www.intersec.co.uk

intersec

The Journal of International Security

May 2024

Aesthetics versus security

Getting the perfect balance

FRANCE PREPARES

Security concerns as Olympics comes to Paris

POLMIL®

ON-GROUND RELOCATABLE SECURITY FENCING

POLMIL® CPNI ASSESSED

POLMIL® PAS 68 RATED
(Test Reports on Request)

POLMIL® MOB ATTACK TESTED

POLMIL® TESTED AND PROVEN

POLMIL® HOT DIPPED GALVANISED FOR COASTAL ENVIRONMENTS

POLMIL® WITH WATER BALLAST

POLMIL® IS A DIVISION OF BLOK N MESH UK LIMITED

THE QUEEN'S AWARDS FOR ENTERPRISE: 2016

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

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

Tel: UK +44 (0) 151 545 3050

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

Tel: FR +33 (0) 3.20.02.00.28

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

Tel: Qatar +974 6652 1197

www.polmilfence.com

intersec
Volume 34 Issue 05
May 2024

EDITORIAL COMMENT

With so much negative press surrounding the thorny issue of artificial intelligence, it's important to remember the security benefits it presents. In the UK, for example, British Telecoms has revealed details of how it has been ramping up its use of AI to counter hacking threats to its business customers. Increasingly using artificial intelligence to help detect and neutralise threats from hackers targeting business customers amid repeated attacks on companies, the £10.5-billion telecommunications specialist has patented technology to analyse attack data to allow companies to protect their infrastructure.

With nearly 90 percent of organisations suffering damage before containing security incidents, according to research by Cado Security, British businesses are routinely facing hacking attempts with some recent high-profile victims including the likes of Royal Mail, British Airways and Capita.

With as many as 725 AI-related patents and patent applications in Europe, the US and China, BT Business chief executive Bas Burger explains: "We have all this data around when criminals try to attack, such as time of day, what type of attack, and we have suppliers to help us with the information … all data we enrich and then we have a piece of AI running across it."

He adds that the technology, called Eagle-i, which was launched in 2021, can provide a helpful indication of what kind of policies need to be implemented in a firewall to make sure they are protected against a specific type of attack in the future. BT is additionally using AI to help detect and establish the cause of more mundane things like network faults. This is helping to improve fix times by finding issues that might have taken longer to identify in the past.

Burger notes the pace of technological change has prompted concerns among some companies about whether they were choosing the right technology as well as anxiety about the potential disruption that implementing new technology would cause to their business. In an effort to examine this further, BT conducted a study of 2,000 business leaders and found that 86 percent of company directors and executives report technology as a source of stress as they seek to modernise their businesses. The study highlighted that 88 percent of businesses were investing in new technology this year in an attempt to improve productivity and gain a competitive advantage, and overall tech investment was up 31 percent year on year.

"Every business today is a digital business," Burger said. "They all want to use technology and they are increasing investment… The flip side is everyone is getting anxious about this. The tempo of innovation is increasing, which in itself gives a lot of business leaders anxiety about 'what should I do?' It's like changing an aeroplane engine while the aeroplane is flying – you're anxious because the aeroplane is in the air."

BT is increasingly pushing into AI and last year announced that about 10,000 jobs would be replaced by the technology as part of a wider push to cut its workforce by as much as 55,000 by 2030. As the company reported its annual results in late May, with underlying profits expected to come in just below £8-billion, the hope is that reinvestment continues AI's fight back against attacks.

Jacob Charles, editor

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

Subscriptions
Annual Subscription Rates: UK £180,
Europe £200,
USA post paid US$350
Other Countries air-speeded £250. 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 2024

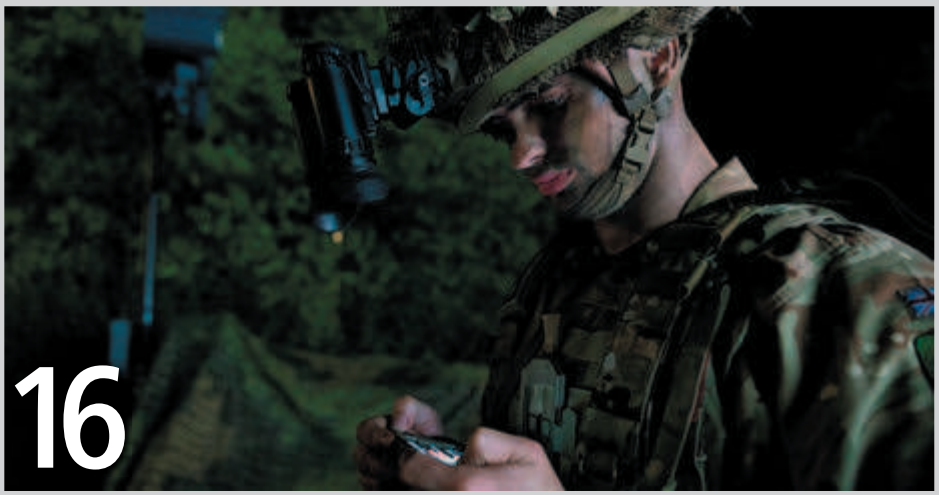
CONTENTS

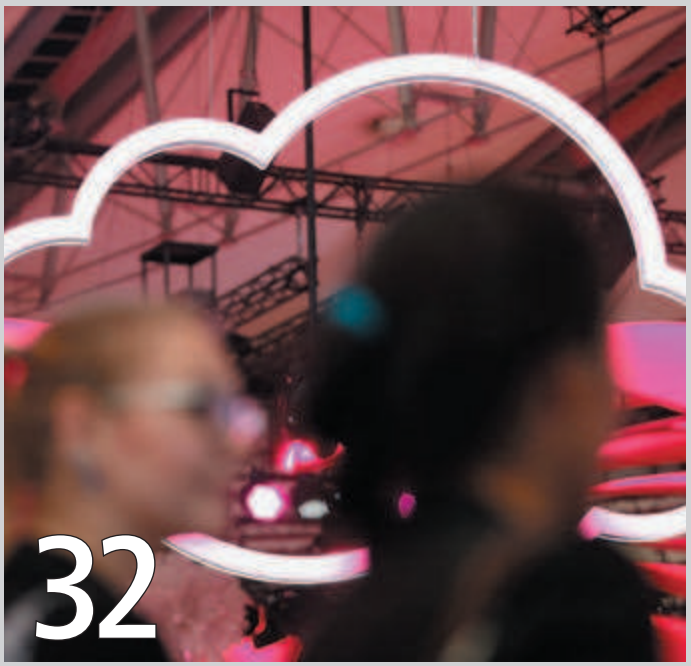
May 2024 www.intersec.co.uk

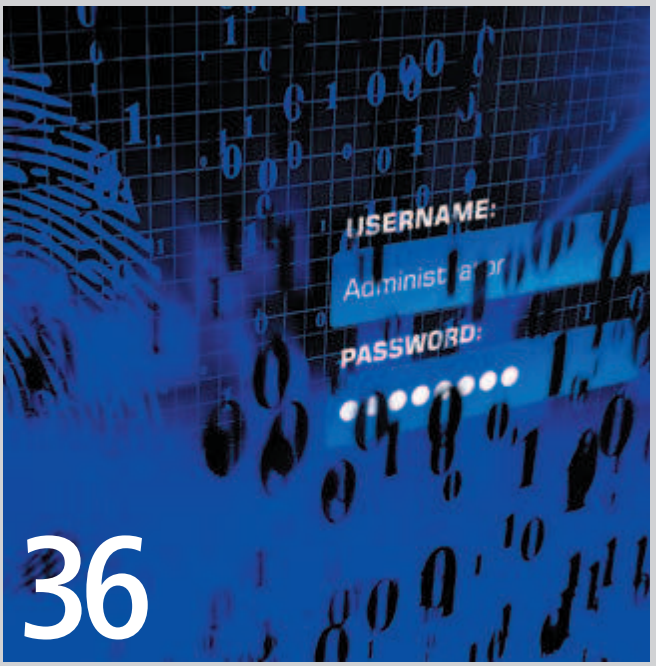
intersec

Features

Regulars







Simon Alderson is CEO of First Response Group

A WELCOME BOOST

Simon Alderson *on the Home Office funding boost to help fight knife crime*

At the end of May, the UK Home Office announced a £4-million funding boost to include investment in new knife detection technology in an effort to try to keep knife crime below pre-pandemic levels. Commenting on the plan, however, police commander Stephen Clayman noted that while the police are taking efforts to tackle symptoms, they quite simply do not have the cure. While I personally would welcome the funding news as it is clearly an important investment for the police, we should nonetheless be mindful that it is our security officers who are increasingly on the front line of weapons-based crime and they need our support to protect them, and the public.

According to the Office of National Statistics, some 50,489 knife crime offences were recorded in the year to March 2023. This is up from 48,204 in the previous 12 months, but lower than the 54,293 recorded in the year to March 2020. With official stats showing a "noticeable increase" in robberies involving a knife or sharp instrument, data like this leads to an inevitable conclusion that security guards are no doubt bearing the brunt of it.

TRAINING STAFF IN ACTION COUNTERS TERRORISM AWARENESS GIVES THEM ALL THE SKILLS THEY NEED

This is why now, more than ever, it is our duty as employers to ensure that our teams are fully equipped in both a training and technological sense, to identify, assess the risk, and handle a weapons-based offence in the appropriate way, with safety as their number one priority. Even the most experienced security officer can fall victim to a weapons-based attack when faced with an unexpected situation. Preparing teams with specific weapons training has the potential to mean the difference between a situation escalating or being safely defused.

The stats previously mentioned only cover knife crime and a weapon can, of course, be anything that is improvised to intimidate, threat or cause harm to a member of the public or our staff. Our teams have first-hand experience of items such as empty bottles, glasses, baseball bats, tools and even everyday household scissors, being used to cause harm. Therefore, the actual figures are most likely higher.

Picture credit: AdobeStock

Training your staff in Action Counters Terrorism (ACT) Awareness and the SCaN programme will give them the skills that they need to prepare them for dangerous situations. By investing in your teams, you are not only prioritising the health and wellbeing of your own people, but you are additionally prioritising the safety of your client and their customers.

And it's not just about training. Investing in technology such as body cameras, biometric technologies, communication devices, surveillance, GPS monitoring and electronic incident reports have all changed the way offences are identified and recorded. In the event of unexpected weapons-based activity, it is essential that teams can communicate effectively and record events. By giving your teams the best technology, you're giving them an extra pair of hands or eyes to help manage a situation.

At FRG we strive to do the best we can for our colleagues, with 'people first' as our priority and that is why we ensure wherever possible that our team has the best training and equipment required for the job. However, sadly until the root cause of knife and other weapons-based crime is addressed, we must be prepared for all eventualities ●

Official stats show a noticeable increase in robberies involving a knife or sharp instrument

Picture credit: Nicolas Michaud

OLYMPICS SECURITY

Kate Fitzpatrick *considers the main security concerns as the world gathers in Paris*

Paris is hosting the Olympics for the first time in 100 years. While many Parisians are planning to leave the city or have been told to work from home, over 15-million tourists, athletes and journalists are predicted to descend on the city.

Paris' infrastructure, including its airports, roads, trains, hotels, the metro underground and cafes and restaurants, will be under enormous pressure during the six-week period of the Games. Furthermore, following the 22 March terrorist attack in Moscow, France raised its national security alert system to the highest level.

The Olympics are taking place from 26 July to 11 August with almost 10-million tickets available for the events, while the Paralympics Summer Games, from 28 August to 8 September, is selling a further three-million tickets.

To fulfil its desire to be the greenest Olympics ever, Paris has chosen to utilise existing buildings and spaces. This means that not only will events be held across the

Around 35,000 police and gendarmes are expected to be mobilised each day during the games

city, stretching security capabilities, they will also be held at iconic landmarks, including the Eiffel Tower, Place de la Concorde and the Grand Palais, adding to the complexity of security logistics. In addition, and for the first time, the opening ceremony is not in the confines of the main stadium but instead is being held on the River Seine.

Hosting this monumental event comes with it a myriad of security challenges, necessitating comprehensive planning and coordination to keep the participants and spectators safe.

With any large-scale event, security is pushed to its limits. They are also a prime target for protests, terrorist acts and general unrest, eg, strikes. With the world's media present, it is the ideal time to raise awareness for a cause or create major havoc.

We know that security is often very tight entering a venue, with the public generally very cooperative with security personnel's checks. However, on exiting people are relaxed and focused on getting home rather than thinking about their surroundings. In 2017, it was at the end of an Ariana Grande concert in Manchester, as the crowds were dispersing, that the terrorists struck, taking advantage of the happy, milling crowd.

Around 35,000 police and gendarmes are expected to be mobilised each day during the games, with a peak of 45,000 expected for the opening ceremony. 18,000 French military troops will also be deployed, including 3,000 responsible for aerial surveillance and supported by up to 22,000 private security agents and 18,000 soldiers. The security operation will also be boosted by military and police personnel from 46 other nations including dog handlers, horse riders and mounted patrols.

The French government is also undertaking one million anti-terrorism checks and investigations in the run-up to the Olympics, which will include athletes and people living close to key infrastructure.

To guarantee the safety of visitors and to manage crowd flows, safety perimeters will be set up around the competition venues. These will restrict vehicles but will allow for the free movement of ticket holders, pedestrians and cyclists depending on which of the four zones is entered. Motorised vehicles may need to be Paris 2024-accredited to gain entry.

The security perimeter will often be in place for the hours preceding and immediately after the last event. Also, at least a week before the start, anyone entering areas of central Paris will need to have registered for a QR code and to show identity papers.

The Opening Ceremony on 26 July is being held on the River Seine with 10,000 athletes sailing on around 100 boats along a four mile (6km) stretch of the river.

From around 20 July onwards, a first security perimeter will be set up around the Seine, following the same regulations as the perimeters for the competition venues. The airspace will be closed and more than 45,000 police officials will be in attendance on the day.

Spectator places have already been reduced from about 600,000 people to just over 320,000 for security reasons. President Macron has said that France has a "plan B and a plan C" if they are forced to cancel this open-air spectacle for security reasons.

Paris' historical landmarks and buildings will form the backdrop of the Olympics, which has prioritised adapting existing buildings and structures to host the 869 events rather than building new ones.

With the Place de la Concorde hosting the basketball, skateboarding and BMX competitions, to the beach volleyball at the foot of the Eiffel Tower, and the fencing and taekwondo at the Grand Palais, the Olympics will stretch all over the city. The Palace of Versailles will also host equestrian events and is on the marathon route.

Holding events outside stadiums requires more sophisticated security arrangements, not least because France is at its highest alert level.

The Olympics will also extend beyond Paris, with the cities of Lyon, Nice, Bordeaux, Nantes and Marseille hosting events, and it even extends to the beaches of Tahiti, which is hosting the surfing.

The security risk will be high, but steps can be taken to minimise exposure and preparation is key to ensuring a safe and enjoyable experience.

UP TO 3,000 FRENCH MILITARY TROOPS WILL BE RESPONSIBLE FOR AERIAL SURVEILLANCE

The Opening Ceremony: This is taking place on the River Seine, so there will be detailed crowd control measures in place. Before attending this event, you should familiarise yourself with the rules governing where you can and can't go. Some streets and exits will be blocked.

Stay Informed: Keep up-to-date on the latest security news, speak to your hotel reception and check for any unrest, protests, *etc*. on reputable websites, including government ones. Download a travel risk app or set up news alerts to be the first informed. Remember social media is not a reliable source of information.

Know your surroundings: Get your bearings and research in advance the best routes to arrive and leave. Have a hard copy of an up-to-date map and mark your hotel, the airport and train station on it, as well as routes to and from the events. Also download an offline map on your smartphone.

Think About Your Personal Situation: Are you a lone traveller, a family, friends, or work colleagues? How fit and mobile is your party? Also, are you at particular risk, for instance are you diabetic and need regular medication? What can you do to mitigate the risks if, for example, you cannot return to your hotel due to a large-scale protest?

Remain Alert: Always remain vigilant and be aware of your surroundings, so you are more likely to notice if something doesn't look or feel safe. Also, keep your valuables close. In crowded situations, there will always be opportunistic thieves and con artists, so leave expensive watches and jewellery at home to avoid being a target.

Smartphones: In a security situation, phone signals are often blocked by the authorities or are just overloaded, so it's important to have back-up sources of information and knowledge such as keeping your hotel address, directions and other important information in the notes section of your phone.

Go Old School: Think about how you would manage without modern technology and prepare accordingly. Have hard copies of important documents, maps and useful information, eg important telephone numbers including next of kin, a passport copy and insurance details. Ensure that all members of your party have hard copies of each other's contact details as well as the address and phone number of your hotel/accommodation.

FROM 20 JULY ONWARDS, A FIRST SECURITY PERIMETER WILL BE SET UP AROUND THE SEINE

Transport: A local taxi firm can be a good option as they know the local area and will be abreast of the latest news. Pick up a card for a local company on arriving in Paris.

React Quickly: Do not wait for a situation to get out of control, if there are red flags that your safety might be compromised then it's important to remove yourself from the situation as soon as possible.

Find a Place of Safety: If you feel in danger because of protests or unrest, find somewhere you can shelter temporarily, like a café or restaurant, until the authorities say it's safe.

Designate an Emergency Meeting Place: With large crowds, it can be easy to get separated so have an agreed safe meeting place to head towards.

Emergency Numbers & Providers: Know the country code for emergencies. For France and the European Union, it is 112. Also, know where the nearest hospitals are and mark them on your hard copy map.

Power pack: Have a back-up power pack to charge your smartphone and spare chargers (remember to have the country-specific adapter).

Cash: Have some cash to hand as cards might not work if power lines are down.

Stay hydrated: Travel with refillable water bottles. It's important not to get dehydrated, particularly as there could be high temperatures in Paris.

Airport / train station: In the unlikely event of a serious incident where you need to leave the city, it's important to know where your main transport exits are located. Write down the directions from the hotel or stadium to the airport, and train stations. If the airport is over-congested, it might be worth taking a train to an alternative airport for a flight home ●

Kate Fitzpatrick
is Security Director EMEA at World Travel Protection.

A Rapier FSC Ground Based Air Defence (GBAD) system was employed in the London 2012 Olympics

Picture credit: Crown Copyright

THE QUEEN'S AWARDS FOR ENTERPRISE: INNOVATION 2020

eskan™

OFFER!

Complimentary situational training on your first purchase of an Eskan product. Quote ESK22CT when ordering.

Increasing security. Reducing risk.

Innovative, state of the art solutions for covert surveillance, counter surveillance (TSCM) and RF jamming

Eskan provide advanced technology solutions and training to increase local and national security, and to reduce the risks of disruption posed by criminals and terrorists. For over three decades our development engineers have been working to provide the most advanced products available for law enforcement, intelligence services and defence organisations worldwide. We are ISO 9001 and ISO 27001 accredited. To find out more or to request a product brochure, please contact us or visit our website.

+44 20 8813 0776 / info@eskan.com / **eskan.com**

BALANCING ACT

Dominic Renney *explores how to get the mix of security and aesthetics right*

With an increase in pedestrianised spaces and placemaking throughout the world, planners have been given an opportunity to look at urban spaces differently; from designing fresh and exciting areas specifically for pedestrians to changing the way that existing town and city centres look and operate.

However, with this new opportunity comes a new responsibility, both for urban designers and councils/venue operators. For when we encourage people to gather – by creating pedestrian zones – there comes the implicit responsibility to ensure safety and security for anyone that uses them.

When designing or redesigning spaces, planners need to consider ways to mitigate potential hostile vehicle attacks and ensure pedestrian security. This can be achieved through the implementation of physical security products, for example HVM bollards. These are designed to mitigate hostile vehicle attacks and can reduce risks by providing a deterrent and impact-tested protection in the unlikely event of an attack. But how do you successfully implement the necessary security measures without compromising on area aesthetics, and do aesthetics have to give way to a 'fortress mentality'?

As with any urban planning project, thinking about the implementation of security can mean making compromises on aesthetics – after all, crash-tested HVM bollards are visible structures that might not fit an architect's vision of a space. However, keeping the public safe should always be one of the primary concerns, and so finding a balance between the two is crucial for any project's viability. The three considerations below offer a simple guide to ensuring the right security while achieving an aesthetic balance.

PROCESS

In security design, 'process' refers to the considerations between security risk, aesthetics and user considerations. This must include thinking about how proportionate a project is and how it justifies its cost, but also how each of the threads come together to make a project work best. This stage involves thinking about it in the broadest possible terms, involving designers, architects and security consultants to uncover any concerns that each might have about the aesthetic-security balance.

Dominic Renney is ATG's Product Specification Manager and has a wealth of experience working collaboratively with clients and designers developing robust project specifications which not only work operationally but also look good and meet security requirements.

Picture credits: ATG

PROPORTIONALITY

The second step to balancing the security and aesthetic concerns is working out the proportionality to balance a project's threat-versus-risk score. This can help to guide the balance between aesthetics, usability and security robustness, hopefully finding an acceptable level for each factor. Security consultants work with developers and architects during this stage to agree on a level of security that not only keeps the public safe, but also lives up to the architect's and designer's expectations.

PEOPLE

The final consideration to ensure that the security and design principles don't impede each other is that people are at the heart of everything to do with projects. Making sure that the right people are brought in at the right stages to be able to start the conversations early is key to finding the right balance.

Finding the right balance between security and aesthetics can be easy when the competing factors are managed successfully, and that compromise is found as early as possible in the process. Every project should have public safety at its heart, and bringing in a security consultant to start the conversation about what needs to be done can help to define the art of the possible.

Likewise, it is vital to look at the security of a specific area holistically, bringing in different stakeholders to develop a wider scheme. This can help to reduce the visual impact of security measures, rather than creating a ring of steel, while ensuring that a wider area is secured – this averts the problem of stakeholders failing to work together and focusing on boundaries.

Other tactics, such as changing road layouts by creating narrower lanes and adding chicanes to reduce vehicle speed, can help to bolster security without damaging aesthetics. The lower the speed and the smaller the vehicle able to gain access to a space, the slimmer and smaller the measures that may need to be deployed.

Finally, some dual-purpose measures can be incorporated into the landscape. So, for example, HVM bollards might be used as cycle stands, planters and bins. Effective planning can help to minimise street clutter and integrate these items as and where they're considered appropriate ●

Bollards can reduce risks by providing protection in the unlikely event of an attack

Sam Stockwell is a Research Associate at The Alan Turing Institute and **Doctor Alexander Babuta** is Director of CETaS at The Alan Turing Institute.

TICKING TIME BOMB

Sam Stockwell *and* **Dr Alexander Babuta** *express concern that there is little time for regulators to counter AI threats before the UK's July general election*

Researchers at The Alan Turing Institute's Centre for Emerging Technology and Security (are urging Ofcom and the Electoral Commission to use a rapidly diminishing window of opportunity to address the use of AI to mislead the public and erode confidence in the integrity of the electoral process.

In a new study, researchers are warning against fears that AI will directly impact election results. They note that, to date, there is limited evidence that AI has prevented a candidate from winning compared with the expected result and that of 112 national elections taking place since January 2023 or forthcoming in 2024, just 19 had suffered AI-enabled interference.

However, there are early signs of damage to the broader democratic system. This includes confusion among the electorate over whether AI-generated content is real, which damages the integrity of online sources; deep fakes inciting online hate against political figures, which threatens their personal safety; and politicians exploiting AI disinformation for potential electoral gain.

The evidence also found that current ambiguous electoral laws on AI could lead to its misuse, such as with people using generative AI systems like ChatGPT to create fake campaign endorsements, which could damage the reputation of individuals implicated and undermine trust in the information environment.

The authors make several recommendations outlining what could be done to mitigate potential threats to the UK's election process including urging the Electoral Commission and Ofcom to create guidelines and request voluntary agreements for political parties detailing how they should use AI for campaigning, while requiring AI-generated material to be clearly marked as such. They also say these organisations should work with the Independent Press Standards Organisation to publish new guidance for media reporting on content which is either alleged or confirmed to be AI-generated, particularly during polling day in light of broadcasting restrictions.

They also recommend that the UK Government's Defending Democracy Task Force (DDTF) and the Joint Election Security and Preparedness Unit (JESP) coordinate exercises with local election officials, media outlets and social media outlets, simulating possible deep fakes of political candidates and AI voter suppression efforts to prepare to deal with these situations when they arise. They say that the DDTF should create a live repository of AI-generated material from recent and upcoming elections so they can analyse trends to inform future public information campaigns.

During the polling period, deep fake attacks, polling disinformation and AI-generated knowledge sources (such as fake news articles) are likely to circulate and create confusion over how, where and when to vote. And after the election, we are most likely to see political candidates being declared the winner before results have been announced, as well as deep fakes and AI bots claiming that there has been election fraud to undermine election integrity.

With a general election just weeks away, political parties are already in the midst of a busy campaigning period. Right now, there is no clear guidance or expectations for preventing AI being used to create false or misleading electoral information. That's why it's so important for regulators to act quickly before it's too late. While we shouldn't overplay the idea that our elections are no longer secure, particularly as worldwide evidence demonstrates no clear evidence of a result being changed by AI, we nevertheless must use this moment to act and make our elections resilient to the threats we face. Regulators can do more to help the public distinguish fact from fiction and ensure voters don't lose faith in the democratic process ●

Ambiguous electoral laws on AI could lead to its misuse

Picture credit: AdobeStock

Kestrel TSCM ® Professional Software

Tap Capture Plot (TCP)™ Total Energy Capture with Dimensional Geo-Location Heat Mapping!

Signals Intelligence Support System ™

Developed in Canada the Kestrel TSCM ® is Well Positioned to Hunt in a Complex Signal Environment!

Our CTO-CGTO Certification Programs, Train Operators to See What We See - That You Don't See

Kestrel TSCM ® Professional Software | Kestrel ® SIGINT Professional Software

Powerful—Disruptive RTSA | SDR Technology for the Modern Spectrum Warrior...

Radio-Frequency Analysis, Power Line Analytics, and Optical Threat Classification within a Standards-Based Software Defined Radio Environment

Total Energy Capture (TEC)™ | Tap Capture Plot (TCP)™ Dimensional Geo-Location Heat Mapping

Kestrel ® is now Artificial-Intelligence (AI) ready!

Are you ready, for the next generation of disruptive signal classification, as a standards-based feature?

The Kestrel TSCM ® Professional Software is by definition and reputation the leading next generation of mission critical TSCM | SIGINT technology with enhanced scalability, flexibility, ease of use, and low procurement cost; as a deployment ready TSCM / SIGINT platform, with near real-time features that address today's and tomorrow's emerging threats!

The Kestrel ® platform now supports the Kestrel ® Lightning RTSA hardware with our Universal Spectral Translator (UST)™ Technology. The UST™ is a dual radio, portable (mobile) handheld platform providing support for the Signal Hound BB60C/D (9 kHz - 6 GHz) and our integrated Kestrel ® Lightning KL63 (9 kHz - 6.3 GHz), KL95 (9 kHz - 9.5 GHz), KL220 (9 kHz - 22 GHz), and KL400 (9 kHz to 40 GHz) within a multiple radio environment!

Kestrel-net ™

Actionable **RF** Intelligence

www.kestreltscm.com

VILUTION
Your vision , Our solution

United Kingdom & European Union Master Distributor

Professional Development *TSCM* Group Inc.

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

WELL CONNECTED

Tristan Wood *explores the power of hybrid networking and how it can underpin robust wide area networks across all arms and services – from land, sea and air*

Defence technology is often a trailblazer for civil systems and applications, and innovation in voice and data communications is no exception. As early as the mid-Eighties, the electronic distribution, sharing and storage of encrypted battlefield data between brigades, divisions and corps headquarters in the British Army of the Rhine (BAOR) was in many ways a rudimentary form of the internet. If an infantry or armoured brigade's tactical headquarters were to be destroyed, the data was resident and shared elsewhere on the 'network'. As national armies innovate with technology to seize and hold the military advantage, the boundaries of possibility are constantly being pushed.

One thing which hasn't changed is the importance of communicating on the move (COTM). Whether on land, sea or in the air, COTM relies on the most robust connectivity solutions to enable rapid information exchange, situational awareness and ISR (intelligence, surveillance and reconnaissance) to allow for seamless command and control, and to ensure human safety.

This has ushered in a new era of satellite communication on the move (SOTM), enabling secure messaging, voice and information exchange, including the emergence of the military internet of things, MIot.

Today's battlefield is not just about decisional information, it has extended to machines and sensors which talk to each other within a wide range of communication networks, from cellular to secure point-to-point systems.

Within less than a decade, MIot technology will enable soldiers carrying a pocket-sized device to locate and identify everyone in their vicinity, even in pitch darkness, so important is situational awareness in the chaos of battle. Nor is this limited to the army; air and naval systems will depend on robust connectivity across

Picture credit: Crown Copyright

MIot technology will enable soldiers carrying a pocket-sized device to locate and identify everyone in their vicinity, even in pitch darkness.

Tristan Wood
is founder of
Livewire Digital.

an exponentially growing number of devices and nodes. Predictive maintenance systems deployed on assault and utility helicopters, naval destroyers and combat aircraft will rely on communication with their digital twins, as will connectivity underpin the rapid growth in autonomous systems at sea and in the air.

Resilient connectivity will support 24/7 automated protective oversight of sensitive locations, being borders, clearance stations for fuel and explosives and forward logistics bases. Meanwhile, connected battlefield health telemedicine systems will enable soldier-worn body sensors to send vital data to field hospitals and medical facilities receiving real-time updates on those in the field or in triage, matched with a soldier's stored medical records.

None of these applications will endure in the face of adversaries' attempts to weaken a force without the guarantee of a wide area network capable of withstanding the disruption of lost connections and damage to nodes.

The solution lies in hybrid connectivity, deploying the resources of the full spectrum of communications infrastructure to avoid reliance on single points of failure and maximise available resources to ensure always-on, intelligent connectivity wherever and whenever it is needed. Hybrid can also sit at the heart of interoperability, between legacy and new technologies, as too with seamless communication between allied forces with different tactical military communication systems and infrastructure.

The concept of agnostically making use of any network, based on location, quality and even cost of service, should dramatically reduce the impact of the problem, and yet awareness and application of 'bonding' technology, or 'true' hybrid connectivity, is nowhere near where it needs to be as machines, people and battlespace demand ever faster 'always-on' connectivity.

The capacity for selective use of satellite networks, alongside the ability to combine this with the power of all other available networks lies at the heart of hybrid connectivity, and the many advantages it can offer.

A key benefit which hybrid connectivity brings to battlespace is its ability to bolster resilience to physical and cyber attack. By combining the resources across the full spectrum of available channels on a wide area network, (WAN) including satellite, hybrid connectivity mitigates against single-point failures and ensures continuity of operations even in the face of persistent interference and disruptions caused by adversaries.

At the core of hybrid is SD-WAN - a technology that uses software-defined networking concepts to distribute network traffic across the WAN. This architecture creates a virtual overlay that bonds underlying private or public WAN connections, such as Multiprotocol Label Switching (MPLS), internet broadband, fibre, LTE, 5G cellular or wireless. As a result, hybrid SD-WAN networking can agnostically combine and transition between these networks. Instead of relying on failover using classic routing techniques – which replaces one bearer with another – hybrid SD-WAN bonds all available connections into a single, seamless and heterogenous 'pipe'. Applying this technique to connectivity on the move, where the availability and characteristics of networks change rapidly, a hybrid solution overcomes the challenges of intermittent connectivity, poor performance and resultant difficulty in scaling.

With hybrid, multiple network technologies are engineered to work seamlessly together and share the load and resources, performing according to any range of preconditions programmed into the underlying architecture. In this way, it can deliver a faster and, crucially, more reliable service, as outlined in Livewire Digital's White Paper, The Future is Hybrid Connectivity.

In civilian settings, bonding and optimisation of communication paths within a hybrid network are enabling drones to deliver live low-latency video

ROBUST CONNECTIVITY WILL BE REQUIRED FOR A GROWING NUMBER OF DEVICES AND NODES

and advanced 3D world sensing & mapping data. This is already being deployed with great success in the policing and first responder markets, from the management of serious incidents involving multiple agencies to the provision of emergency telehealth, deploying remote diagnostics and supervisory support from hospital-based doctors and other specialists right down to the roadside.

A technology that can seamlessly combine multiple networks, such as 4G, 5G, Wi-Fi, GEO and LEO satellite connections, into one fast, secure and highly resilient service is a 'true hybrid' solution. Because it is programmable and not hardware-centric, the variables are potentially limitless for adapting the performance and prioritisation of the network. Classic routing technology may be fine for fixed network applications in peacetime and the office, but not in battlespace where the characteristics and even availability of WANs is constantly changing. This more elastic SD-WAN environment also allows for much greater interoperability of hardware, facilitating a unifying architecture which supports greater collaboration between the three-armed services, as well as between armies and logistic infrastructure.

By harnessing the power of a software-defined approach, all applications and solutions come with improved operational efficiency and economy of resources, as well as cost. It is also scalable, allowing legacy systems to continue operating alongside more advanced network technologies, weapon platforms and equipment. As international geopolitics become more and more turbulent and complex, this degree of interoperability will assume ever greater importance to Defence and Security Alliances to operate with a unified defence system without holding back the evolution of different defence platforms and technologies.

In summary, battlespace and its ether will become increasingly contested. As myriad military hardware and the armed forces that depend on them – on land, sea and air – rely increasingly on a connection, it is vital that the wide area networks which support them benefit from the most robust connections and hybrid is increasingly proving to be its holy grail ●

INSIDER THREAT

Noah Price *examines the risks employees can pose and how to prevent them*

If asked to describe a physical security breach that can impact a company, most people would think of an external criminal intent on harming an organisation. But what if the attack comes from within? Perpetrated by someone you should be able to trust? Insider threats are a serious security risk that every business must prepare for. Failing to do so could be reputationally or financially damaging. According to G4S's first-ever World Security Report, internal threats are expected to increase next year, with 92 percent anticipating their company will be targeted.

Threat actors who commit an insider threat are usually classified as a 'knowing insider' or an 'unknowing insider'. A knowing insider is someone who deliberately uses their access on purpose to cause harm. They are often motivated by financial gain. Or, sometimes they steal company data to gain a competitive edge. Usually, they are a lone wolf who acts on their own without any other influences.

An unknowing insider is someone who may not fully understand what they are doing, or becomes an Insider threat by mistake. Unknowing insiders can also be unaware that they are being taken advantage of by others. They might download malware, give information to scammers or click on a link in a phishing email.

Concerningly, internal threats are increasing. 89 percent of CSOs say their company experienced some form of internal threat in the last 12 months according to the World Security Report; this is expected to increase to 92 percent in the year ahead. Misuse of company resources or data is the most common internal threat, with 35 percent having experienced this, followed closely by leaking of sensitive information at 34 percent. This threat is expected to become the biggest internal threat in the next 12 months.

"Misuse of company resources or data" has the strongest correlation with "implementing more effective security." This was the internal incident most likely to drive companies to improve their security in the last year.

"Unauthorized access to company resources or data," "industrial espionage" and "intellectual property theft" are all expected to increase in the next year. Perceived financial gains may entice a company employee to share confidential information in exchange for payment. Insider threats make headlines; news outlets regularly report on high-profile or unusual incidents - which can damage a brands reputation in the media, with customers and stakeholders.

Fostering a culture that combines security awareness alongside up-to-date equipment and technology is the best preventative measure when it comes to preventing an insider threat. Employees should be regularly trained to identify phishing attempts and suspicious behaviour, as well as reminding them of data security protocols. They should also only have the access they need to certain documents and areas of a building.

Additionally, implementing strong access controls restricts digital and physical theft or leakage. Ideally, access controls should be enhanced with surveillance technology. When employees know the cameras are on them, it's harder to do anything deceitful. Cameras can also help with the issue of people using each other's access cards. The CCTV footage will show who actually entered any specific area, and exactly what they did there. Of course, CCTV will never be enough by itself but should be part of a full security system and monitored by a well-trained team ●

An unknowing insider may not fully understand what they are doing and become an insider threat by mistake

Noah Price is Academy International Director at G4S.

Picture credit: AdobeStock

MESA 2.0 Advanced WiFi Detection Just Got Better!

Detect, analyze and locate WiFi devices.

New Firmware Update Delivers New Capability.

MESA 2.0

Portable Spectrum Analyzer

The MESA®2.0 WiFi mode is just one part of a complete portable spectrum analyzer system for detecting and locating illegal, disruptive, or interfering transmissions. MESA's advanced WiFi mode includes:

- WiFi Access Points (APs), secured and unsecured
- WiFi Client devices, both connected to access points and not connected to access points (NC) such as cell phones, computers, WiFi cameras, etc.
- Bluetooth devices such as cell phones, watches, fitness devices, Bluetooth speakers, Bluetooth tracking devices such as AirTag, Tile, SmartTag, etc.
- Other WiFi and Bluetooth devices (Evil Twin, Piggybacking, Cracking and Sniffing, pineapple…)


Spectrum View


SmartBars™ (Patented)


Mobile Bands


WiFi


Bluetooth

MESA® 2.0 hand-held Spectrum Analyzer

FOR MORE INFORMATION CONTACT:

International Procurement Services (Overseas) Ltd

118 Piccadilly London W1J7NW

Phone: +44 (0)207 258 3771

Email: sales@intpro.co.uk

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

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

Picture credit: Durabook

TOUGH ENOUGH

Fred Kao *reveals how rugged technology is revolutionising the military and defence sector*

Identifying emerging opportunities within the rugged technology sector is never an exact science, particularly in volatile economic markets, but the past 12 months have highlighted its increasing importance within the military and defence sector. Its emerging role in improving communication and productivity on the battlefield has led to an increase in demand for more sophisticated devices, but new methods of warfare have also helped to shape the functionality and capabilities of this technology. Increasing situational awareness through digital application and advanced technology remains vital, helping protect forces and keep them one step ahead of the enemy, but customisation and the emergence of 5G technology, artificial intelligence and the Internet of Things is proving a game-changer. These developments within the rugged technology market are

Sensing and computing devices worn by soldiers and embedded in their equipment collect a variety of static and dynamic biometric data

transforming the military and defence sector and, as these devices continue to offer a strong return on investment, we anticipate that demand will continue to grow.

Over the past year, increased aerospace and defence spending budgets across Europe resulted in strong investment in technology. This includes investment in the Internet of Military Things (IoMT) and technology that improves situational awareness on the battlefield. Durabook experienced an 11 percent uplift in sales for the military and defence sector alone, and we expect to see continued requirements and spending across several territories in the year ahead to support the digitisation within this sector. We also anticipate more emphasis on information technology integration for drone, real-time imaging, telemetry and surveillance applications to combat increasing hostilities.

The deployment of 5G technology, the Internet of Things (IoT) and artificial intelligence (AI) is revolutionising the rugged devices market, and the military and defence sector is leading this charge. Not only does this technology facilitate the smooth flow of data across all branches of the military but also support the safety of troops. For example, the sensing and computing devices worn by soldiers and embedded in their equipment collect a variety of static and dynamic biometric data. The detail of the data collected from cutting-edge rugged devices can also be consolidated and analysed so it can be used immediately to help inform missions and courses of action for teams on the ground, including recovery operations. Rugged devices with 5G capabilities can transmit data and images from the battlefield, allowing military personnel to monitor progress and make informed decisions. Military organisations are also integrating robotics and autonomous systems (RAS) into their armoury and weaponry. Protecting troops, improving situational awareness and reducing soldiers' physical and mental workload while gaining ground on the battlefield are key objectives for military organisations. Beyond operational functionality, AI is also crucial for saving time and costly repairs by enabling predictive maintenance. Engineers can implement AI to forecast a system fault and take proactive measures to avoid failure. This can lead to speedier maintenance but, more importantly, it can mean the difference between life and death on the battlefield.

The flexible and secure transmission of real-time data has never been more important to the military, and the latest cutting-edge combat information systems are transforming operations. For example, the SCORPION combat information system (SCIS) deployed by the French Army is putting data at the heart of the battlefield by allowing battle groups to connect and share combat information. This allows them to enhance combat capabilities and allow soldiers to quickly adapt to new operational challenges. This information system gives them real-time tactical superiority over the enemy. From the central command post down to combat vehicles, it brings combatants and weapon systems together, facilitating the transmission and sharing of tactical information. The flexible use of rugged hardware that forms part of the information system means devices can be deployed on military vehicles, including tanks and drones, which serve a control centre function to instantly share friendly and enemy positions via GIS maps. These rugged tablets can also be carried by infantry units, either on a chest mount or in a backpack, alongside radio equipment to allow a 360° view of the battlefield. Crucially, the versatility of this system means that the Army can also interact with allied forces, for greater situational analysis and operational planning. This information system is redefining joint combat and the digitised battlespace.

THE LATEST DEVICES CAN TRACK LOCATIONS IN THE FIELD AND FEED BACK TO THE CONTROL CENTRE

The rugged devices market has witnessed increasing demand for customised solutions that cater to industry-specific needs. For example, some organisations require devices that can withstand extreme temperatures or hazardous conditions while others need those with extended battery life – for the military, all of these requirements apply. Today's devices can easily be expanded to become a portable cloud or local storage device or server providing immediate and safe analysis, capture and analysis of data for accurate decision-making, such as GIS maps for mission planning. Plug and play expansion capabilities also mean rugged devices can be used as a remote control or radio system for automated technologies such as unmanned aerial vehicles (UAV), drones or other robots, or could be integrated with other technologies such as thermal imaging, heat sensors or night vision goggles. Aerial drones or unmanned aerial vehicles collect massive amounts of data from their journeys recording live streams for optimum surveillance or inspecting and monitoring mission zones. A central rugged device has the capacity to collect and process this data in real time to provide instant intelligence to teams on the ground.

Military and defence organisations are constantly adapting their Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) strategies to improve efficiency, operations and decision-making. Adaptability is a core requirement of this technology, which must perform a range of tasks, such as asset management and repair, diagnostics and maintenance, logistical organisation, flight maintenance and mission control. Rugged devices have radically improved over the past few years to meet this need. Leading manufacturers are producing laptops and tablets that focus on size, weight and power (SWaP), producing smaller, lighter and more intuitive systems. However, this new SWaP focus doesn't mean compromising on performance. Command control systems (CS2) require increasing levels of computing power, so the latest computers still pack in more power for an uninterrupted performance on and off the battlefield. These devices need to operate in all conditions, from sand and snowstorms, to rain and extremely high and low temperatures, all while withstanding drops, knocks and spillages that come with the territory. To meet this demand, modern rugged devices are tested to the highest standards

and include both MIL-STD and IP certifications. The latest computers go beyond even these benchmarks, ensuring continued function in explosive atmospheres or where there is solar radiation, salt fog or fungus. These cutting-edge tablets and laptops, for example, incorporate seamless design and fanless functionality for extreme resilience, robustness and durability in the even most uncompromising environments.

COMBAT INFORMATION SYSTEMS GIVES SOLDIERS TACTICAL SUPERIORITY OVER THE ENEMY

The ability to safely access and transmit sensitive data while in the field is mission critical, so rugged devices must guarantee top secret security classification to protect against cyber hacks, infiltration or other security threats. Data in transit can be a significant risk, so connectivity must be encrypted too. Devices should include a trusted platform module (TPM), which stores RSA encryption keys for hardware authentication and FIPS 104-2 compliance – mandated by US and Canadian governments and generally accepted worldwide – which means the device has been validated for effective cryptographic hardware. This level of flexible connectivity and advanced wireless capability allows soldiers to communicate whenever and wherever they need to, allowing instant access to data and information and using mobile communications in real time for enhanced situational and operational circumstances. The latest devices are part of the 'modern' soldier's equipment and can be used to track locations in the field and feed back to the control centre. More importantly, high-speed voice and radio-activated transmission systems operate with military satellites to enable the secure exchange of large flows of data, while preventing EMC emissions over a given geographical area. Other important security features that can help minimise the threat of a cyber attack include: personalised identification and authentication via fingerprint and smart card readers and RFID. It is also essential that storage devices can be removed easily and rapidly in case of an emergency, so that data can be protected away from the device.

As technology continues to advance, we can expect to see more rugged devices that are smarter, more efficient and more reliable supporting military organisations across more territories. Innovation and digital transformation are shaping the way organisations operate across every industry worldwide, but now here is this more prominent than in the military and defence sector. The most successful and dynamic organisations are investing in flexible and versatile systems and networks that improve operations and recognising that this is where investment is most beneficial. While speed and agility is critical, the growing risk of cyber warfare cannot be underestimated. This is why the latest intelligence systems are designed to meet stringent military standards that protect data in every environment. The most advanced rugged devices are, revolutionising the sector and setting the pace for digital change that can affect the shape of warfare ●

Fred Kao is CEO of Twinhead International Corporation. Before being named CEO in February, 2010, Fred was Twinhead's Vice President responsible for the global product planning, sales and marketing of its core brand Durabook. Prior to Twinhead, Fred was an executive in charge of brand marketing and sales for an image processing device company, having started his professional career as analyst of macroeconomics and derivative products for an investment bank.

These devices need to operate in all conditions, from sand and snowstorms, to rain and extremely high and low temperatures, all while withstanding drops, knocks and spillages that come with the territory

Picture credit: Durabook

DURABOOK

Prepared for the Unexpected

R8 Tablet

EXTREME POWER, ULTRA COMPACT.

- Intel® Core™ 12th gen processor
- 8" DynaVue® sunlight readable display with four touch modes
- Compact and lightweight for enhanced portability
- Versatile connectivity – supports Thunderbolt 4, Wi-Fi 6E and Bluetooth V5.3
- Fanless design with IP66, 6-feet drop and ANSI C1D2 certification

MIL-STD 810H · MIL-STD 461G · IP66 CERTIFIED · 6 ft drop · COOLFINITY™ · C1D2 ANSI · DynaVue

Durabook's cutting-edge rugged tablets manage real-time data safely and securely to support modern workforces across every sector. Beyond its data management capability, the R8 delivers value by streamlining and improving workflows and simplifying processes to support digital and remote operations anywhere, anytime. Optimized for use in even the harshest work environments, organizations across the utility, transportation, logistics, oil and gas, manufacturing, public safety, defence sectors are already realizing how the R8's 8" ultra-compact modular design with revolutionary enterprise performance and unrivalled functionality is primed to meet their needs.

intel. CORE i7 · intel. CORE i5 · intel. PENTIUM GOLD

www.durabook.com

ELECTRONIC COUNTERMEASURES

IPS EQUIPMENT & SWEEP TEAM SERVICES

***NEW** REI MESA MOBILITY*
ENHANCED SPECTRUM ANALYZER

***NEW** ANDRE DELUXE 12GHZ*
WITH ULTRASONIC PROBE

Looking for a

VIDEO POLE CAMERA
2.0 INSPECTION TOOL

EDD-24T NON LINEAR
JUNCTION DETECTOR (HANDHELD)

TSCM TRAINING
COURSES &
CERTIFICATION
UK/US/GLOBAL

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.

IPS

Web: www.intpro.com

Picture credit: AdobeStock

LET US PRAY

Sukrit Varma, Valerie Lapteva *and* **Eugenia Marina** *investigate how facial recognition technology provides reassurance in places of worship*

In a world where places of worship serve as the beating heart of communities, their significance cannot be overstated. Regardless of the religion being celebrated, sacred spaces are the very basics of spiritual worship and practice. The sacred spaces create unity, offer comfort and also assert the customs for followers. From mosques to churches, temples to synagogues, the security of these places becomes the top priority; it is the fundamental necessity of religious freedoms for fostering communal tranquillity. Hence, this makes it absolutely necessary to manage the complexities of those places of worship so that people are able to worship or just express their spirituality freely without any fear or trepidation.

From cases of vandalism, robbery, religious hate crimes to terrorist attacks, religious institutions worldwide have seen a wide variety of security threats. Such hostilities not only introduce physical danger to the spiritual seekers, but they also disrupt and render such spaces devoid of the peace and harmony they are designed to maintain. One of the potential answers to the problems of security and being able to worship safely comes in the shape of facial recognition technology. By adopting the power of sophisticated algorithms and biometric analysis, the technology brings the possibility of augmenting security measures in a way that would not lead to interferences that might violate the sanctity of the such environments. It has to be appreciated how technology can actually help to create a more peaceful environment within these holy places when it is applied skilfully and responsibly.

Islamic institutions face a higher incidence of burglary

In the past few years, faith communities have been at the intersection of issues that pose a myriad of silting factors that undermine the security and sanctity of these holy places. From cities to the countryside, every religious institution of any denomination, ranging in size and followers, is being traumatised by the simultaneous occurrence of security incidents which supersede geographical boundaries and, instead, transcend religious affiliations.

Occurrences such as destruction of symbols of religion, property and desecrating sacred places leaves worshippers feeling victimised and offended. Likewise, thefts, which target precious religious symbols, artistic pieces or money that has been donated for charity, offer criminals not only material gains, but also – importantly – they affect the trust and goodwill within society.

Globally, trespassing is the main issue that affects temples and gurudwaras. Hinduism also faces issues with burglary, theft, and robbery while Sikhism encounters a significant number of verbal attacks and/or harassment.

However, burglary, theft, and robbery collectively account for crimes in churches, slightly higher than vandalism. In contrast, Islamic institutions face a higher incidence of burglary.

Besides these biased crimes that have been happening within or against religious institutions, the most horrifying are those with an anti-religion slant. Such cruel incidents, the product of prejudice, exclusion and radicalism have cost lives, brought about widespread anxiety and a tangible feeling of uncertainty among worshippers. These attacks are purported by different religious, racial or ideological factors regardless of the place of worship. They are a great threat to religious tolerance and eventually strike at the peace and tranquillity that worshippers seek within their sacred places.

In the Asia-Pacific region, 27 of 50 countries (54 percent) saw religion-related property attacks, while in the Americas, 15 of 35 countries (43 percent) experienced property damage incidents. In the Middle East and North Africa, properties were targeted in 12 of 20 countries (60 percent). These sobering statistics emphasise the urgent need for concerted efforts to uphold and protect religious freedoms worldwide.

During times like religious holidays or special events when overcrowding is commonplace, handling a considerable number of people within a limited space can be difficult. Overcrowding is the cause of the majority of accidents, such as stampedes or falling during pushing and shoving between worshippers. Emotions may become heated, disagreements happen, people argue over sits where or who is standing, and these arguments sometimes end up being the cause of hard feelings and disputes that tend to disturb what is supposed to be a peaceful atmosphere.

Political instability and conflicts have both an added dimension of complexity which reflects even more so in regions where tensions intersect with political turmoil. Places of worship situated at such locations are more vulnerable to security constraints like targeted violence, forced shutdowns and various restrictions from the government. In addition, the violence associated with civil disorder increases another dimension of the insecurity of places of worship. While protests and riots are somewhat expected, in most cases their occurrence is unpredictable and can lead to a disturbance or, worse, chaotic situations.

Where a sense of safety is lacking, there is clearly a need for greater security to protect places of worship and worshippers who overwhelmingly would like to see a range of physical solutions. This includes a strategic deployment of an advanced video management system, which serves a dual purpose. Firstly, it provides extensive surveillance of access points, enhancing situational awareness and threat detection. Secondly, with its capability to capture incidents discreetly, including physical attacks and verbal abuse, the video management system becomes an indispensable tool in preserving the sanctity of these sacred spaces while addressing security concerns.

THERE'S AN URGENT NEED FOR CONCERTED EFFORTS TO UPHOLD AND PROTECT RELIGIOUS FREEDOMS

Nevertheless, the use of facial recognition systems ushers in the inventive surveillance and, to some extent, invasiveness of privacy. The utilisation of such advanced technologies not only enables existing video management systems to know what has been happening, but also puts the identification of persons of interest in a place of prominence, developing the capacity to preempt and deal with any law and order issues. Consequently, the responsiveness of the authorities in this matter is very important in the matter of keeping and guaranteeing the sacredness of these sanctuaries and in improving the general emotional condition of the believers.

In addition to numerous religious institutions, facial recognition technology is now used to ensure security and safety of worshippers. The reasons for implementing the technology may be different but generally involve the worries about increasing insecurity which could manifest as vandalism, theft or may even be a terror act targeting sacred places.

In Singapore, the alarming surge of 11 police reports regarding thefts at places of worship during the first half of 2023, doubling from the previous year, underscores a pressing need for enhanced security measures. Integrating such technology offers a potent solution for securing donation boxes at places of worship, providing an extra layer of protection for these sacred spaces. By integrating facial recognition systems, these institutions can ensure that only authorised personnel have access to the donation box area, thereby minimising the risk of theft or tampering.

Facial recognition systems tailored for use in places of worship boast specific features and capabilities, such as real-time monitoring of entry points, automated identification of suspicious individuals, and integration with existing security infrastructure. This way of implementing a security system in a religious community not only provides the means for enhancing security, but also allows for preserving the holiness and its openness of places of worship.

Facial recognition systems can be applied as an important tool for resolving the crowd problem and processing civil unrest in such places. The authorities can identify hot spots for crowds and predict events that might lead to blockage or congestion with the help of facial recognition systems which provide instantaneous monitoring of crowd flows and crowd densities. Furthermore, these systems have the potential to point out those people most likely to incite violence or cause unrest. This creates an opportunity for targeted interventions, resulting in tension de-escalations and order-restoration.

FACIAL RECOGNITION CAN PREEMPT AND DEAL WITH ANY POTENTIAL LAW AND ORDER ISSUES

Notably, facial recognition technology can also help officers track the path on which individuals in civil disobedience move, identifying and apprehending suspects who cannot stop themselves from breaking into public stores or other criminal acts, ensuring the safety and well-being of worshippers during times of overcrowding and civil unrest.

When all aspects of security seem too big a threat to be overlooked, the combination of facial recognition technology systems with the perimeter intrusion detection can be an incredibly powerful solution. Especially considering such places have transformed into historical landmarks or tourist sites, the conservation strategy offers a sturdy defence against such human activities as well. Imagine this: as an individual approaches the perimeter, the cameras with the facial recognition systems record the face in the blink of an eye. In seconds, the system calculates a matching score and does a global comparison against the database of registered faces to see whether the individual is permitted to be inside. If the system detects an unauthorised presence doing so will send a signal, alerting security personnel or whatever predetermined responses deemed suitable such as alarm activation. Not only does this fusion of technologies make threat identification more exact, but also provides proper and available responses in a short time that guarantee the security and the sanctity of these sacred areas.

Physical security solutions are essential in enabling regular users of places of worship to feel safe, but the aesthetic considerations of such measures are equally important: while on-site security design must serve to keep trespassers out and help prevent crime, it should also be welcoming and instil a sense of ease. There is a fine balance to be struck between effective security and aesthetics.

By fostering ongoing evaluation, community engagement and ethical reflection, religious institutions can harness the potential of facial recognition technology to create safer and more welcoming spaces for worshippers. The objective in the end is to seek the balance between security requirements and the values of an open and inclusive system of the practice of the religion where individual rights are truly respected. Joint efforts and smart decision-making, however, guarantee the technology to be utilised as a tool of divine harmony and spiritual nurturing during worship ●

Sukrit Varma is Global Marketing Partner, APAC & MENA Region at RecFaces.
Valerie Lapteva is Business Development Director, APAC Region, at RecFaces.
Eugenia Marina is Business Development Director, MENA Region, at RecFaces.

Facial recognition systems tailored for use in places of worship boast specific features and capabilities that can integrate with existing security infrastructure

Picture credit: AdobeStock

ELF

Electronic Lens Finder

Electronic Lens Finder & Delivery Set

QCC ELF – Electronic Lens Finder is a device developed and manufactured in the UK, primarily for the detection of covert camera lenses. Simple to operate, the ELF is an essential item not just for TSCM professionals but anyone who has concern over the deployment of covert camera technology.

The ELF system makes use of optical illuminators, that generate a reverse reflection from hidden camera lenses. This reflection, visible as either green or red dots, can be clearly observed through the ELF's dedicated optics, aiding in the accurate identification and location of concealed cameras.

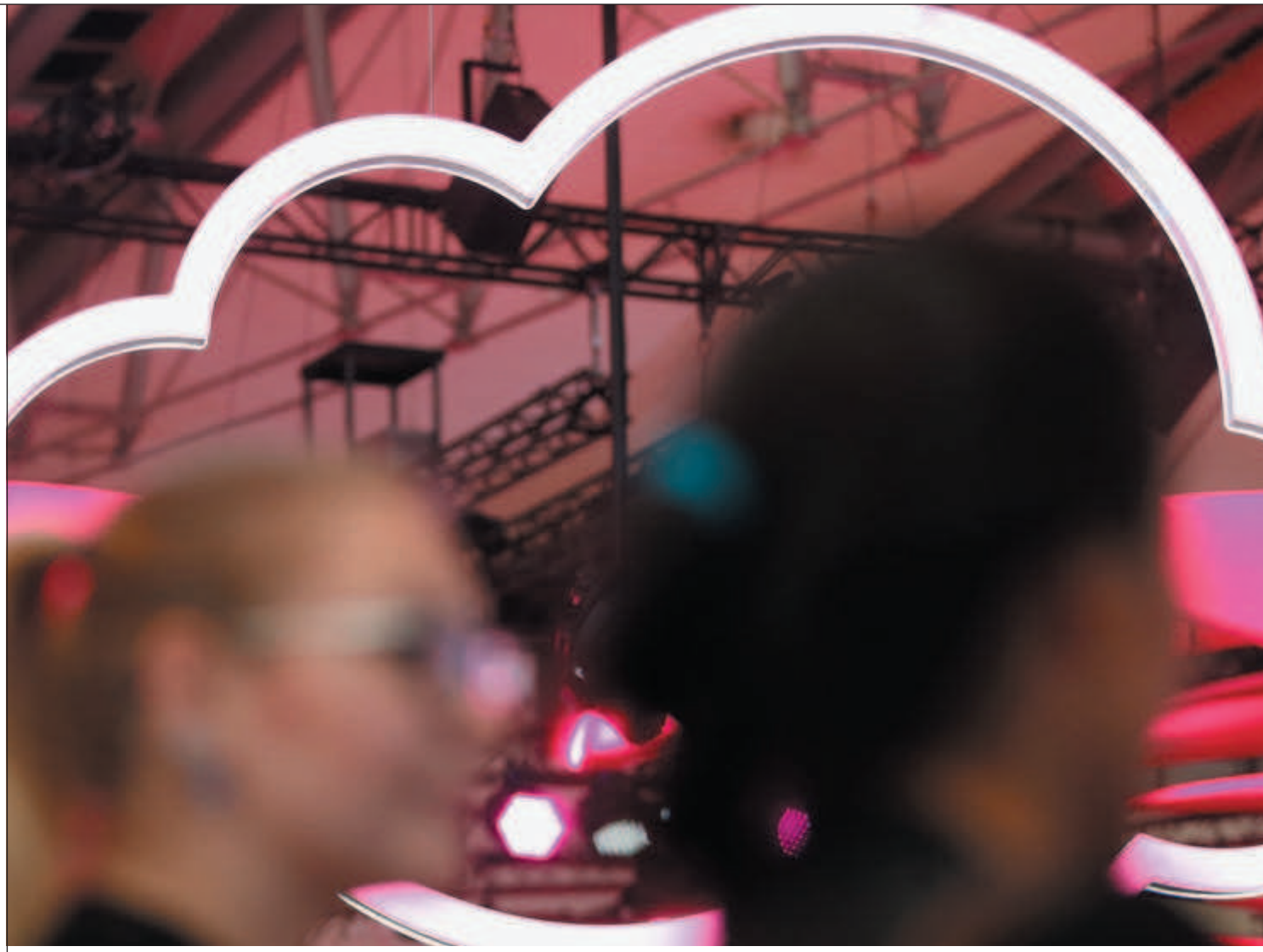
- 1x Worldwide 30W USB charger
- 2x Rechargeable Li-ion batteries
- 1x Multiway charge lead
- 1x Camera lens detector & strap
- 1x Carry pouch with strap
- 1x Custom case & foam inserts
- 1x Operation Manual

LONDON
T: +44 207 205 2100
E: contact@qccglobal.com

SINGAPORE
T: +65 3163 7100
W: www.qccglobal.com

MADE IN BRITAIN

Keeping your business, ***your*** business !



Picture credit: Getty

SKY HIGH

Chris Doman *examines how organisations can respond to evolving threats in the cloud*

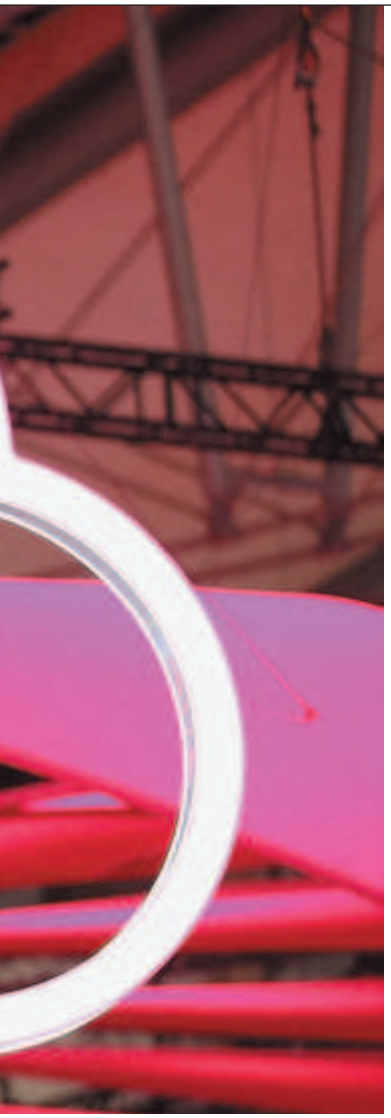
The seismic shift towards cloud migrations has been impossible to ignore. While the pandemic necessitated the adoption of cloud models for many organisations to efficiently accommodate remote workforces, businesses swiftly recognised the benefits that a departure from on-premises setups could offer on a long-term basis.

While the operational advantages are evident, organisations must not overlook the potential security hurdles that can accompany cloud migrations, maintaining a balanced perspective that acknowledges both the vast opportunities and potential challenges.

One of the most obvious benefits of cloud models is that they ensure data accessibility for employees at any time and from any location. In addition to supporting the flexible working models that many organisations have come to rely on, cloud computing supports innovation by simplifying the process of testing new concepts and developing applications. It also provides enhanced flexibility – resources and storage can be swiftly scaled up to meet evolving demands, eliminating the need for substantial investments in on-prem infrastructure.

From speed gains and lower costs, to better scalability and collaboration enhancements, the cloud has become an indispensable tool. According to data cited by Wissen Technology, 61 percent of businesses migrated their workloads to the cloud as a result of the COVID-19 pandemic. And while cloud adoption reached near-ubiquity with 94 percent penetration in 2023, the total spend associated with cloud technologies continues to grow.

Looking ahead, Gartner estimates that worldwide end-user spending on public cloud services will grow 20.4 percent to $678.8-billion in 2024 – up from $563.6-billion in 2023 – as businesses continue to explore the opportunities associated with deepening their cloud-based operations. As their investment in and reliance on cloud services rise, it's crucial



As much as 61 percent of businesses migrated their workloads to the cloud as a result of the COVID-19 pandemic

that organisations do not overlook the associated security implications.

In on-premise environments, safeguarding entry points was a relatively straightforward endeavour. Enterprises had direct physical control over both hardware and software, facilitating direct oversight of potential risks.

In the cloud, however, they are presented with an entirely different challenge. The proliferation of potential vulnerabilities – from cloud misconfigurations and insecure APIs, to zero-day threats and poor access management practices – creates a significantly more complex landscape.

It has been a challenge for many enterprises to secure the rapid migrations they have executed adequately and quickly enough, and attackers are taking full advantage of this. We're also seeing a rise in cloud threats due to the increasing amount of infrastructure being hosted in the environment.

To capitalise on the instabilities of those enterprises that haven't adequately adapted and improved their security practices in line with their cloud migrations, adversaries are developing an increasingly expansive arsenal of attack methods specifically designed to exploit cloud-centric vulnerabilities. In fact, research from Crowdstrike suggests that cloud-based attacks increased by 75 percent in 2023.

Cado Security's most recent Cloud Threat Findings Report delves deeper into this trend, uncovering three principal ways in which cyber criminals are actively targeting enterprises in the cloud.

First, many current malware campaigns are targeting web-facing cloud services such as Docker, Redis, Kubernetes and Jupyter as a means of gaining unauthorised access to their target environments.

Looking at the Qubitstrike campaign that was uncovered in October 2023 as an example, we saw how threat actors worked to exploit a Jupyter Notebook, spawn a Bash terminal using Jupyter's terminal feature and run additional payloads on the underlying host. Furthermore, not only are threat actors using credential exfiltration scripts to hunt for cloud service provider credentials, but they're also seeking to identify and exploit misconfigured service deployments.

Second, threat actors are looking beyond using cloud and Linux-centric campaigns for cryptojacking, diversifying their toolbox of techniques to exploit a wider range of cloud vulnerabilities.

The recent discovery of cloud-centric hack tools such as Legion, Fbot and AndroxGh0st all highlight this shift, the latter having been the subject of an advisory released by the Cybersecurity & Infrastructure Security Agency (CISA). Instead of being centred around cryptojacking, these hack tools seek to automate the hijacking of cloud SMTP services, leveraging their speed and scalability to carry out mass-spamming attacks.

Thirdly, threat actors are also exploiting novel programming languages, resulting in the continued proliferation of Rust malware. In the same way that Rust enables developers to compile services for several operating systems at once, ransomware developers are using cross-platform development support to target Linux systems.

Given that very few malware analysis tools can handle Rust binaries effectively, and very few malware specialists are familiar with the language, the volume of malicious payloads developed in Rust is likely to continue to grow moving forward.

The message comes through loud and clear: as threat actors intensify their cloud-focused assaults, organisations must act decisively to counter this trend through the rapid identification, investigation and containment of threats and attacks.

In this environment, prompt and effective incident response and forensic analysis are essential to the protection of digital assets. Cloud forensics is a field that applies the traditional scientific techniques of digital forensics to attacks in the cloud. This domain can be divided into two primary categories: the forensics of a cloud estate and the forensics of cloud-specific systems and controls.

USING CLOUD FORENSIC PLATFORMS ENABLES PROFESSIONALS TO CURB THE SPREAD OF MALWARE

Done manually, the process involves a heavy burden of data collection and normalisation, before malicious activity can be identified, and the root cause and scope of an incident determined.

It's important to access and investigate both logs and resources. The ability to unearth 'undocumented logs' is really important, for instance, as these often hold essential information and history about activities and incidents within the cloud infrastructure. They sometimes reside in unexpected locations.

Access to the required resources is one of the biggest obstacles here: analysts often have to wait for access to be granted while the attacker runs riot. What's more, data is often distributed across multiple cloud services, making it difficult to capture everything that's required.

Security professionals must also have a solid grasp of the most common anti-forensics techniques used by attackers. One such tactic is log tampering, where an attacker manipulates system logging tools to obscure their actions. Attackers can tamper with log files or forensic artefacts, which allows them to remove entries related to their activities or even insert new events to mislead investigators and waste their time. When done properly, log tampering can keep an intrusion undetected without arousing suspicion.

Lastly, data destruction is a very common technique. Attackers will often delete payloads from the disk following executions, so responders do not have direct access to the malware sample. They will also often shred log files such as bash history or audit logs, eliminating evidence of their actions and making it significantly harder for responders to figure out the attacker's activities on the system.

Inadequate or outdated incident response strategies will give attackers the upper hand and can lead to potential damage. Traditional forensics tools and approaches have made investigation and response strategies overly tedious and complex – especially in cloud environments. Organisations must embrace a modernised approach, taking advantage of cloud automation and data processing technologies and tools. This will lighten the load on analysts' shoulders by simplifying the cloud forensics process, accelerating mean time to response (MTTR) and reducing risk.

Adopting a specialised cloud forensics and incident response platform that provides the right capabilities and incident management tools can pay dividends.

It's crucial that the platform can handle deep datasets. There's a common misconception that cloud forensics revolves solely around log analysis. While logs offer valuable insights, investigations demand a deeper understanding from additional data sources such as disk, network and memory within the infrastructure. Full disk analysis, for example, can supplement log analysis by providing crucial context for identifying the root cause and scope of an incident. Therefore, a holistic approach that integrates diverse data sources is vital.

MANY OF THE CURRENT MALWARE CAMPAIGNS ARE TARGETING WEB-FACING CLOUD SERVICES

A platform must also protect the chain of custody, guaranteeing the integrity of data throughout the investigation of an incident. In complex, multi-cloud environments, preserving unaltered copies of forensic evidence securely is easier said than done. Organisations should look to ensure that any solution can autonomously manage and maintain the chain of custody, recording and safeguarding evidence without human intervention.

Automated data capture across key cloud resources – including virtual machines, containers and serverless functions – will also be highly useful in accelerating the speed at which security teams can respond to an incident. This is especially important in ephemeral environments in which resources are constantly spinning up and down, and where data can simply disappear if it's not captured quickly.

By enabling immediate access to forensic evidence in the cloud, and automating both data collection and system isolation if an event is detected, cloud forensic platforms will equip professionals to curb the spread of malware and limit potential damage while investigations take place. The ability to automatically surface key malicious activities in parallel with a complete timeline of events, meanwhile, will boost both the efficiency of an investigation and accuracy of incident response.

Implementation can also open up the opportunity for parallel data processing, allowing security teams to look at hundreds of systems simultaneously, reducing the time it takes to kick off a deeper dive investigation once something malicious has been identified.

A platform must also be easy to use, streamlining the process rather than adding to the increasing operational pressures security professionals already face.

Cross cloud support will ensure a platform works as intended – even if incidents span several cloud service providers at once. Further, usability features such as an incident dashboard, single timeline evidence view, saved search and faceted search can all be extremely useful, making the navigation of platforms easier. Not only will features such as these help analysts achieve greater efficiency, they will also support novel analysts in undertaking more complex investigations.

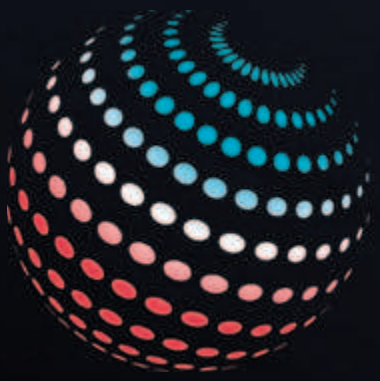
Advanced data forensics and incident response capabilities are more crucial than ever. With threat actors continually developing and enhancing a diverse array of cloud-specific threats, organisations must embrace the tools and solutions needed to modernise their security setups and counter evolving cloud threats.

By helping organisations to navigate the complexities of resource-level cloud forensics and expedite incident response, sophisticated solutions will enable enterprises to stay ahead of attackers and fundamentally reduce their exposure to evolving cloud risks ●

Chris Doman is CTO and co-founder, Cado Security and is well known for building the popular threat intelligence portal ThreatCrowd, which subsequently merged into the AlienVault Open Threat Exchange, later acquired by AT&T.

There is a rise in cloud threats due to the increasing amount of infrastructure being hosted in the environment

Picture credit: AdobeStock



INTERNATIONAL SECURITY EXPO

24-25 SEPT 2024
OLYMPIA, LONDON

CONNECTING THE GLOBAL SECURITY COMMUNITY

Where the world's security leaders & end users come together to discover the latest innovations, learn from leading global industry experts, network and meet with Government.

10,000+
SECURITY DECISION-MAKERS

300+
INTERNATIONAL EXHIBITORS

HIGH-LEVEL
SUMMIT & CONFERENCE

IMMERSIVE
LIVE DEMONSTRATIONS

SCAN TO REGISTER

SECURE YOUR FREE PASS TODAY

internationalsecurityexpo.com

FIRST LINE OF DEFENCE

Alan Stephenson-Brown *reveals the true cost of a weak password and shares best practices to protect businesses*

New laws that came into force as recently as 29 April this year – as part of the Product Security and Telecommunications Infrastructure (PSTI) regime – are a welcome move that should significantly improve the UK's resilience from ongoing cyber attacks. Going forward, manufacturers of all internet-connected devices must implement minimum security standards. This will mean a clampdown on some bad digital habits that too many of us have become guilty of, but which have potentially devastating consequences for businesses.

The laws are coming into force as part of the PSTI regime, which has been designed to improve the UK's resilience from cyber attacks and ensure malign interference does not impact the wider UK and global economy. Manufacturers will be legally required to protect consumers from hackers and cyber criminals from accessing devices with internet or network connectivity – from smartphones to games consoles and connected fridges – as the UK becomes the first country

Manufacturers will be banned from having weak, easily guessable default passwords

in the world to introduce these laws. Under the new regime, manufacturers will be banned from having weak, easily guessable default passwords like 'admin' or '12345' and if there is a common password the user will be promoted to change it on start-up. The move marks a significant step towards boosting the UK's resilience towards cyber crime, as recent figures show 99 percent of UK adults own at least one smart device and UK households own an average of nine connected devices. The new regime will also help give customers confidence in buying and using products, which will in turn help grow businesses and the economy.

All this is intended to increase consumer confidence in the security of the products they buy and use, delivering on one of the government's five priorities to grow the economy. The new laws are part of the government's £2.6-billion National Cyber Strategy to protect and promote the UK online. If successful, the move will help prevent threats such as the Mirai attack in 2016, which saw 300,000 smart products compromised due to weak security features and used to attack major internet platforms and services. Since that incident, which left much of the US East Coast without internet, similar attacks have occurred on UK banks including Lloyds and RBS leading to massive disruption to customers.

Passwords play a crucial role in maintaining the integrity of corporate assets, yet in 2022, more than 24-billion passwords were exposed by hackers and around 80 percent of confirmed breaches are related to stolen, weak or reused passwords. Clearly, robust password policies are critical for ensuring the security of digital assets and accounts. Not only do they make it more difficult for hackers to access accounts, systems and sensitive information, as cyber threats evolve it allows organisations to adapt and respond to new challenges effectively. To fully understand the benefits of such policies, it's helpful to look at the consequences of using weak passwords.

Studies have found the most commonly used passwords in the UK last year were '123456' and 'password', which will now be disallowed thanks to the new legislation. But what's so bad about them? Weak passwords represent a significant security risk, exposing individuals and organisations to various threats, including unauthorised access, data breaches, identity theft, and loss of trust and reputation. Often short or easy to guess, they can be cracked in minutes using methods like credential stuffing. One survey found that 30 percent of respondents – all IT professionals – had experienced a data breach because of a weak password and an additional 23 percent were unsure whether they were involved in a data breach.

Because weak passwords can be easily guessed or cracked by automated tools, they make it easier for attackers to perform account takeover attacks and access to a user's account and misuse it for malicious purposes, such as stealing sensitive information or spreading malware. 560,000 new pieces of malware are detected daily and the first half of 2022 alone saw 236.7-million ransomware attacks globally, with an average cost of $4.54-million per incident. There has been an alarming increase in malware infections over the last decade, a trend set to continue, with the cost of cyber crime predicted to hit $8-trillion in 2023.

Additionally, weak passwords increase the risk of identity theft, where attackers impersonate individuals to access their financial accounts, make transactions or fraudulently apply for loans *etc.*

Approximately 1 in 10 Europeans claim to have recently experienced online identity theft (European Commission) and between $24-million and $55-million is lost annually to card ID theft in the UK (UK Finance). Lesser-known risks include the erosion of trust and damage the reputation of individuals and organisations.

THE PSTI REGIME HAS BEEN DESIGNED TO IMPROVE THE UK'S CYBER ATTACK RESILIENCE

In June 2018, hackers delivered an attack that harvested personal, passport and credit card information for nearly 500,000 British Airways passengers. Besides large fines from Britain's Information Commissioner, BA faced lasting reputational damage after the incident, falling from 31st to 55th in reputation score. This example also demonstrates how non-compliance with existing regulations is also a consequence of a data breach. Many industries have long-standing regulations and standards requiring the implementation of strong password policies to protect sensitive information and maintain data security. Failure to comply with these regulations can result in legal and financial penalties.

Compromised accounts resulting from weak passwords can lead to data breaches, exposing sensitive information such as personal data, financial records or intellectual property, so it's imperative to implement password policies that will protect businesses. Under the new UK law, if a user suggests a common password they will be prompted to change it on creation of a new account. But there are other proactive steps businesses can take.

BEST PASSWORD PRACTICES

Create strong and unique passwords using three random words. The best way to make a password difficult to hack is by using a sequence of three random words that are easy to remember. You can make it even stronger by including special characters and numbers, but don't fall into the trap of thinking that using symbols on short common words, eg "P@$$W0rd1" will make it harder to guess. Alternatively, consider using passphrases, which are longer and easier to remember than traditional passwords.

Whenever possible, enable multi-factor authentication (MFA) for your accounts to add an extra layer of security by requiring additional verification beyond just a password, such as a code sent to your phone or generated by an authenticator app.

Use different unique passwords for every email, social media and banking account. Store passwords in your browser when prompted, or use a password manager; both options are easier than

remembering multiple passwords and safer than re-using passwords. Despite the fact that 91 percent of people say they know reusing the same password or a variation of it is risky, 66 percent still do it at least some of the time, if not all the time. This is why it's crucial for businesses to have guidelines for redundancy outlined in their password policies.

APPROXIMATELY 1 IN 10 EUROPEANS CLAIM TO HAVE EXPERIENCED ONLINE IDENTITY THEFT

Regularly updating passwords is especially important for accounts that contain sensitive information or are critical to business operations. Cyber security experts recommend changing important passwords every three months, but you should change your password immediately if your account is hacked, you're impacted by a data breach in any way, you have used an unsecure network or have discovered malware.

Regularly monitor accounts for any suspicious activity or unauthorised access. Enable notifications for login attempts, password changes and other account-related activities to alert you to any potential security incidents.

ISO 27001, formally known as ISO/IEC 27001:2022, an information security standard created by the International Organisation for Standardisation (ISO), provides a framework and guidelines for establishing, implementing and managing an information security management system (ISMS). According to its documentation, ISO 27001 was developed to: "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system." It includes password requirements that have been established as an international standard, ensuring passwords used by any organisation are strong, secure and regularly updated. Specifically, this standard defines rules and policies for choosing secure passwords and changing them regularly.

Having a standard for information security is no longer an optional extra, every single business or organisation needs a set level of information security. Because the most popular standard of security is ISO 27001, Evolve's approach to implementation has seen all our customers achieve the standard and maintain it. Not having an ISO 27001 Accreditation directly impacts how your customers and stakeholders perceive your business – ISO 27001 shows your customers that you are dedicated to ensuring your business is secure.

Poor password practices are an entirely avoidable mistake that cost businesses dearly every year. An estimated 81 percent of data breaches are caused by poor or reused passwords, and in 2022, the average cost of a data breach for organisations in the US was $9.44-million ($2.98-million for small businesses specifically). Stolen or compromised login credentials have already led to several high-profile data breaches in 2023, impacting businesses like PayPal, MailChimp, Reddit, Activision and others.

By following password best practices, businesses should be able to significantly improve their security posture and reduce the risk of data breaches and other cyber security threats. Moreover, implementing robust password policies demonstrates a commitment to security, which can enhance trust among customers, clients and stakeholders ●

Alan Stephenson-Brown is CEO at Evolve

In 2022 24-billion passwords were exposed by hackers

MCQUEEN TARGETS

LIVE FIREARMS TRAINING TARGETRY

AIM FOR THE BEST.

CIVILAIN TARGETS

MILITARY TARGETS

POLICE TARGETS

THREAT ASSESSMENT

3-D FOAM TARGETS

3-D FOAM ACCESSORIES

Hit the mark every time with

MCQUEEN TARGETS

GALASHIELS, SCOTLAND

info@mcqueentargets.com

+44 (0)1896 664269

mcqueentargets.com

INCIDENT BRIEF

Europe

8 May, Wigan – UK
Two men were arrested over a machine gun terrorism plot to attack Jewish communities in North-West England, as well as police and military targets.

8 May, Berlin – Germany
Germany's chancellor, Olaf Scholz, strongly condemned a rash of separate attacks on four politicians, a senator and a former mayor of Berlin in less than a week.

14 May, Normandy – France
Gunmen attacked a prison van, killing two prison officers and freeing the high-security inmate being transported inside.

14 May, Bedfordshire – UK
A man was arrested on suspicion of possession of articles for terrorist purposes after previously being arrested on 6 May on suspicion of causing explosions likely to endanger life.

15 May, Handlová – Slovakia
Slovakia's Prime Minister, Robert Fico, was shot five times outside the House of Culture while meeting supporters, initially leaving him in critical condition. He has since stabilised and is expected to survive.

17 May, Rouen – France
French police shot dead a man armed with a knife and an iron bar after he set fire to a synagogue in the Normandy city.

18 May, Munich – Germany
Eight climate activists were arrested after causing Munich airport to close, leading to about 60 flight cancellations.

Americas

16 May, California – USA
Authorities successfully rescued a 17-year old girl after she was trafficked to Ventura county from Mexico two months previously and texted 911 for help. In the messages, the girl – who did not know where she and her captor were – was able to identify landmarks and provide other identifiable information.

17 May, Philadelphia – USA
More than a dozen pro-Palestinian activists, including six students at the University of Pennsylvania, were arrested after attempting to occupy a hall on the university campus.

17 May, Chiapas – Mexico
A mayoral candidate and five other people were killed when gunmen opened fire at a campaign rally in the violence-racked Southern state.

17 May, Phoenix– USA
A man suspected of shooting his six-month-old son multiple times after taking the boy and his mother hostage was found dead of an apparent self-inflicted gunshot wound in the rubble of his home after it caught fire during a swat standoff.

30 May, El Salvador
Police arrested seven suspects after stopping a plot to detonate explosives at locations across the country as President Nayib Bukele was inaugurated for a second term.

31 May, USA
Live Nation, the parent company of Ticketmaster, revealed that it had been the victim of a cyber attack that compromised user data after it discovered an: "unauthorised activity within a third-party cloud database," on 20 May.

Asia

4 May, Perth – Australia
Police shot and killed a 16-year-old who attacked a man in a car park. Police said the incident: "certainly has all the hallmarks" of a terrorism-related attack.

17 May, Bamiyan – Afghanistan
Three Spanish tourists and an Afghan civilian were killed in a shooting attack in the central province.

17 May, Brisbane – Australia
A 17-year-old boy was charged with attempted murder after a fight ended in a stabbing in the suburb of Acacia Ridge.

17 May, West Bank – Israel
Israeli jets struck 70 targets across Gaza in 24 hours, while Islam Khamayseh, the leader of the Jenin battalion of Al-Quds Brigade (the armed wing of militant group Palestinian Islamic Jihad), was also killed in a separate airstrike.

17 May, Bamiyan – Afghanistan
Three Spanish tourists and an Afghan civilian were killed in a shooting attack in the central province.

19 May, Sydney – Australia
A police officer was repeatedly stabbed in the head with a 30cm kitchen knife in the business district. He is in a stable condition.

20 May, Ahmedabad – India
Four ISIS terrorists were arrested, days after the city airport received a bomb threat. The Sri Lankan nationals were arrested by the Gujarat Anti-Terrorism Squad after a tip-off.

21 May, Jerusalem – Israel
Police thwarted a planned series of pipe bomb attacks when they arrested four 14-year-old boys plotting attacks against transport vehicles and security forces in the Silwan area.

21 May, Sejong – South Korea
A grenade explosion during army training left one person in cardiac arrest and another hospitalised.

31 May, Colombo – Sri Lanka
Sri Lankan Police arrested the suspected handler of the four ISIS terrorist arrested at Ahmedabad airport, India on the 20 May.

Africa

4 May, Goma – Congo
Bomb attacks on two camps for displaced people near the Eastern city killed at least 12 people, including children. A rebel group known as M23 is understood to be responsible.

4 May, Morocco
Moroccan police arrested five people in a major counter terrorism operation connected to Islamic State. The suspects, aged between 22 and 46, were apprehended in Casablanca, Tangier, Tetouan and Essaouira.

6 May, Mogadishu– Somalia
A suicide bomber rammed a car laden with explosives into a cafe killing eight people. The attack was claimed by Islamist militant group al-Shabaab.

7 May, Olievenhoutbosch – South Africa
Political party ActionSA's Gauteng chairperson and Youth leader survived a kidnapping ordeal after their Toyota Hilux was hijacked. They were found in nearby Benoni around midnight and were not physically harmed.

18 May, Circle of Bankass – Mali
More than 20 civilians were killed when insurgents targeted the village in the Mopti region.

19 May, Kinshasa – Democratic Republic of Congo
The leader of an attempted coup was killed and around 50 people including three American citizens arrested by the army.

21 May, Sambisa Forest – Nigeria
Nigerian military forces rescued 209 children, 135 women and six men from Boko Haram. Many of the hostages had been held captive by the terrorists for years.

24 May, Niger – Nigeria
Ten people were killed and 160 other villagers kidnapped from a remote community in the village of Kuchi. A large number of armed men, suspected to be Boko Haram, was responsible.

24 May, Eritrea
A massive cyber attack hit the country's internet system, but was foiled by defensive counter measures.

NEWS

Europe

UK given stark warning over 'negligible' air defence systems

Britain's air defence systems are "very limited, to the point of being negligible", a key defence contractor has claimed, as the Ministry of Defence warned of the gravest risk of attack from the skies in 30 years. Northrop Grumman UK, a provider of defence technology to the RAF and Royal Navy, offered its assessment in response to questioning by a parliamentary committee examining lessons to be learned from the war in Ukraine. Asked whether there was a need for increased investment in integrated air and missile defence, the company said Britain's lack of capacity was a major risk to national security. "Current capabilities are very limited, to the point of being negligible, which is the result of long-term under investment and an over reliance on Nato partners' capabilities," the company said. "This capability gap poses a significant risk to national security and the war demonstrates why IAMD is now a critical requirement." The intervention ranks among the starkest of public assessments of Britain's state of readiness by an organisation with intimate knowledge of the country's defence capabilities.

Director of GCHQ: Russia directing hackers to attack UK

Russia is increasingly seeking to encourage and direct hackers to attack British and other Western targets, the director of GCHQ said in her first keynote speech as head of the British intelligence agency. Anne Keast-Butler said her agency was "increasingly concerned about growing links" between the Russian intelligence services and proxy hacker groups who have long taken advantage of a permissive environment within the country. "Before, Russia simply created the right environments for these groups to operate but now they're nurturing and inspiring these non-state cyber actors," she said in what she described as a "globally pervasive" threat. The spy chief referenced the threat from ransomware as "the most acute and pervasive cyber threat" and said GCHQ is "doing everything we can" to counter ransomware actors. GCHQ's public-facing internet security arm, the National Cyber Security Centre (NCSC), published a guide in late May in conjunction with three insurance trade bodies to persuade businesses not to pay the ransoms that fund Russian and other hackers. Felicity Oswald, the interim CEO of the NCSC, said it was: "a dangerous misconception that paying a ransom guarantees the end of an incident".

German coup plot trial begins

The trial of a group of far-right conspiracists who plotted to violently overthrow the German state is taking place in Frankfurt amid high security and huge media interest. On trial are the group's alleged ringleader, Prince Heinrich XIII, his Russian girlfriend, and seven other founding members including a former policeman and a former judge who is now an MP for the far-right AfD party. According to prosecutors, the group planned to storm the Reichstag in Berlin with armed support via its paramilitary wing, to arrest members of the Bundestag and to parade a shackled Olaf Scholz on German television in the hope and expectation of winning ordinary Germans around to their coup. In the event of the group's success, Heinrich, 72, was expecting to become the new chancellor of Germany. The group is part of a growing movement known as Reichsbürger, or citizens of the Reich who refuse to acknowledge the legitimacy of the modern German state and would like German borders to be redrawn to pre-1918 lines.

Inmates dug through Winchester prison walls with plastic cutlery

The latest annual assessment from the independent monitoring boards (IMBs), which audit prisoner treatment, has revealed that one in 10 prisons in England and Wales are barely fit for purpose. "At Winchester, there were several occasions throughout the year where prisoners were able to damage and attempt to dig through cell walls, on one occasion through the wall to the landing, using simple implements such as plastic cutlery," it noted. Last year, the chief inspector of prisons, Charlie Taylor, noted that about 14 Victorian jails were so poorly designed, overcrowded and ill-equipped that they could not provide proper accommodation for inmates.

UK police could get 'backpacks' to halt ebike getaways

Police officers in Britain could be armed with backpack-style devices that fire electromagnetic rays to shut down the engines of ebikes being used in a crime. Gavin Stephens, chair of the National Police Chiefs' Council (NPCC), said the weapon was in development and could be months away from being available, though it is expected to be longer than that. He said it would be housed in a backpack and designed to tackle crime linked to newer vehicles such as electric bikes and electric scooters. The device is being developed with the Defence Science and Technology Lab, which is overseen by the Ministry of Defence, alongside other technological innovations that British police are hoping to use. It fires an electromagnetic pulse at a vehicle that an officer wants to stop and tricks the engine into thinking it is overheating, which shuts it down and brings the vehicle to a stop. It requires a line of sight to work. Though E-scooters and ebikes are potentially an environmentally friendly way to travel, they are being increasingly used in thousands of crimes. They are fast and nimble, so for instance a rider can jump on to pavements to snatch a mobile phone and then make a quick getaway.

NEWS

Americas

Illegal immigration creates "high threat" for US terrorist attack

America is facing a high threat level for a terrorist attack because of the crisis at the Southern border, says the head of a group working to curb illegal immigration. Julie Kirchner, executive director for the Federation for American Immigration Reform observed: "It does not take a lot of people to inflict an extraordinary amount of damage," and noted that more incidents are happening across America that should raise alarm bells over the threat illegal immigration poses to the safety of the nation. At the beginning of May two Jordanian illegal aliens attempted to breach a US military base in Quantico, Virginia. One of the men is reported to have crossed the Southern border in April and another overstayed a student visa. The two men tried to drive onto the base "and only due to the quick thinking of some of these guards were they stopped". After more than 10-million illegal aliens have crossed the US border under President Joe Biden, the administration has indicated Biden plans to issue an executive order on the border.

Trump supporters call for riots and violent retribution

Following former president Donald Trump's conviction on 34 felony counts by a New York jury, pro-Trump websites were flooded with calls for riots, revolution and violent retribution. After Trump became the first US president to be convicted of a crime, his supporters responded with dozens of violent online posts, according to a Reuters review of comments on three Trump-aligned websites: the former president's own Truth Social platform, Patriots.Win and the Gateway Pundit. Some called for attacks on jurors, the execution of the judge – Justice Juan Merchan – or outright civil war and armed insurrection. Threats of violence and intimidating rhetoric soared after Trump lost the 2020 election and falsely claimed the vote was stolen. As he campaigns for a second White House term, Trump has baselessly cast the judges and prosecutors in his trials as corrupt tools of the Biden administration, intent on sabotaging his White House bid. His loyalists have responded with a campaign of threats and intimidation targeting judges and court officials. Sentencing is set for 11 July, days before the Republican Party is scheduled to formally nominate Trump for president ahead of the November election.

Violence intensifies as FARC group attacks police and military

Violence intensified in South-Western Colombia in mid-May when a bomb blast injured six people in the city of Jamundi and an attack by insurgents on a police station in the rural town of Morales left two officers dead. Colombia's government attributed the attacks to the FARC-EMC a rebel group that broke off from the Revolutionary Armed Forces of Colombia and refused to sign a 2016 peace deal in which more than 14,000 rebels demobilised. The group's western faction walked away from a new round of peace talks with the government in April and has since staged a series of attacks on military and police, including a roadside bomb in mid-May that killed an 11-year-old. Elizabeth Dickinson, a Colombia analyst at the International Crisis Group, said the attacks show that the EMC's Western faction is trying to set itself apart by becoming "the only armed or criminal group in Colombia that is directly attacking the state." Dickinson said the FARC-EMC's Western front, which is led by commander Ivan Mordisco, could end up splitting from EMC groups in Eastern Colombia that are still involved in peace talks with the government.

US/Russia space weapons clash

The United States claimed that Russia launched a satellite that could be part of weaponising space in mid-May – a possible future global trend that members of the United Nations Security Council condemned even as they failed to pass a measure against it. The Security Council resolution drafted by Russia rivalled one backed by the US and Japan that failed in April. The rival drafts focused on different types of weapons, with the US and Japan specifying weapons of mass destruction. The Russian draft discussed all types of weapons. Russia's UN ambassador, Vassily Nebenzia, denied that his nation was trying to mislead the world. Backed by China and others, he called the vote: "a unique moment of truth for our Western colleagues," before adding: "If they fail to support this, then they will clearly show that their main priority remains keeping freedom of the way for themselves to expedite the militarisation of outer space."

State Department warns of terrorist attacks at Pride events

The US State Department has issued a global security alert warning Americans abroad that terrorists could target lesbian, gay, bisexual, transgender and queer people at LGBTQ-related events during Pride Month. Due to the potential for terrorist attacks, demonstrations or violent actions against US citizens and interests, the Department of State advises United States citizens overseas to exercise increased caution," the warning reads. Officials advised Americans abroad to stay alert in tourism districts, at Pride events and in venues frequented by LGBTQ people. They added that before travelling overseas, Americans should enrol in the State Department's Smart Traveler Enrollment Program to receive alerts from the department and to make it easier for officials to locate Americans in emergency scenarios. Authorities did not specify if there are any countries or regions of the world that are of particular concern and did not name any terrorist organisations suspected of planning attacks.

NEWS

Asia

Engineering firm falls victim to £20-million deepfake scam

The British engineering company Arup has confirmed it was the victim of a deepfake fraud after an employee was duped into sending HK$200-million (£20 million) to criminals by an artificial intelligence-generated video call. Hong Kong police said in February that a worker at a then-unnamed company had been tricked into transferring vast sums by people on a hoax call "posing as senior officers of the company". Arup said in a statement that it was the company involved, confirming that at the beginning of the year it had: "notified the police about an incident of fraud in Hong Kong". It confirmed that fake voices and images were used. It added: "Our financial stability and business operations were not affected and none of our internal systems were compromised". Arup's global chief information officer, Rob Greig, who oversees the company's computer systems, said the organisation has been subject to frequent attacks including deepfakes: "Like many other businesses around the globe, our operations are subject to regular attacks, including invoice fraud, phishing scams, WhatsApp voice spoofing and deepfakes. What we have seen is that the number and sophistication of these attacks has been rising sharply in recent months." Arup is one of the world's leading consulting engineering firms and employs more than 18,000 people.

China accelerates naval modernisation

China has unveiled its inaugural drone carrier in response to heightened tensions and evolving geopolitical dynamics in the Asia-Pacific region. This marks a significant stride in its ambitious military modernisation efforts, reflecting its commitment to bolstering naval prowess. With a focus on enhancing maritime surveillance and asserting dominance in contested areas like the South China Sea, this strategic move aims to safeguard China's regional interests, according to analytics company GlobalData. GlobalData's *Global Naval Vessels and Surface Combatants Market Forecast 2024-2034* report reveals that China will be spending about $46.2-billion on procuring various naval vessels over the next 10 years. Out of which, 8.5 percent will be directed towards amphibious vessels, which includes the drone carrier. Harsh Deshmukh, Aerospace & Defence Analyst at GlobalData, comments: The growing US assistance to Taiwan and escalating territorial disputes with its neighbours in the South China Sea have long been an irritant for Chinese policymakers. In response, China is advancing its naval capabilities with the introduction of dedicated drone carriers, following the deployment of fixed-wing aircraft as well as helicopters in recent years."

Smart Axiata debuts global standard security solutions

Cambodian mobile network operator Smart Axiata launched its Next Generation Signalling Firewall (NGSF) and Intrusion Detection System (IDS) in collaboration with global telecom cyber security firm SecurityGen. The systems mark a significant milestone in Smart's ongoing efforts to safeguard its network infrastructure and protect customer data. The NGSF serves as a bastion of network security, ensuring comprehensive protection for voice and data services. By thoroughly inspecting the signalling controls for voice calls, data sessions and internet connectivity, the NGSF provides protocol-level inspection and intrusion prevention capabilities. Collaborating with SecurityGen, Smart has implemented a robust system that fortifies its subscribers against potentially advanced threats from anywhere around the globe.

Ex-Royal Marine charged with spying for Hong Kong dies

A former Royal Marine commando who was charged with spying for the Hong Kong intelligence service was found dead by a member of the public in a park near where he lived in Maidenhead, Berkshire. A Home Office immigration officer, 37-year-old Matthew Trickett appeared in court along with two other men in mid-May accused of monitoring, surveillance and harassment of pro-democracy activists in the UK. Trickett, Chung Biu Yuen, 63 and Chi Leung "Peter" Wai, 38, were charged with unlawfully assisting the Hong Kong intelligence service and engaging in foreign interference by forcing entry into a British address. Thames Valley police detectives are continuing to investigate if there was anyone else involved in the death.

Chinese network behind one of world's 'largest online scams'

More than 800,000 people in Europe and the US have been duped into sharing card details and other sensitive personal data with a vast network of fake online designer shops operated from China. An international joint investigation by British, German and French newspapers *The Guardian*, *Die Zeit* and *Le Monde* revealed that some 76,000 fake websites were created offering discounted goods from Dior, Nike, Lacoste, Hugo Boss, Versace, Prada and many other premium brands. Published in multiple languages from English to German, French, Spanish, Swedish and Italian, the websites appear to have been set up to lure shoppers into parting with money and sensitive personal data. So far, an estimated 800,000 people, almost all of them in Europe and the US, have shared email addresses, with 476,000 of them having given over debit and credit card details, including their three-digit security number. All of them also handed over their names, phone numbers, email and postal addresses to the network.

ATG

PROTECTING WHAT MATTERS

Crash Rated Solutions

ATG Access designs and manufacturers a wide range of innovative, intelligent physical security solutions to protect critical national infrastructure and crowded places around the world. Keeping people and places safe from hostile vehicle attacks.

ATG ACCESS
PROTECTING WHAT MATTERS

W: www.atgaccess.com | **E:** sales@atgaccess.com

NEWS

Africa

Firm to train 1000 entrepreneurs and students on AI security

Africa Cyber Security and the AI Foundation (ACAIF) is targeting to train 1,000 entrepreneurs across Africa, including 200 from Kenya, in a cyber challenge as it aims to increase the uptake of Artificial Intelligence in small, medium and large business enterprises. ACAIF chairperson Evalyn Oloo made the revelation during the Acyberschool Advanced Cybersecurity Fellowship (AACF) and Cybersecurity and AI Acceleration Program (CAAP) seminar at the University of Nairobi's Chiromo Campus in late May. As part of the programme, students pursuing cyber security and AI will get a one-year fellowship grant to enhance their skills and create more jobs in the sector. "As a foundation, what we are doing across the continent is capacity building and connecting that capacity to meaningful engagements. We have training in terms of scaling individuals who are able to support institutions to better their cyber security posture. We are also equipping individuals with skills to protect themselves while transacting, engaging online or taking advantage of the digital economy that is currently growing in Africa. So the challenge is what we have launched today," Oloo announced.

US military completes major exercise in Africa

High-ranking military officials from the US and its top African allies came together during African Lion, the United States' largest annual joint military exercise on the continent, which concluded at the end of May in Morocco. Over the previous two weeks, around 8,100 military forces manoeuvred throughout Tunisia, Ghana, Senegal and Morocco as part of the war games held this year as militaries confront new challenges in increasingly volatile regions. Generals from the US and Morocco, which hosted the finale of the two-week event, celebrated African Lion's 20-year anniversary and how partnerships between the US and African militaries have expanded since it began. "This exercise has grown over the years since 2004, not only have the number of multinational service members that we train with, but also the scope of the training as well, which has expanded to more than just security," said Gen. Michael Langley, the head of the United States' Africa Command. The US military showcased part of what it offers countries facing instability inside and just beyond their borders. Besides tanks and bombers, the joint exercises included operations and practice in field hospitals, medical evacuations and humanitarian assistance. The exercise emphasised a "whole of government" approach to addressing the root causes of instability, ranging from climate change to displacement, rather than solely focusing on military might.

Lagos State government launches cyber security project

The Lagos State government, through the Ministry of Innovation, Science and Technology (MIST), has launched its cyber security project designed to safeguard the State's digital infrastructure against potential attacks that are becoming rampant. The cyber security project involves partnerships with leading cyber security firms and international organisations, and the collaborations will provide the state with access to cutting-edge technologies and expertise, enhancing its capacity to defend against sophisticated cyber threats. The Lagos State Commissioner for Science, Innovation and Technology – Mr. Olatunbosun Alake – revealed that the cyber security project is part of a broader strategy to improve overall security and governance within the state and that Lagos is also pushing for a State Innovation Bill through which it can implement policies and laws that improve the development of technology. If passed into law, the Innovation Bill seeks to create incentive packages for technology companies registered in the State that will enable them to grow and drive technology development in Lagos.

Africa Cloud & Security Roadshow launches In Tanzania

Industry leaders, policy makers, and cloud and cyber security professionals converged in Dar es Salaam, Tanzania, in late May for the Africa Cloud & Security Roadshow. Organised for the first time in Tanzania by dx5, Africa's technology driver, and powered by BUI East Africa – an award-winning global technology consultancy and managed services provider specialising in cloud, security and networking solutions – the roadshow is a series of events dedicated to advancing the technological landscape of East Africa. Among the major topics of discussion were Risk Management in Cyber Security, Artificial Intelligence (AI) and Machine Learning in Cloud Computing, Navigating Cloud Migration, The Future of Cyber Security, Cloud Infrastructure and Management, and Cyber Security Leadership. These topics were tackled by various thought leaders and experts from across the continent.

Kenya public hearings into alleged abuses by UK troops

Kenya has launched public hearings into allegations of human rights violations and abuses of power by British troops based in the central town of Nanyuki. The British Army Training Unit Kenya (Batuk) maintains a permanent base there and soldiers have been accused of committing offences including murder. In the most high-profile case dating back to 2012, the body of a young Kenyan mother was found in a septic tank having been last seen alive with a British soldier. The sessions investigated allegations of human rights violations, including mistreatment, torture, unlawful detention and killings. The case is due to be heard on 10 July.

DIARY DATES

2024 Conference and Exhibition planner

17-21 June
Eurosatory 2024
Paris, France
Organiser: Defence and Security
Tel: +33 (0)1 80 92 71 48
Email:helpdesksupport@eurosatory.com
www.eurosatory.com/en/

17-20 September
Security
Essen 2024
Essen, Germany
Organiser: Messe Essen
Tel: +49.(0) 201 7244-0
www.security-essen.de

24-25 September
International Security
Expo 2024
London, UK
Organiser: 19 Events
Tel: +44 (0)20 8947 9177
Email: info@internationalsecurityexpo.com
www.internationalsecurityexpo.com

1-2 October Cyber Security
& Cloud Expo 2024
Amsterdam, Netherlands
Organiser: TechEx Media Ltd
Tel: (+44) 1628 947 727
Email: admin@techex.co.uk
www.cybersecuritycloudexpo.com/europe

9-10 October International
Conference on Digital Forensics
& Cyber Crime 2024
Dubrovnik, Croatia
Organiser: European Alliance for Innovation
Tel: +42 1 911 111 156
Email: contact@eai.eu
www.icdf2c.eai-conferences.org/2024/

16-17 October Global Airports
& Aviation Forum 2024
Saudi Arabia
Organiser: Fair Exhibition Organizers
Tel: +966 (0) 56 127 7177
Email: ceo@gaaf2024.com
www.gaaf2024.com

8 November Close Protection
and Security Conference 2024
London, UK
Organiser:Close protection World Events
Tel: +44 (0) 7515 526209
www.events.closeprotectionworld.com/
homepage/

19-21 November
ISC East 2024
New York, USA
Organiser: The Security Industry Association
Tel: +1 203 840 5602
Email: inquiry@isc.reedexpo.com
www.discoverisc.com/east/en-us.html

19-21 November
MAST Australia 2024
Adelaide, Australia
Organiser: MAST. Tel: +44 7411 732978
Email:admin@mastconfex.org.
www.mastconfex.com

HEALD®

DESIGNERS, MANUFACTURERS AND INSTALLERS OF AWARD WINNING PERIMETER SECURITY PRODUCTS

Secured by Design

Official Police Security Initiative

PSSA

Perimeter Security Suppliers Association

SafePQQ VERIFIED

OSPA WINNER 2022

Outstanding Security Equipment Manufacturer

MADE IN BRITAIN

Constructionline

Gold Member

SafeContractor APPROVED

+44 (0)1964 535858 info@heald.uk.com www.heald.uk.com

Heald Ltd, Northfield, Atwick Road, Hornsea, United Kingdom, HU18 1EL

@healduk Heald Ltd Heald Ltd HealdLtd

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

Allegion Schlage XE360 Series wireless locks

Allegion has introduced its Schlage XE360 Series wireless locks, a new electronic lock portfolio designed with multifamily market needs in mind.

With modern lever styles, the XE360 Series operates in an offline or No-Tour environment, which eliminates the need for property managers to visit the lock as credentials update access rights. The XE360 Series integrates with Schlage Control mobile-enabled smart locks and features applications across the entire building. The XE360 Series' open architecture design provides property owners and operators the flexibility to choose between management systems and supports MIFARE, Bluetooth and NFC mobile, with advanced encryption to keep data and communications safe. The new FleX Module board allows locks to be easily upgraded in the field to allow migration from an offline to networked solution and adapt to emerging trends in security and connectivity as the building's needs or technology change.

QinetiQ achieves UK first jet-to-jet teaming

QinetiQ has successfully trialed the UK's first Crewed-Uncrewed-Teaming demonstration between a crewed aircraft and autonomous jet drone. The trial saw a QinetiQ jet aircraft take off Boscombe Down in Salisbury, while a modified Banshee Jet 80 drone was launched from MOD Hebrides, Scotland. Flying from Boscombe to the Hebrides, the aircraft soon gained control of the Banshee, with the drone receiving its orders from the aircraft before automatically conducting the mission assignment, flying at 350 knots. The mission was also completed by a number of digital Banshees within a live-virtual swarm, successfully acting in a co-ordinated manner. In-built safety systems can override the autonomy to ensure the drone stays at all times within a safe operating area.

BQT Solutions unveils Bluetooth-enabled YG80 lock

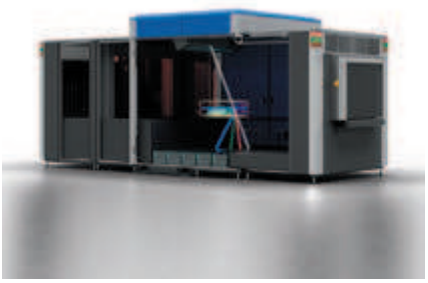
BQT Solutions unveiled the Bluetooth-enabled version of its YG80 industrial lock at ISC West 2024. Equipped with built-in Bluetooth, the YG80B can be installed within a facility, ensuring it remains out of reach from potential attacks while still allowing convenient and secure operation from a smartphone. The YG80B features a UV- resistant lid and a built-in heater, making it well-suited for challenging environmental conditions. The motor-driven, high strength lock includes additional features including user-selected fail safe/fail secure operation, multiple attempts to lock/unlock and the option to hardwire the YG80B into the facility's physical access control system. Exceeding the highest UL 1034 strength standards the 18mm stainless steel bolt pin and reinforced strike also feature concealed mounting bolts to eliminate attack points.

Apricorn introduces 24TB hardware-encrypted USB drive

Apricorn has announced the release of a 24TB version of its Aegis Padlock DT and Padlock DT FIPS Desktop Drives. The manufacturer is the first to bring a 24TB encrypted drive to market, having previously introduced the 20TB and 22TB devices. Both drives come with AegisWare, the proprietary firmware and feature set unique to Apricorn's Aegis Secure Drives and Secure Keys. Passwords and commands are entered by way of the device's on-board keypad, while all authentication and encryption processes take place within the device itself and never involve software or share critical security parameters with the host computer. Additionally, all have military grade 256-bit AES XTS encryption so firmware is locked down and can't be updated or modified, defending against malware and ensuring data remains secure and accessible only by the user.

Smiths Detection launches X-ray Diffraction scanner

Smiths Detection has unveiled the SDX 10060 XDi, a ground-breaking X-ray scanner powered by diffraction technology. X-ray Diffraction (XRD) is a powerful inspection technology offering highly accurate material discrimination and substance identification based on an object's molecular structure. It is particularly suited to detecting constantly evolving compounds in powder, liquid or solid forms, such as 'homemade' explosives or narcotics, even for materials with similar densities. Due to its exceptional sensitivity, XRD technology can also be effectively deployed to support customs agencies in screening for a range of contraband items including narcotics. The SDX 10060 XDi can integrate seamlessly with existing material and baggage handling systems and is designed to meet ECAC Standard 3.1/3.2 and TSA 7.2 plus future regulations. Certification is underway.



Hanwha Vision launches AI PTZ Plus cameras

Hanwha Vision has unveiled two new AI PTZ Plus cameras, the XNP-C9310R and XNP-C7310R. These leverage AI for rapid zoom and focus to enable greater situational awareness and quicker response times. Quick Zoom is a fast zoom movement, powered by an AI engine, that enables operators to rapidly see specific details of an unfolding event, which is particularly helpful in high-traffic areas - for example within cities, or during large public gatherings. Quick Focus complements this, using AI and pre-stored information to provide faster auto focus of a frame. When a face, person or object is detected, the camera automatically calculates the distance between the device and object, to rapidly adjust the focus and provide clear images. AI-powered video analytics, carried out on the camera itself, improves operational efficiency and enables rapid forensic search through accurate object detection and classification (of people, faces, licence plates, and vehicles).

ATG ACCESS
PROTECTING WHAT MATTERS

BEAUTIFULLY SECURE

Pedestrianised spaces and placemaking concepts have increased in popularity across the world. This provides an opportunity to rethink urban spaces and to get the balance right between security and aesthetics.

For crash tested product solutions to help you bridge the gap between security and aesthetics visit the ATG Access Website:

W: www.atgaccess.com | **E:** sales@atgaccess.com

Milipol
QATAR

Milipol Qatar 2024

وزارة الداخليـــــــة
Ministry of Interior
State of Qatar • دولـــة قطـــر

@milipolqatar
www.milipolqatar.com