick solution to an immediate need within the forces around COVID-19 3E/4E frontline processes.

Using the platform, they produced a 'minimum viable product' for frontline officers in six weeks, having been quoted six months from one of their existing providers. This approach also achieved an estimated saving of £20K-£50K.

Mark Gilmartin, Director of Support Services, Essex & Kent Police, commented: "The ability to take a requirement from the operational leadership and convert it into an application that can be deployed effectively, so quickly. That level of agility and responsiveness is the big, big plus for this particular initiative."

This is a great example of the future direction of frontline policing – it is no longer about the 'Big Consultancy, Big Project' approach of the past, but instead it is about adaptable SaaS platforms that align with the NEP blueprint.

The SaaS-first approach will allow forces to develop and integrate their own processes if they wish, using 'no-code/low-code' solutions, share their process designs with other forces at no or low cost and take advantage of scalable integration platforms to overcome the logjam of proprietary legacy integrations.

The challenge with the 'build-your-own-apps' approach is that forces have a significant number of processes that they would like to digitise; "upwards of 1,000 processes between Kent and Essex" was mentioned at the Summit. While many of these could be replaced with other solutions like RPA ('Robotic Process Automation', a form of business process automation) this would still leave many that will need to be carried out by frontline officers.

COMMON USER INTERFACE

This approach would require hundreds of Power Apps, each with their own user interface and limited ability to share data, which would be far from ideal. We are advocates of Forces using tools such as Power Apps to build their own solutions and reduce their reliance on 'Big Consultancy', but they should be mindful of important factors like interoperability, data quality and security – and the user experience – when doing so. It is important to adopt a common user interface to reduce the training burden on officers, use common data standards to ensure data is applicable and sharable across different processes and enforce good data quality by minimising the amount of manual input and rekeying of data wherever possible.

It is certainly good that the Microsoft Power Platform has demonstrated the agility of cloud-based solutions in response to urgent needs and made a strong case for more cloud/SaaS solutions within policing. However,

▶

general purpose 'citizen developer' platforms may not be a panacea for the particular requirements of operational policing, specifically when it comes to data security, sharing, re-use and interoperability. Two summit sessions showcased two different uses of Power Apps, each having different user interfaces and no built-in support for data security or sharing. Maintaining consistency across many processes, perhaps authored by different forces, introduces new challenges.

Rhys Willis, Business Change Consultant at the National Enabling Programmes, commented: "People should view Power Apps as low code, quick and dirty solutions to challenging business-critical issues. The NEP COVID app is a great example of this. They can be used to replace basic paper processes that forces have produced around Taser use, training *etc*."

The point is that Forces need to transform all frontline processes – including their existing mobile policing solutions, which connect to critical police services such as RMS, Command and Control, Intelligence, PNC, NLEDS, HO Biometrics *etc*. Modern frontline apps should be sufficiently agile to handle urgent new requirements, without going back to vendors for often costly custom development.

A two-track route (new low-code solutions like Power Apps alongside the established first-generation police solutions) also increases the financial cost and training requirements. When it comes to mobile solutions for the frontline specifically, an alternative approach is to adopt a fresh generation of police-specific frontline applications, which address the specialist needs of policing, and which also adopt the agile no-code/low code approach of modern platforms.

While Power Apps are a great solution to allow Forces to streamline many of their business-critical processes themselves, they do not necessarily allow forces to build exactly what they need for frontline policing. Frontline operation has many niche requirements, for example the need to be able to work offline for long periods, re-use data between processes without re-keying, use on-device integration to biometric scanners, ANPR and the like, plus the ability to capture information from identity documents such as driving licenses and passports – while also ensuring appropriate levels of data security. Such functionality, if built in at the start by virtue of using a SaaS-based platform, would be applied automatically to any new process without the need for complex development work – ie, adding new processes becomes easy, seamless and quick.

INFORMATION REQUIREMENTS

As a final word, it is worth remembering that the 'I' is as important as the 'T' when it comes to Information Technology. There can be a tendency to rush to adopt 'shiny' tech without full consideration of the actual data or information requirements. Solutions must be fit for purpose – not just to meet the immediate requirement, but also to be flexible enough to meet likely future requirements. Forces' cloud journeys are building out the strategic architectures to make this possible.

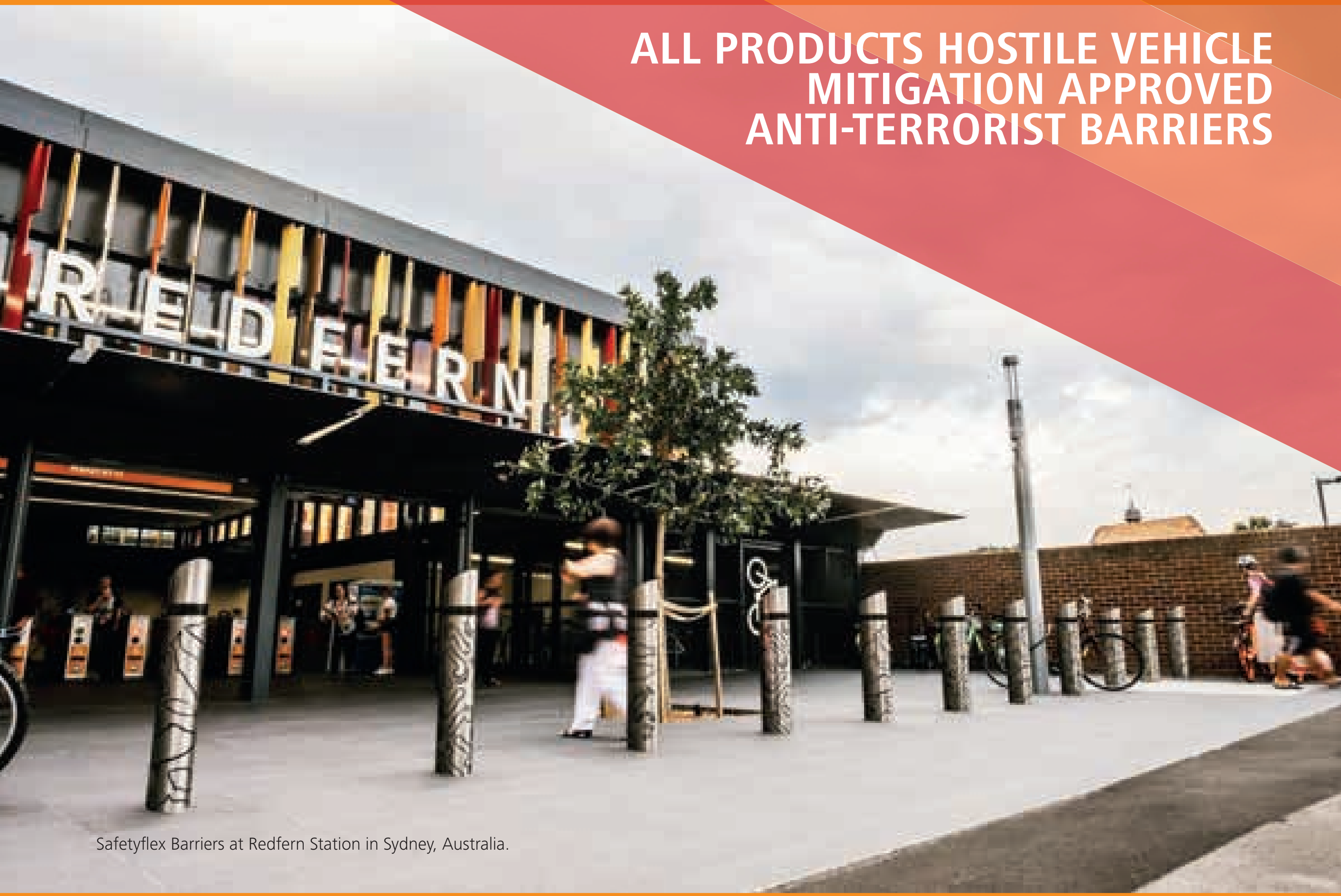
The next step is to adopt appropriate next-generation applications that can bring the long-awaited benefits the cloud – and SaaS – promises. Digitisation of processes is not just about the data either, it is about reducing workloads on officers, even when offline, improving data quality, automating data capture and re-using data, eliminating duplication of effort, as well as meeting all of the requirements of integrity, security and governance. For next-generation apps, these capabilities should come 'out of the box'. All of this should be realised in a way which facilitates interoperability, even in the absence of universal data standards and eliminate the age-old problem of data silos and data sharing.

We are truly heading into an exciting new era of policing where instead of seeking early retirement to get away from it, our officers will be inspired by the capabilities of the technology that is available to them ●

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

Digitisation of processes should not just about gathering data, it needs to focus on reducing officers' workloads

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

CULTURAL SHIFT

Helen Dudfield *explains the growing need to build a defence from a solid foundation of training*

The democratisation of technology has made it possible for society to navigate seismic shocks like those seen by the pandemic, but for those in defence, it presents new challenges in the form of the rise of asymmetric – or grey zone – warfare. This battleground is one in which the weapons of warfare are not the conventional rifle or tank, but rather commercial-off-the-shelf (COTS) computers, which give bad actors the ability to inflict considerable economic and physical damage on their targets, as shown by the £50-million losses caused by the drone disruption at Gatwick airport in 2019. Nowadays, potential enemies are increasingly harder to identify as those with access to a computer or an off-the-shelf drone are capable of causing as significant harm as conventional weaponry, while at the same time not provoking a conventional response or being recognised as a formal act of aggression.

The weaponisation of everyday technologies is blurring the lines between the skills applied and tools used by those within and outside the military, with acts often combining both. The lack of distinction between what is a military skill and what is not, presents a major challenge to the defence sector.

> BEING AN EARLY ADOPTER OF DISRUPTIVE FORMS OF TECHNOLOGY PUTS THE UK AHEAD OF ADVERSARIES

Introducing those with relevant skills and knowledge firstly requires a change in the recruitment process. Approaching those who fit the traditional military hire is no longer enough to address the growing forms of attack. The net must now be cast further, in order to court the digitally native generation who may not have seen the defence sector as the natural home for their skillset. Secondly, recruiters must illustrate to potential talent why a job in the defence sector is a worthwhile career choice, as they will be competing directly with the strength of the private sector, the promise of tech start-ups and the huge salaries on offer within the banking sector.

However, the tech talent pool in the UK may not be ready to service the demand. Research from recruitment firm Robert Walters Group found that the pandemic has put pressure on demands, with 58 percent of hiring managers putting information security as their most required skill, while only 10 percent of IT professionals have the skills needed to fulfil the roles.

With a small talent pool, focus must also be put on a second approach: targeted investment into reskilling current personnel so that they are capable of countering the new threats being posed. This calls for a shift in focus.

CONTINUOUSLY ADAPTING

The linear process of 'train – deploy – return – train again' no longer matches the constant nature of grey zone campaigns or the unpredictability of their impact. Training should be a constant process – not a set piece of timed activity. Defence and security forces need to continuously adapt to changes in the environment and incorporate new skills into the way they operate. This is particularly important when force numbers are reduced but strategic effect needs to be maintained.

Secondly, the spread of learning and development tools needs to widen to make the most of novel technologies including mixed reality, AI and robotics. This is increasingly necessary as defence and security forces will be training across multiple generations and incoming personnel are likely to be more comfortable with new digital ways of learning. It also enables a shift from basic 'muscle memory' training to more cognitive training, which in turn helps individuals to shift more easily between traditional fighting skills to those required for effective protection, deterrence, assurance and civil support.

Finally, training should be more collaborative. Regular training with allies reinforces the message of how powerful integrated responses can be, and provides a visible deterrent for adversaries no matter what novel tactics they may be exploring for grey zone conflict.

Experimentation has become more prevalent in recent years, spurred by the success of the rapid prototyping and innovation cultures championed by Silicon Valley: fail fast, learn and improve. The value of experimentation in defence has already been realised in several interdisciplinary multi-national exercises, such as the Unmanned Warrior exercise, which provided a testing ground for unmanned systems and Formidable Shield which tested eight NATO countries' defence capabilities versus ballistic missiles. These accelerate the development and integration of technologies and operating concepts by allowing them to be tested in a controlled, safe environment.

Applying this capability to the grey zone could take the form of incorporating penetration testing and Red

Picture credit: Crown Copyright

Training using virtual reality is cost-effective, and boosts learning and retention rates

Teaming to ensure defenders are prepared. Penetration tests actively attempt to practically exploit vulnerabilities and exposures in an organisation's infrastructure, applications, people and processes. Red Teaming on the other hand is scenario based and a goal driven test, with the ultimate aim of emulating the real-world adversaries and attackers who are trying to break into a particular system or steal information.

The use of virtual and constructive simulations allows personnel to train with scarce or high value assets and means that live training capabilities can be adapted to meet evolving operational needs. A technology-agnostic approach should be taken throughout; integrating training systems, simulators and equipment supplied by different manufacturers to build the most effective synthetic representation possible. Training using virtual reality is cost-effective, and boosts learning and retention rates. 'Rehearsing' operations in a realistic environment leads to increased operational efficiency and production, and cuts downtime required to carry out maintenance.

While an intention to improve training is important, with the issue of grey zone, forces will need the science and technology being used by the enemy to hone their skills on. Traditionally slow to take on new forms of technology, the West needs to do more to accelerate the adoption of technologies and ensure that forces have the necessary equipment to train and develop capabilities to combat grey zone attacks.

To achieve this, a path needs to be cleared for the accelerated transfer of civil sector technology into military and security use to improve its effective response to attacks that also stem from the civil sector. For the UK, being an early adopter of disruptive forms of technology will go some way to putting it ahead of adversaries and giving it a leading role in this area among its allies.

However, to successfully integrate technologies from the civil sector calls for further collaboration with those in the industry. Defence and security forces have first-hand understanding of their operational challenges, while academia and industry are continuously exploring potential solutions; close communication and collaboration between all parties is essential to ensure development and innovation

▶

remains mission focused. And this all falls back into the need for a modernised training programme, both in terms of techniques and tools which are used. Training partnerships with industry and allies will be able to deliver the needed tactical training to combat realistic threats while forging closer cross-government, inter-Service and international integration.

RECRUITERS MUST SHOW POTENTIAL TALENT WHY A JOB IN THE DEFENCE SECTOR IS A GOOD CHOICE

The primary obstacle to increased collaboration is the tendency of defence enterprises to be extremely protective of their intellectual property, and open collaboration can feel at odds with the need to maintain the necessary competitive advantage. Collaborative training spaces can be configured in ways that meet these confidentiality requirements, by sharing key outputs without giving away knowhow. Data would remain the property of the various partners, overseen by an independent curator that understands and mines the data to produce a coherent picture.

Defence enterprises must work together to agree common standards and principles on the use of collaborative environments, threads and twins. Only once this is understood, and a collaborative culture is embraced, can the timesaving, cost-saving and performance-enhancing benefits of collaborative training be realised.

The accelerating transfer of consumer technology from lab to user continues to lower the bar for entry and we are likely to see an increased number of those with the capabilities and technology to deploy commercial, consumer technologies to great effect within the defensive sphere. With such undefined battle grounds, there is really no limit to the potential growth the grey zone could enjoy. What's more, it's becoming increasingly clear that we are set to see both state and non-state actors become willing to operate within it in order to achieve whatever their aims may be.

The British Forces have already begun their immediate response to the new form of battle, as Royal Marine commandos begin to be deployed on covert missions overseas with the specific task of operating in the space between peace and war to disrupt enemy activity. Nevertheless, a further cultural shift is needed, and can be achieved through putting in the framework that ensures employees are prepared for grey zone threats.

While in the short-term, tactical recruitment will go some way to helping, in the long-term the necessary capabilities can only be delivered through a focussed and modernised training programme, which provides further credence to the Government's Integrated Review and Defence Command White Paper. The structure emphasises the importance of science and technology to the strength of defence going forward. A cross-industry collaboration will ensure the UK's forces can explore, experiment, evaluate and exploit new technologies, techniques and tactics vital to future operational advantage, security and prosperity ●

Helen Dudfield is Chief Scientist for Training and Human Performance at QinetiQ. Over the course of her 20-year career with the company, Helen has played an essential role in the Simulation and Training department, currently acting as a Senior Fellow and Chief Scientist for Training and Human Performance and Senior Fellow. Helen is also a RAEng Visiting Professor at Nottingham Trent University.

Critical training should take place during deployment to shorten the timeframe for achieving maximum strategic effect

Picture credit: US Dept Defense

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?

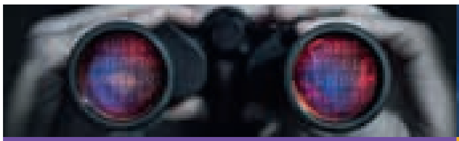
We don't just make and sell TSCM equipment, we use it & understand it.

QCC solutions include:

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

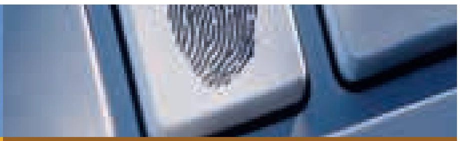
TSCM equipment from all leading manufacturers, to cover all threats with training.

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 !

Picture credit: AXIS Communications

MINIMISING RISK

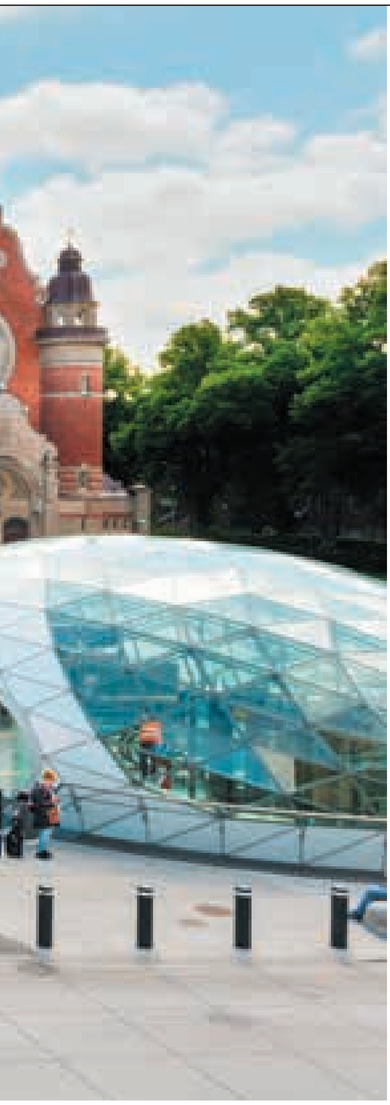
Andrea Sorri *reports on the importance of tackling cybersecurity risks in smart cities*

Many organisations around the globe have security cameras installed to increase safety, security and often also efficiency of processes. From schools to hospitals to businesses and more, surveillance cameras are monitoring people, buildings, and public spaces. Unfortunately, network-connected surveillance cameras have become the focus for attack by extremely organised, technically proficient and well-resourced cyber criminals. The consequences of an attack are potentially devastating.

If cyber criminals gained access to the live video footage of hundreds of thousands of security cameras, it would effectively allow the attackers to spy on the affected organisations and the people within them. It would leave people at the establishments feeling worried about their safety and the privacy of their data, and the organisations themselves concerned about potential corporate espionage. These kinds of cyberattacks aren't created in the imagination of a Hollywood movie or novelist, they're happening today and aren't isolated cases.

Whether looking to cause disruption or extract a ransom, cyberattacks are growing in numbers and in sophistication and smart city infrastructure has become a popular target. A key reason is that the unique set-up of a smart city provides numerous potential entry points – the success of these types of cities relies on an increasingly interconnected network of Internet of Things (IoT) devices such as connected sensors, lights, surveillance cameras and meters to collect, share and analyse data.

The data from these is being used to optimise and streamline services, infrastructure, public utilities and other operations. While the common rule is, the more



Different stakeholders in a smart city should ideally join forces so that the security chain is as strong as possible

connected IoT devices providing their data, the better the outcome, it also means more network entry points that need securing. And with the growth in smart cities comes an associated growth in risk.

It is reported that governments have been investing £124-billion over the past year in smart city initiatives globally and according to the GSMA, an industry organisation that represents the interests of mobile network operators across the world, the number of IoT devices is expected to grow to £18.1-billion by 2025. Ensuring that all these touchpoints of the network in a smart city are cybersecure is a challenge and requires an advanced cybersecurity strategy – on both a physical and electronic level.

THE RIGHT MIX

The reason why the 'attack surface' of a smart city's infrastructure is increasing almost exponentially, as more IoT devices are being added to the network and more separate systems become integrated, doesn't lie in the transformation per se. It comes through a mixture of outdated technologies, poor control and maintenance of connected devices and a lack of a digital transformation and security strategies.

It's crucial for municipal authorities and operators to adjust to the new networked urban landscape and set the right priorities. The scenario described earlier, and which reflects aspects of real cases, gives an insight into the risks that a successful cybersecurity breach can pose to a smart city, particularly when targeting critical infrastructure. While the implications clearly depend on the size and circumstances of the attack, the consequences in a smart city would be chaos in the 'best' case scenario and disruption or even loss of life in the worst.

An example for one of these large-scale impacts (aka worst-case scenarios) that posed a genuine security risk for the city and its residents, was a ransomware attack on the majority of police surveillance cameras in Washington DC. The devices had to be rebooted to function again, leaving the system offline for four days. The police had been using the surveillance system to ensure public safety and security, for example in rapid response to incidents and by investigating criminal cases with material evidence from the video footage. The implications of these systems being rendered inoperable was potentially disastrous.

There is also the aspect of reputational damage and fines. If a city's surveillance system was attacked, the chances that people trust these solutions again are decreased. Plus, regulations like the General Data Protection Regulation (GDPR) make the protection of data a legal requirement, which can result in fines if the terms aren't met and unauthorised third-parties are allowed access to personally identifiable information (PII).

The key principles that smart city authorities need to apply to avoid situations like the above and to achieve a successful security approach are consistent for both physical security systems and cybersecurity: the identification and classification of a smart city's assets and resources and understanding what needs protection; the identification of plausible threats and vulnerabilities that these threats may exploit; and an analysis of the consequences/risks of such an attack.

Protecting cities from cyberattacks has two levels: on the one side it's essential to ensure as many IoT devices and potential entry points that are connected in a smart city's network are as secure as possible. This aspect of is a shared responsibility between all stakeholders: users, organisations, manufacturers and integrators.

But we shouldn't just think about cybercriminals as acting remotely - often they are aided by those with physical access. Physical security systems therefore play an important role. Video surveillance and access control solutions help to keep crucial physical assets, facilities and control rooms secure from intruders (and even disgruntled employees) who could use physical access as a route to infiltrate the network.

As sophisticated as cyber criminals are nowadays, the IT experts responsible for cybersecurity haven't been sitting around twiddling their thumbs. The cybersecurity measures are being improved on a constant basis. It is often still necessary or advantageous for the attackers to find a physical touchpoint to the network. Data centres and important control rooms are attractive targets as once infiltrated, criminals can potentially move through the network to disrupt critical infrastructure and processes within a smart city. Thus, deploying a layered protection at these locations is key.

> CYBERATTACKS ARE GROWING, AND SMART CITY INFRASTRUCTURE IS A POPULAR TARGET

Hence, physical security – eg in the shape of video surveillance – can be the solution to protect these assets and shield the network from a cyberattack by preventing unauthorised people from accessing the facilities.

This starts with perimeter protection, for example, with the help of radar and audio speakers. Once an alert is triggered, they can play live or pre-recorded messages to deter an intruder. Access control solutions that combine video verification with access credentials through mobile phones or cards can be set up to only grant selected and authorised individuals access to the respective buildings.

Within the critical rooms – for instance the server room in a control centre – installing high-resolution cameras programmed to automatically pan and zoom when specific server cabinet doors are unlocked or opened can help to prevent the implanting of malware or spyware, which would effectively give cybercriminals access and control over the system.

While physical security of key data management points plays an important role, it's even more essential to ensure that these physical devices and touchpoints themselves are as cybersecure as possible across the whole supply chain, particularly as many IoT devices often have no built-in security. That requires understanding the vulnerabilities of a network; if operators aren't aware of potential cyber vulnerabilities, threats and issues, the prevention of these threats becomes challenging (if not impossible).

In previous cases, the attackers have gained access to the system after finding the password for one of the administrator's system accounts, which was, for instance, accessible on an internal service that had become exposed to the internet. It's an example of the human error creating a cybersecurity risk and it's only one of several aspects that can create a vulnerability for an interconnected system. Often the vulnerable links are created through poor 'cyber hygiene' of the network, which can roughly be separated in three main factors:

A lack of alignment between security and IT: if the teams have different understandings of the security protocols or processes, the risk of breaches increases.

IT IS STILL NECESSARY FOR CYBER ATTACKERS TO FIND A PHYSICAL TOUCHPOINT TO THE NETWORK

Failing to put in place and follow IT security policies: many cybersecurity issues have their origin in lapses in security protocols or human errors. These can arise if operators in smart cities haven't clearly defined the requirements to secure the IoT devices and the network or if network users aren't following the procedures that are in place.

Having no device lifecycle management and proactive maintenance in place: systems that are not well maintained, updated and cared for provide a higher risk of becoming the target of a cyberattack. Thus, installing updates when they're released and staying informed about security controls for services and devices is key. In a city with thousands of connected devices, such as air sensors, street lights or cameras, it's critical that these upgrades can be performed in bulk, rather than manually.

The solution is to find the optimal way of merging the best practices of both the physical security world with the best practices of a traditional IT domain without introducing new cybersecurity vulnerabilities for other components in the converged system. A converged security approach breaks down silos and empowers different teams to collaborate towards a common goal. Cybersecurity is a shared responsibility, meaning the different stakeholders in a smart city should ideally join forces so that the security chain is as strong as possible.

Integrators, installers and distributors need to be transparent about the origin of the equipment and make sure the installed devices are patched with the most recent updates. Device manufacturers are responsible for hard coded passwords and that the devices don't have a backdoor, which allows hackers to enter the system easily. Plus, they should be informing partners and channels if a vulnerability is detected. This information usually comes from the researchers, who typically inform the manufacturer and give them a chance to fix the issue before making it public (unless it's a critical vulnerability).

It's not only the number of smart cities and cyberattacks that's growing, it's also the level of sophistication on both sides. Smart cities will incorporate increasingly advanced technologies and criminals will upgrade their approaches accordingly.

Therefore, it's cities and operators that have to think about appropriate steps now, ensuring that a foundation for cybersecurity is created that can keep IoT devices and network end points secure and withstand the future.

The task is never completed, and it is crucial to understand that cybersecurity is all about hard work and diligence every day. Comprehending and detecting potential threats is the basis and working with an ecosystem of partners that work closely together (and towards the same goal) is critical ●

Andrea Sorri, Segment Development Manager Smart Cities EMEA at Axis Communications, is a 20-year veteran in the company and has created and implemented the Smart Cites strategy for Axis. He has held various positions such as Global Business Development Director, Regional Training and Engineering Manager and Country Manager.

Video surveillance solutions help to keep crucial physical assets secure from intruders looking to infiltrate the network

Picture credit: AXIS Communications

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

1 May, multiple locations – UK

Counter terror police arrested five people – including a 16-year-old – as part of an investigation into right-wing terrorism. All suspects were taken to West Yorkshire for questioning.

1 May, Berlin – Germany

As many as 93 police officers were injured as 354 protesters were detained after traditional May Day rallies in the capital turned violent, resulting in police being pelted with bottles and rocks.

3 May, Istanbul – Turkey

Turkish police captured a man codenamed Basim – the alleged military head of Isis and a close aide to the terrorist group's former leader. Travelling under a fake passport, the man was thought to have disappeared when the group was driven out of Syria in 2017.

5 May, Berlin – Germany

The German Government announced it is banning Islamic organisation Ansaar International for financing terrorism around the world and police raided affiliates of the group.

11 May, Kazan – Russia

Seven students and two school employees were killed and 20 wounded when a 19-year-old went on a mass shooting spree. The shooter is now in custody.

14 May, Ireland – UK

Ireland's Health Service Executive was forced to temporarily shut down its IT system to protect it after suffering a "significant ransomware attack".

Americas

1 May Portland – USA

May Day protests quickly turned into riots when around 100 people engaged in "autonomous demonstrations" near an ICE facility, forcing police to make six arrests – including one individual who was threatening police with a knife.

3 May, Bogota – Columbia

16 demonstrators and a police officer were killed and hundreds injured following a weekend of protests about an unpopular tax reform. Police were criticised for the way they fired on protesters and rammed crowds with motorbikes.

3 May, Langley – USA

Shots were fired when an intruder attempted to drive into the CIA's headquarters and was stopped by armed guards at the gates.

3 May, Salton City – USA

Border Patrol agents arrested a woman attempting to smuggle 42 packages of methamphetamine through an immigration checkpoint in California after investigation of her car.

4 May, Northern Michigan – USA

A man hijacked a bus and inadvertently crashed it into a woman's car. The man was arrested and the woman treated for minor injuries. No one else was hurt in the incident.

6 May, Rio de Janeiro – Brazil

At least 25 people were killed after heavily armed police stormed one of the country's largest favelas in pursuit of drug traffickers in what is being described as the deadliest raid in the city's history.

Asia

1 May Ghazni – Afghanistan

Taliban insurgents attacked and overran a key army base in the south-eastern province, capturing several soldiers. On the same day that the US and NATO partners formally began their withdrawal from the country.

1 May, Baghdad – Afghanistan

A series of separate attacks across Baghdad resulted in the death of 18 Iraqi military personnel. The armed attacks targeted army convoys and is thought to be the work of Isis.

3 May, Logar province – Afghanistan

A bomb exploded near a school in western Afghanistan wounding 21 people – most of them young students. No one claimed responsibility, but Taliban insurgents have a presence in the area.

3 May, Western Bago – Myanmar

A parcel bomb killed five people including an ousted lawmaker and three police officers who had joined a civil disobedience movement opposing military rule.

5 May, Krong Pinang district – Thailand

Two insurgents and a ranger were killed following a firefight between a government security force and armed militants.

5 May, Kirkuk – Iraq

Islamic State fighters killed a policeman and injured another before blowing up two oil wells in the country's northern province.

6 May, Male – Maldives

Mohamed Nasheed, the first democratically elected president of the country, was injured after an IED on a motorbike was detonated near him as he got into his car

9 May, Zabul – Afghanistan

At least 11 people were killed and dozens injured when a bus was bombed in the southern province. The attack came as the Taliban declared a three-day ceasefire to mark the Eid al-Fitr holiday.

10 May, Dunedin – New Zealand

Four people were injured, three critically, after a stabbing attack at a supermarket. Police arrested the suspect and took them into custody.

Africa

May, South Africa

Virgin Active became the target of a sophisticated cyber attack, forcing the health and fitness company to switch all of its IT systems offline.

1 May Sarh – Chad

Four people were shot and wounded in the country's southern Mandoul region when security forces fired on a crowd demonstrating against the military's takeover of the country.

2 May, Ajiri – Nigeria

Eight people were killed in an attack by Boko Haram when militants attacked a military base in Borno state.

2 May, Pietermaritzburg – South Africa

A police truck ferrying 45 prisoners from magistrate court to prison was hijacked by five armed men looking for a prisoner involved in a murder case. The men didn't find the suspect and no one was hurt.

4 May, Ajiri – Nigeria

For the second time in two days Boko Haram attacked a military base, this time killing 12 people including soldiers and civilians.

9 May, Kano – Nigeria

Nigerian troops arrested 13 suspected Boko Haram militants in the north-west state, the army revealed.

9 May, Mogadishu – Somalia

Six people (including two senior police officers) were killed and six others wounded when a suicide bomber blew himself up in a police station in the capital's Waberi district.

10 May, Filin Lazio – Nigeria

The Nigerian army arrested 13 suspected Boko Haram members in Kano State following an operation by troops to flush out criminals.

11 May, Maiduguri – Nigeria

Nigerian troops repelled an incursion by Boko Haram militants as Muslim residents observing Ramadan were about to break their fast. Five insurgents were killed.

NEWS

Europe

EU passes new online terrorist content law

The European Parliament's Home Affairs Committee has agreed a new EU regulation to prevent the dissemination of terrorist content online. The regulation allows the authorities in any of the 27 EU countries to have content removed, even if hosted by a third-party member, within one hour without requiring a court order. The removal orders must come from the "competent authority" of each EU country and can be addressed to all 27 members of the EU. The law comes into force 20 days after it is published in the EU Official Journal. Companies can face fines up to 4 percent of their global turnover for non-compliance. They have said they shared regulators' efforts to tackle the issue and keep the content off their platforms. The law was first proposed in 2018 after the EU became increasingly concerned about the role of terrorist content after a series of attacks by self-radicalised lone-wolf attackers in several European cities.

France's tighter security measures for released terrorists

French Interior Minister Gérald Darmanin has called for stringent security measures to be placed on convicted terrorists after they're released from prison. If the new measures are passed into law, a released terrorist could have their movement limited, including where they can live or what public events they could attend. Under the proposed changes, released terrorists will face a period of strict supervision for several years beyond the original sentence. The measures, which are part of a broader counter-terrorism bill, would enhance surveillance and data collection methods by authorities in France as a whole. Authorities would be able to use advanced data collection algorithms and artificial intelligence to attempt to predict attacks before they happen. It would also allow for monitoring of extremist websites online. France now joins the UK in calling for enhanced security supervision for those coming out of its prison system. The UK is ending early release for convicted terrorists and now requires them to serve at least two-thirds of their sentences, instead of half as well as curbing overseas travel and requiring released terrorists to wear GPS ankle bracelets and submit all their electronic devices for monitoring.

UK Cyber Security Association opens membership

The UK Cyber Security Association has officially launched and is open for membership, it has been announced. The body is designed to provide a community for anyone working in – or with an interest in – the sector, helping promote best practices and information sharing in the UK and internationally. It also aims to work alongside government, trade bodies and cybersecurity groups to share information and initiatives. Membership has now opened for individuals and organisations actively working in the industry. Those who join will be given access to an online portal and forum to engage with other members and the chance to participate in a programme of events and training sessions, among other benefits. First started in 2019 by industry expert Lisa Ventura, the UK Cyber Security Association has been in an expressions of interests phase until now. So far, it has undertaken project work and campaigns in areas such as growing neurodiversity and women in cybersecurity, addressing the cyber-skills gap and helping individuals and small businesses stay secure online during the global pandemic.

Germany sees significant rise in far-right crime

Germany's Interior Minister Horst Seehofer has revealed that the country experienced a significant jump in politically motivated crimes, while offences committed by far-right supporters hit a record high in 2020. Far-right offences are understood to have increased by nearly 6 percent from the previous year at 23,064, and accounted for more than half of all politically motivated crimes – the highest level since police started collecting such data in 2001. Meanwhile violent crimes classified as political in nature rose by nearly 20 percent year-on-year to 3,365 and included 11 murders and 13 attempted murders. Security is rapidly emerging as a key political issue ahead of the upcoming national election in September. German intelligence fears that far-right activists are trying to exploit public frustration over lockdowns imposed to halt the spread of COVID-19 to incite violence against state institutions. "These numbers are very alarming mainly because a trend has been established over the last few years," the Interior Minister explained.

Air Partner launches NSSA

Redline Assured Security and aviation safety specialist Baines Simmons – which form the Safety & Security Division at Air Partner – have said safety and security standards must sit at the top of the aviation industry agenda as the UK returns to international travel. As a result, Air Partner has launched its newly branded National Safety & Security Academy (NSSA) in Doncaster. Formerly the National Security Training Centre (NSTC) run by Redline Assured Security and endorsed by ICAO as an Aviation Security Training Centre, the NSSA will provide safety and security training for the aviation industry under one roof. NSSA scheduled courses include Redline's Aviation Security Managers course, to equip security managers knowledge of threat, risk and crisis management. Additionally, Redline offers Recognition of Firearms & Explosive (RFX) Instructors courses – a pre-requisite for a Certified Instructor to deliver the RFX component of regulatory aviation security courses.

NEWS

Americas

Senators propose new bill to bolster US cybersecurity

Senators Jacky Rosen and Marsha Blackburn have introduced the Civilian Cyber Security Reserve Act in an effort to bolster nationwide cybersecurity efforts in the US. The lawmakers noted the bill would establish a pilot Civilian Cybersecurity Reserve programme to provide the Department of Defense and the Department of Homeland Security with cybersecurity-trained civilian personnel to ensure the government has the necessary talent to address cyber vulnerabilities. "The recent, unprecedented cyberattacks targeting the United States demonstrate the risks of not addressing our severe cyber workforce shortage," Rosen said. "As cybersecurity threats continue to grow in scale, frequency and sophistication, it's critical that we find innovative solutions to address this deficiency," said Senator Rosen. "I'm proud to introduce this bipartisan legislation to ensure the federal government has the cyber experts needed to quickly respond to threats, especially when our nation is under attack." Blackburn added: "Creating a reserve corps similar to our National Guard or Army Reserve will allow our national security agencies to have access to the qualified, capable and service-oriented American talent necessary to respond when an attack occurs."

Slotkin: need for intel on foreign white supremacist groups

Former CIA analyst turned Democratic congresswoman Elissa Slotkin has urged America's top national security officials to increase intelligence gathering on foreign white supremacist groups so that they can be designated as terrorist organisations. Applying that designation would expand US law enforcement's ability to pursue Americans domestically who have contacts with foreign groups such as neo-Nazi organisations based in Europe. The concern among some US national security officials is that such foreign groups might go on to inspire American white supremacists and potentially provide them with training and resources to carry out violent attacks on US soil. Before the US government can officially label a foreign entity as a terrorist organisation it has to meet a certain threshold of evidence to back up its case. And right now it is not collecting enough intelligence on these groups to do so. "My biggest fear is an increase in the sophistication and frequency of lone wolf white supremacist terrorist attacks in the US," Slotkin told CNN.

Nearly 50% of ransomware-hit organisations are in US

US organisations are extremely profitable for hackers as they tend to reach a wider market than most other countries, which often means that they have more resources. Moreover, having more employees, contractors and using more services creates a broader attack surface for hackers to exploit. On a similar note, 39 (12 percent) of businesses in Canada got trapped by ransomware and were forced to pay up. Ransomware is a lucrative market. The average ransom paid by organisations in the United States, Canada and Europe rose by 171 percent from $115,123 in 2019 to $312,493 in 2020. Several ransomware families have demonstrated their ability to exfiltrate data and use double extortion tactics, including NetWalker, RagnarLocker, DoppelPaymer and several others. Instead of only encrypting data on the victim's computer, hackers also export files to their own computers in order to further compel the victim to pay the ransom. In case the ransom is not paid, criminals threaten to publish the data on leak sites and forums that are operating on the Dark Web. By far the most effective ransomware family is NetWalker, which was used in 33 percent of attacks last year.

Attorney general calls for more funding for domestic terrorism

Attorney General Merrick Garland has pressed Congress for increased funding to combat domestic terrorism and prosecute hate. Testifying to Congress for the first time as attorney general before a House Appropriations subcommittee, Garland also spoke about policing reforms, including a budget request to enhance community-oriented policing. Asked what dangers trouble him the most, Garland described foreign and domestic terrorism as an emerging and accelerating threat, noting: "Both forms of terrorism are of extraordinary concern to me. We never want to take our eyes off of what happened on 9/11 and the risks that our country continues to face from foreign-origin attacks on the homeland," he said. "Likewise, we have a growing fear of domestic violent extremism and domestic terrorism. Both of those keep me up at night." Garland revealed that President Biden's budget request for the Justice Department is designed to address both international and domestic terrorism and includes $40 million to US attorneys to manage domestic terrorism caseloads."

New pipeline security regulations after Colonial attack

Homeland Security is preparing to issue new regulations for pipeline security following the ransomware attack that disrupted Colonial Pipeline's operations in early May. *The Washington Post* reported the agency would issue security directives which would require companies to report cyber incidents to federal authorities. Although Colonial Pipeline worked with the FBI following the attack, lawmakers took issue with its engagement with the Cybersecurity and Infrastructure Security Agency. The CISA's acting chief Brandon Wales testified at a recent hearing that he does not believe the company would have contacted his agency at all if the FBI had not acted as an intermediary.

NEWS

Asia

Japanese companies ditch Chinese drones

A number of leading Japanese infrastructure companies have decided to end their use of Chinese-made drones, following the government's efforts to curb potential security risks. There have been concerns that drones made by Chinese companies transmit sensitive data to their manufacturers, and Japan is following suit after the US effectively blacklisted Chinese drone maker DJI last year over national security concerns. The guidelines apply to drones used to inspect infrastructure, in addition to those used for national security purposes. The government is also asking private-sector contractors to step up their security measures. Japanese drone makers are consequently ramping up development efforts to take advantage of the likely rise in demand for homegrown products. Autonomous Control Systems Laboratory, which is listed on the Tokyo Stock Exchange's startup-focused Mothers market, is developing a drone with Yamaha Motor and other partners to go on sale as early as October. The drone's flight data and any images it takes will be protected."Major electricity and gas companies have approached us, saying they want to switch to domestically made drones for inspections and other uses," ACSL President Satoshi Washiya said.

Philippines data breach flagged by UK security firm

More than 300,000 files and documents, some of which contained sensitive information, belonging to the Office of the Solicitor General of the Philippines were accessed by an unknown party, according to UK-based cyber security provider TurgenSec. The cyber security provider said in an online post that the data breach contained files ranging from documents generated in the day-to-day running of the Solicitor General of the Philippines, to staff training documents, internal passwords and policies, staffing payment information and information on financial processes and activities including audits. The breached information also included several hundred files titled with presumably sensitive keywords such as Private, Confidential, Witness and Password, the company claimed. TurgenSec has alleged that the information was public facing, meaning anyone with a browser and internet connection could access it. It is claimed that the breached data was accessed and downloaded by an unknown third party that was not TurgenSec. The company explained that the data breach was particularly alarming, given that at least some of the information contained governmental sensitivity and could impact on-going prosecutions and national security.

North Korea: Biden has made a big blunder

North Korea has warned that the United States will face: "a very grave situation" and alleged that President Biden: "made a big blunder" in his first address to Congress by calling the North a security threat. In the speech, Biden referred to North Korea and Iran's nuclear programmes as: "serious threats" to American and world security and said he'll work with allies to address those problems through diplomacy and stern deterrence. "His statement clearly reflects his intent to keep enforcing the hostile policy toward the DPRK as it had been done by the US for over half a century," Kwon Jong Gun, a senior North Korean Foreign Ministry official, said in a statement. Kwon refused to be drawn on what steps North Korea would take, and his statement could be seen as an effort to apply pressure on the Biden administration as it's shaping up its North Korea policy.

Indian firms struggle to educate employees on cybersecurity

As many as 80 percent of Indian organisations have struggled to provide adequate education to their leaders and employees regarding cybersecurity, according to the findings of the second edition of the Sophos survey *The Future of Cybersecurity in Asia Pacific and Japan*, in collaboration with Tech Research Asia. The study has revealed that despite the increase in cyberattacks, cybersecurity budgets have remained stagnant and executive teams continue to underestimate the level of damage an attack can do to their organisation. Perhaps more worrying, findings revealed that 56 percent of Indian organisations were not running up-to-date cybersecurity protection at the time of the most significant attack they suffered in the past year. The survey additionally identified the top cybersecurity frustration of IT leaders to be that executives assume that their organisation will never get attacked. This was followed by the assumption that although their organisation may be compromised, there is nothing they can do to stop it

Isis: Android downloads could leave jihadists vulnerable

An ISIS-supporting cybersecurity group that launched cloud and chat platforms in April has warned its followers that Android downloads could leave them: "vulnerable to penetration and targeting." Launched in 2016, the Electronic Horizons Foundation advises ISIS supporters on how to encrypt their communications and avoid detection online while coordinating with and recruiting jihadists. Earlier this year it provided guidelines telling supporters that "spies of intelligence agencies are using a new method to track down supporters through Google Play Store" – specifically, a custom app that: "collects identifiable information of android phones." Their latest alert lists the Play Store as an authoritative source for downloads and tries to steer ISIS supporters away from less reputable download sources. "A widespread danger and threat, which we have repeatedly warned from, which is downloading applications in APK (Android Package Kit) format from unknown sources," said the alert posted in Arabic, English and French. "The curse of corrupted files targeting the munasirin (supporter) has spread, and most of those who fall into the traps of this matter are simple munasirin, who do not have technical experience in examining corrupted or suspicious files." In a mid-April alert, the group also warned against using Bitcoin "for financial transactions and money transfer".

SMART SECURITY SOLUTIONS

DTP 320DV

DUAL VIEW PASSENGER VEHICLE AND VAN
X-RAY INSPECTION SYSTEM

DTP 7500LVR

RELOCATABLE VEHICLE X-RAY INSPECTION SYSTEM

AI POWERED

TRANSMISSION
X-RAY
TECHNOLOGY

CONPASS SMART 5AI

UNIQUE HIGH INSPECTION SPEED BODYSCANNER

AI
ARTIFICIAL
INTELLIGENCE

BV STREAM

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

0480-SP15112019

X-RAY SECURITY SCREENING SYSTEMS

ISO 9001 SYSTEM CERTIFICATION SGS | CE

info@adanisystems.com
www.adanisystems.com

ADANI

NEWS

Africa

Boko Haram "on verge of caliphate" in Sub-Saharan Africa

Boko Haram and affiliated Islamic terrorists are poised to form a caliphate in Sub-Saharan Africa, according to international religious liberty leaders. US Commission on International Religious Freedom (USCIRF) member Johnnie Moore and Open Doors CEO David Curry have both claimed that conditions are ripe for Boko Haram and associated terrorists to form a caliphate in the region, with Nigeria proving one of the most dangerous countries. Moore notes that the fact that USCIRF has named Boko Haram and a handful of other terrorist groups as entities of particular concern indicates that they already have some type of territorial control, a requirement for the commission's EPC designation. In its 2021 Annual Report, USCIRF recommended US policy changes to counter terrorism in the region. Moore points out the US relationship with Nigeria, which has focused largely on economic and humanitarian concerns including food security. "And yet, it doesn't seem like we've had a comprehensive approach solving the internal insurgency in the country," he noted.

Boko Haram lures residents with cash and recruits children

Suspected Boko Haram members are reported to be recruiting children and using them in their operations in Yobe State and other areas in Nigeria, sources have revealed. The insurgents are also luring residents of Gaidam in Yobe State with N20,000 each and other items as Ramadan gifts. Some residents are reported to have received N20,000 each from Boko Haram fighters loyal to the Islamic State in West Africa Province (ISWAP). A credible source in Gaidam said many people in the town had received the amount, with some families willingly collecting the money while others reluctantly doing so fearing that they will be targeted if they don't. "They don't want to be flogged or killed if they reject it. The group has suffered major military losses in the area, it seems to be adopting new strategies to revive its influence in the region," the source said. Another source claimed Boko Haram terrorists have been gathering people and preaching to them freely without any fear of security agencies, before urging the government and security operatives in the area to confront them.

Mozambique Leaders meet to thrash out Total security deal

Business and political leaders flocked to Maputo in May to thrash out a security deal that would allow workers to return safely to the Rovuma gasfields off the northern coast of Mozambique after terror attacks brought all development to a halt in March. French energy giant Total suspended works on its natural gas project in Cabo Delgado, the country's northernmost province, when Islamic State-backed terrorists overran the town of Palma in March, leaving dozens dead and forcing hundreds of thousands more to flee the area. Now it has declared '*force majeure*' and pulled its staff from the area, with thousands of contractors linked to the project returning home awaiting new of further developments. Also discussed was the need for a '*cordon sanitaire*' around the town and its surrounds that will prevent a repeat of the attacks. It is reckoned this will need a multinational force of 2 900, backed by helicopter support and rapid intervention teams.

Nigeria introduces new small arms control centre

The Nigerian government has approved the establishment of a small arms control centre to tackle the illicit flow of weapons and step up responses to insecurity in the country. Named the National Centre for the Control of Small Arms and Light Weapons, the new centre is part of the ongoing restructuring of the country's security architecture to address emerging threats, said a statement from the Office of the National Security Adviser. The centre will serve as an institutional mechanism for policy guidance, research and monitoring of all aspects of small arms and light weapons in the west African country. The impact of the proliferation of small arms across national borders in Africa and the Sahel region has resulted in terrorism, human trafficking, organised crime and insurrections in west Africa and Nigeria. "Therefore, as one of the measures in tackling this threat, the new centre will be fulfilling the requirements of the Ecowas (Economic Community of West African States) moratorium on import, export, and manufacture of light weapons as well as the UN (United Nations) plan of action to prevent, combat, and eradicate the illicit trade in SALW," a report noted

Nigerian researcher creates 'terrorist-tracking' drone

A Nigerian researcher has developed a carbon emission tracking drone he believes will prove effective in locating and arresting criminals, kidnappers and terrorists as they try to avoid detection in remote hiding places. Doctor Olusola Ayoola has equipped his drones with powerful sensors that pick up carbon-based traces left by human beings in natural settings. Because people leave carbon tracks in most things they do – including walking to or sitting around a spot – Ayoola says the Carbon Emission Detection Based Aerial Surveillance drone will become a valuable tool to police and military forces hunting down a wide range of trouble makers – from terrorists to kidnappers. Founder of the Robotic and Artificial Intelligence Nigeria (RAIN) research institute, Ayoola explained that his unit began looking into ways to combat the scourge of often violent criminal activity that plagues his country – as it does many others in Africa.

DIARY DATES

2021 Conference and Exhibition planner

1-30 June IFSEC International Connect
Online event
Organiser: IFSEC International
www.ifsecglobal.com/event/en/register.html

8-10 June Shield Africa 2021
Abidjan, Côte d'Ivoire
Organiser: Coges Events
Tel: +33 1 44 14 51 11
Email: hotline@cogesevents.com
www.shieldafrica.com

13-15 July Info Security Europe 2021
Olympia, London
Organiser: Reed Exhibitions
Tel: +44 (0)20 8271 2130
www.infosecurityeurope.com

17-20 August AFAC 2021
Sydney, Australia
Organiser: Interschutz
Tel: +61 2 9280 3400
Email: info@afacconference.com.au
www.afacconference.com.au

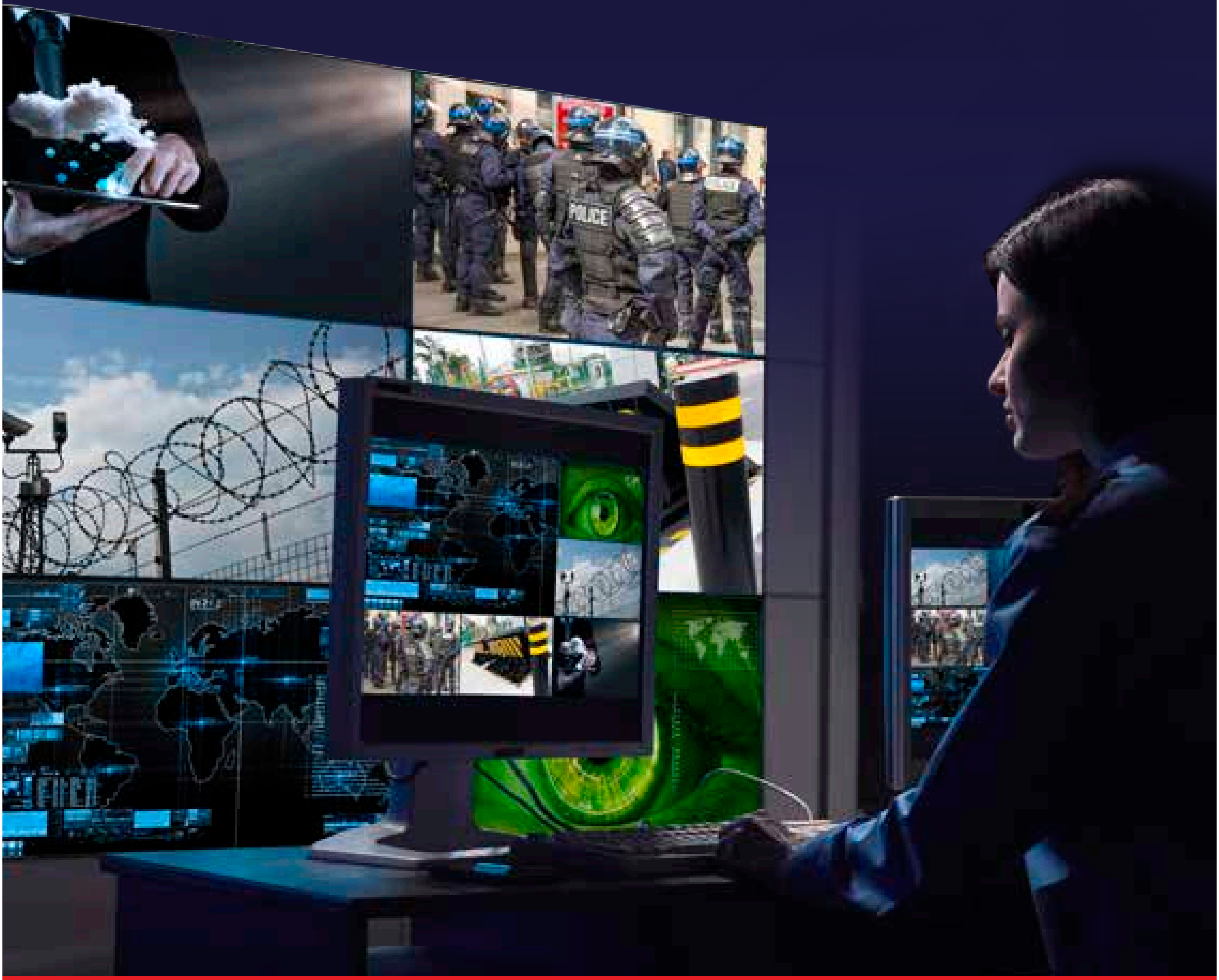
14-16 September CTX 2021
ExCeL, London
Organiser: Clarion Defence and Security Ltd.
Tel: +44 (0) 20 7384 8232
Email: security@clarionevents.com.
www.ctexpo.co.uk

12-14 October ITSA 2021
Nuremburg, Germany
Organiser: Nürnberg Presse GmbH
Tel: +49 9 11 86 06-80 00
www.it-sa.de

13-16 October Interschutz USA 2021
Pennsylvania, USA
Organiser: Interschutz
www.interschutzusa.com

1-3 November IFSEC/FIREX Egypt 2021
Cairo, Egypt
Organiser: Informa PLC
Tel: +971 (0) 4 407 2515
Email: info@ifsecandfirexegypt.com
www.ifsecandfirexegypt.com

9-11 November IFSEC South East Asia 2021
Kuala Lumpa, Malaysia
Organiser: IFSEC
Tel: +44 (0)20 7921 8063
Email: ifseccustomerservice@ubm.com
www.ifsec.events/kl/


POLICE

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

MOVIT® 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

Hensoldt's collision warning system for drones

Sensor solutions provider Hensoldt is pushing ahead with the development of a collision warning system for civil and military drones. After the radar sensor as the core element of a collision warning system was already successfully tested in flight as part of the ProSA-n (military) and KoKo2 (civil) study programmes, work on the software required for interaction with an autopilot is well advanced. As early as this summer a demonstrator of the collision warning system is to prove in flight tests that the sensor performance and the software-supported avoidance logic correspond correctly with the autopilot. Since the beginning of the year, Hensoldt has also been involved in the European Detect and Avoid System programme, in which several European companies are developing a concept for bringing large military medium altitude/long endurance drones, such as the Eurodrone recently released by the German parliament, into European airspace. The company's detect-and-avoid radar uses the latest Active Electronically Scanning Array technology, which allows multiple detection tasks to be performed simultaneously and enables very rapid target detection. The scalable radar can be used in large military drones as well as on board smaller civilian drones.

SmartSearch SmartOne fraud protection

Anti-money laundering solution provider SmartSearch has unveiled SmartOne a new digital solution, ensuring businesses and professional service providers can quickly and easily perform accurate ID checks on individuals in the UK and international markets. Fraudsters are targeting legal, property and financial services using false identities, which are easily forged to get round any checks on ID or age verification required to access products and services. By simply entering an individual's name, address and date of birth, users can receive a full identity check which scans multiple global data sources in less than two seconds. Working in real-time, SmartOne is also more efficient than a manual check as all searches are automatically saved on the SmartOne system, allowing instant access to customer data whenever you need it. John Dobson, CEO at SmartSearch, notes: "As the rate of fraud continues to increase, electronic checks are the only way to effectively protect your business. Our solution is updated in line with laws and Financial Conduct Authority regulations, ensuring your business always meets its legal requirements."

Tether Technology brings AI to CCTV

Tether Technology has partnered with South African company DeepAlert to bring artificial intelligence to its range of CCTV cloud technology. Tether enables rapid and intuitive decision-making within the security space, by integrating all surveillance devices across multiple sites with its intelligent cloud analytics platform to visually interpret events. Tether Technology has introduced The Tetherbox and Tether Platform to provide an adaptable and economical solution to bring all physical security devices into a single visual dashboard. The system automatically detects and manages all cameras connected to the Local Area Network, stores images from selected cameras and provides a secure VPN to the cloud platform. Tether is non-proprietary and will integrate with any other security device it comes across. Meanwhile DeepAlert makes use of motion triggers and object detection using deep learning models. The system uses neural network technology to process and determine whether the video image matches known classes of objects, which it has been trained to identify

ATG Access shallow foundation innovation

ATG Access has unveiled the latest addition to its shallow foundation bollard portfolio, the SP400 SM 48. Successfully impact-tested to both the BSI PAS 68 and IWA 14-1 standards, it can arrest a 7,500kg vehicle travelling at 48kph and is ideal for securing critical national infrastructure and crowded places. The SP400 SM 48 can cope with curves, gradients and changes in ground levels using just one foundation module. Additionally, the foundation bases can be installed ahead of the bollards, further enhancing the ease and speed of installation in busy urban environments that are operational 24 hours a day. The bollard has a slim profile, making it aesthetically pleasing and it can be fitted with a multitude of bespoke sleeve designs or incorporated into street furniture designs. With a compact, modular design requiring limited components, the product can be transported easily and efficiently. This, combined with the small quantities of concrete required for installation, helps to minimise the SP400 SM 48's impact on the environment.

FLIR Systems radiometric thermal imaging module

FLIR has introduced a new camera core that represents its best high-performance uncooled thermal imaging technology within a small, lightweight, and low-power package. The new Boson radiometric camera core comes in two versions, 640 x 512 or 320 x 256 resolutions with multiple lens configurations and the ability to capture temperature data for quantitative assessment. The camera core is meant for use in systems across a variety of applications including security, firefighting, surveillance, unmanned systems, industrial inspection and fixed-asset monitoring. Featuring radiometric accuracy that provides ±5 °C (±8 °F) or ±5% temperature measurement accuracy, the Boson Radiometric cameras include a Spot Meter Accuracy software feature that provides an assessment of how accurate a given temperature measurement appears in the scene. Available as telemetry data accessed through the Boson SDK or the Boson graphical user interface, this feature provides guidance across five confidence grades offering in-the-moment assessment to help improve temperature measurement confidence.

3DX-RAY

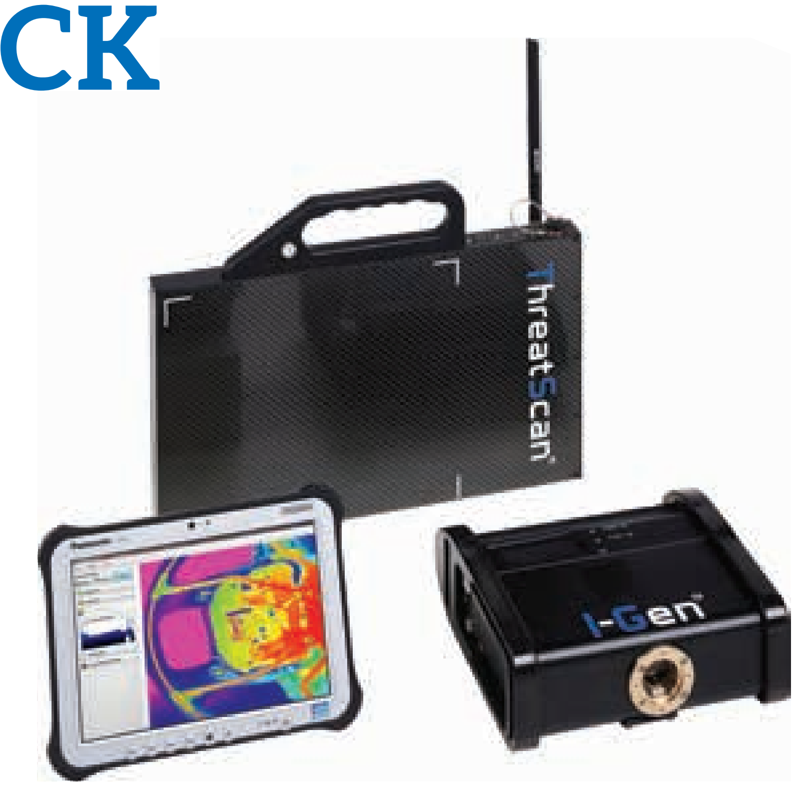
INSIGHT WHERE IT MATTERS

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