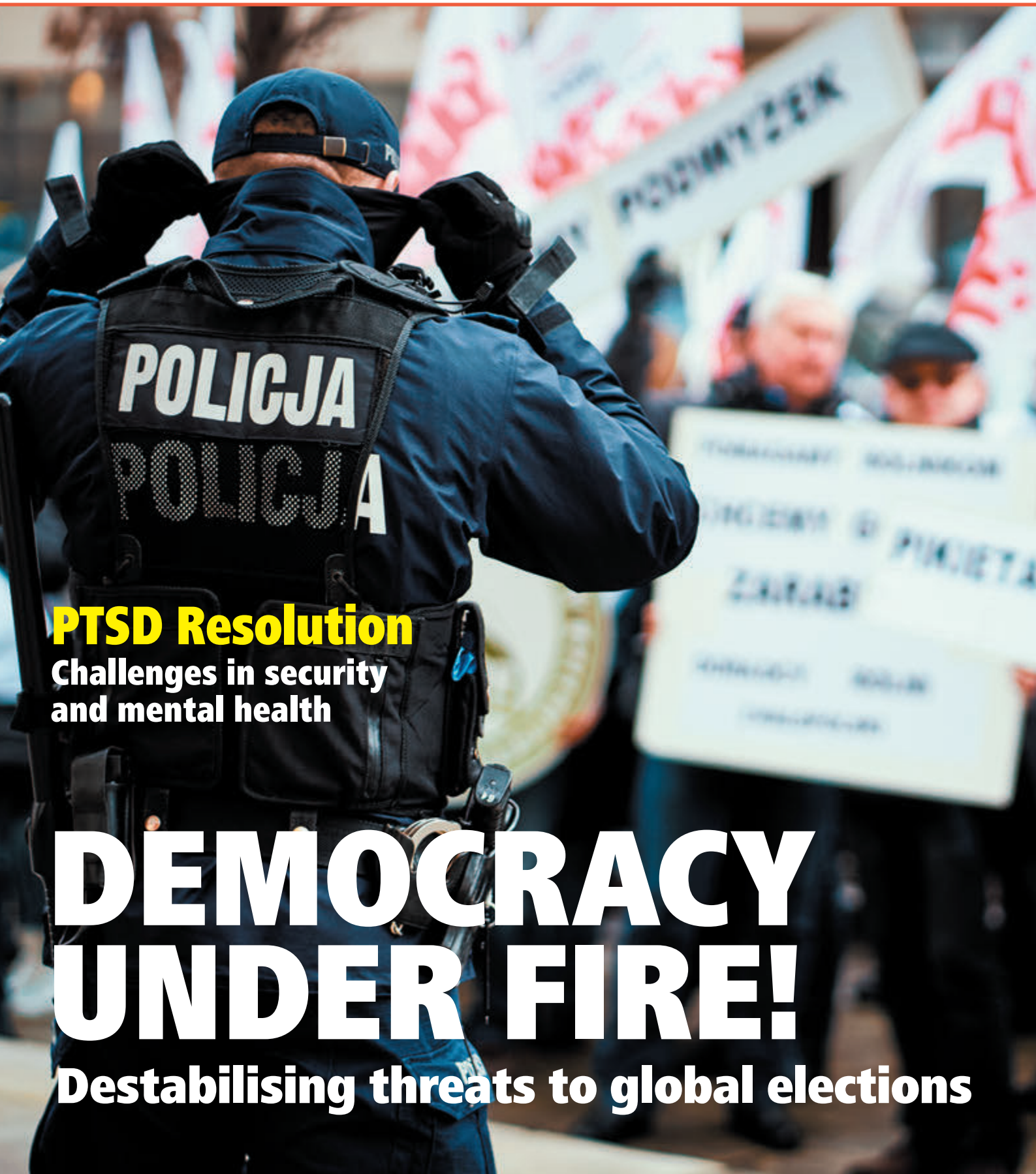
www.intersec.co.uk

intersec

The Journal of International Security

March 2024



PTSD Resolution

Challenges in security and mental health

DEMOCRACY UNDER FIRE!

Destabilising threats to global elections

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 03
March 2024

Picture credit: AdobeStock

Editor
Jacob Charles

Principal Consultant Editor
Maj. Gen.
Julian Thompson CB OBE

International Arctic Correspondent
Barry Scott Zellen

Design & Production
jellymediauk.com

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

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

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

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

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

EDITORIAL COMMENT

Produced by international think tank the Institute for Economics & Peace, The Global Terrorism Index has been published annually for the last 24 years and is widely considered as the most comprehensive resource on global terrorism trends. Using multiple factors to calculate its score – including the number of incidents, fatalities, injuries and hostages, combined with conflict and socio-economic data – it provides a holistic picture of terrorism. The 2024 report has recently been published and makes for fascinating reading.

It probably will comes as no great surprise to learn that the Index highlights that terrorism remains a serious global threat, with total deaths from terrorism increasing by 22 percent to 8,352 in 2023 – the highest since 2017. Even excluding the Hamas attacks of 7 October, deaths would still have increased by 5 percent. This is despite terrorist incidents decreasing by 22 percent to 3,350, resulting in a 56 percent increase in the average number of people killed per attack – the worst rate in almost ten years.

Burkina Faso suffered the biggest impact from terrorism in 2023, with deaths increasing by 68 percent despite attacks decreasing by 17 percent. Terrorism in the country has deteriorated every year since 2014. Neighbouring Mali and Niger were also deeply impacted in 2023.

Pakistan recorded the most incidents of any country, with 490 attacks that resulted in 689 deaths. This is the fourth successive year where both deaths and incidents have increased in the country. Iraq recorded the largest improvement in the last decade with deaths from terrorism falling by 99 percent since its peak in 2007, to 69 in 2023.
The deadliest terrorist incident in 2023 was the aforementioned Hamas-led attack in Israel, which killed 1,200 people. Its consequences are still unfolding, with more than 30,000 Palestinians killed from Israel's military operation by mid-February this year.

However, terrorism was not revealed to be the deadliest form of violence in the world. Armed conflict results in nine times more fatalities, homicide over 45 times more and deaths from suicide 72 times higher.

Terrorism incidents in Western democracies recorded a drop of 55 percent compared with the previous year. There were 23 attacks, resulting in 21 fatalities, marking a 15-year low. However, the US recorded 76 percent of these fatalities from seven attacks. Five of these were linked to individuals with far-right beliefs, while religiously motivated attacks dropped significantly.

Sub-Saharan Africa, the Middle East and North Africa (MENA), and South Asia accounted for 94 percent of deaths from terrorism in 2023, with sub-Saharan Africa alone accounting for just under 59 percent of all fatalities. The Sahel accounts for almost half of all deaths from terrorism globally. The impact of terrorism has been falling in MENA since its 2016 peak, with deaths down 66 percent and incidents by 72 percent.

IS and its affiliates remain the world's deadliest terrorist group, responsible for 1,636 deaths, despite its attributed deaths falling by 17 percent. IS was followed by Hamas, JNIM, and al-Shabaab. Together, they were responsible for over 75 percent of terrorism-related deaths globally. In an indication of how the landscape is changing, a decade ago they were responsible for less than 25 percent.

Jacob Charles, editor

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: March 2024

CONTENTS

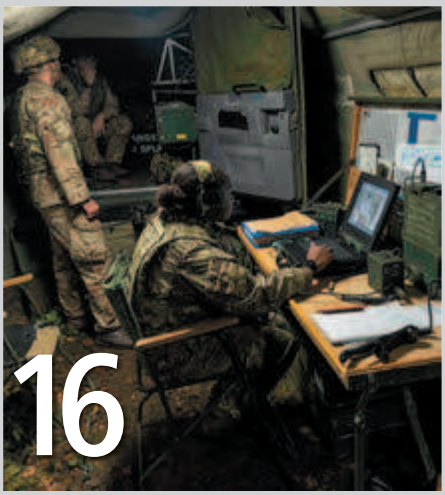
March 2024

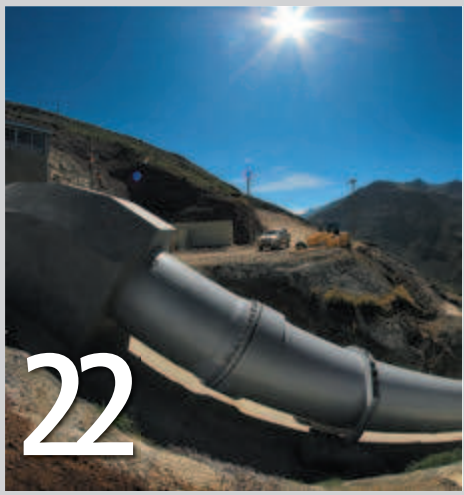
www.intersec.co.uk

intersec

Features

Regulars





Identify yourself

Dr Mark Deakes *considers the role holography plays in securing government ID documents.*

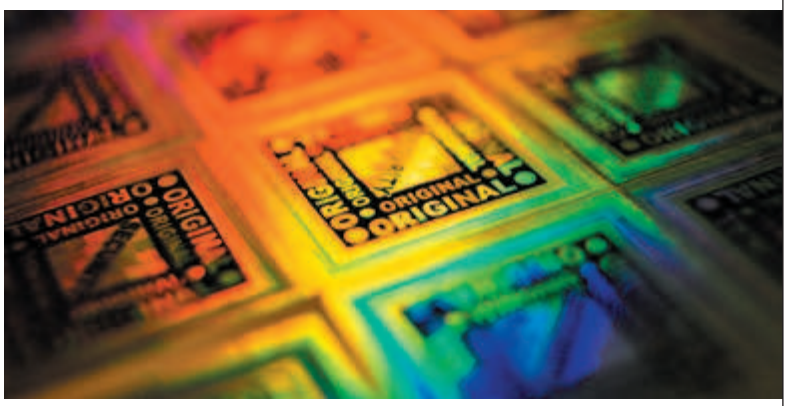
In an era marked by technological innovation, the safeguarding of personal identities has become a paramount concern for governments worldwide. As the frequency of identity theft and fraudulent activities rises, the incorporation of holography in essential documents such as ID cards, driving licences and passports has emerged as a cornerstone in the fight against counterfeit and forgery. Let's explore the profound importance of holography and attempt to provide insight into some of its characteristics in enhancing the security features of these critical documents.

The International Hologram Manufacturers Association (IHMA) is made up of over 80 of the world's leading hologram companies and includes producers and converters of holograms for banknote security, anti-counterfeiting, brand protection, packaging, graphics and other commercial applications around the world. Members actively cooperate to maintain the highest professional, security and quality standards.

Holography serves as a powerful visual deterrent against counterfeiters. The intricate and dynamic holographic images incorporated into ID cards and passports are exceptionally difficult to replicate using traditional printing methods. The three-dimensional nature of holograms adds a layer of complexity that not only enhances the visual appeal of the documents, but also discourages counterfeit attempts due to the difficulty involved in reproducing them.

One of the key advantages of holographic features is their ease of authentication. Law enforcement officers, border control agents and other authorities can quickly and reliably verify the authenticity of a document by visually inspecting holographic elements with the naked eye. This facilitates efficient and accurate identity checks, contributing to enhanced border security and reduced instances of identity fraud.

Holographic features often include elements that are extremely sensitive to tampering for all substrate types. Attempts to remove, alter or modify the hologram usually results in visible damage, serving as an immediate red flag to authorities. This tamper-evident quality not only deters potential counterfeiters, but also aids authorities in quickly identifying suspicious or altered documents during routine inspections.



Advances in holographic technologies have led to the development of a variety of innovative security features at all security levels (overt, covert and forensic). Features at the nano scale and pixel-level encoding provide an additional layer of sophistication, making it even more challenging for counterfeiters to replicate or forge holographic elements. These cutting-edge technologies contribute to staying one step ahead of counterfeit threats.

The integration of holographic security features instils a sense of trust and confidence in the general public. Knowing that their personal information is protected by state-of-the-art holographic technologies enhances the perceived reliability of government-issued documents. This, in turn, fosters public trust in the integrity of identity verification processes.

The use of holography in secure documents aligns with global standards, facilitating international collaboration in combating identity-related crimes. Shared practices in holographic security contribute to a unified front against counterfeiters, promoting consistency and effectiveness in identity verification procedures worldwide.

As the digital age brings both opportunities and challenges, the importance of holography in securing ID cards, driving licences and passports cannot be overstated. The integration of holographic features not only raises the bar for counterfeiters, but also serves as a testament to governments' commitment to protecting the identities of their citizens. In an interconnected world, where the movement of people is constant, holography stands as a stalwart guardian, ensuring the authenticity and integrity of the documents that define our identities ●

Dr Mark Deakes is the International Hologram Manufacturers Association Chair

Picture credit: IHMA

Picture credit: Alisdare Hickson

DEMOCRACY UNDER FIRE

Beth Hepworth *considers a big year for global elections in this digital threat forecast*

2024 is set to be a monumental year for democracy; with over two billion people across 50 countries going to the polls to elect representatives at local, national and intra-continental levels. This includes elections in some of the world's most populous countries, such as India, Brazil, Indonesia and the US.

While this year will certainly be a milestone in the long evolution of democracy, many of these elections take place amid a backdrop of increasing divisions in international relations, an uptick in populist politics and a widespread disenchantment with political representation in some of the world's most developed democracies.

All these issues transcend real-world and online spaces, creating distorted and muddied political landscapes prime for exploitation. This will likely manifest in diverse online adversarial threat behaviours and narratives aiming to both manipulate public opinion and capitalise on volatile information environments to cause harm. In view of this, we have outlined the primary digital threats posing significant risks to elections across the world in 2024.

MISINFORMATION AND DISINFORMATION

Electoral misinformation and disinformation will likely remain highly prevalent in elections across the world in 2024. Online threat actors, such as partisan pseudo-

Some actors will exploit polarised information environments and target wedge issues to seed hateful discourse

media entities and amateur political commentators will likely continue sharing content designed to sow distrust in the electoral process through both authentic and inauthentic means, while attempting to generate engagement for both ideological and commercial gain. Across geographies, false narratives are likely to target voting systems and the integrity of electoral institutions, particularly in countries with heightened polarisation and in the aftermath of closely contested elections.

This type of disinformation at scale will have a significant impact on highly volatile political environments and countries with a history of contentious fraud claims in previous elections. Electoral disinformation narratives played a significant role in elections across the world in 2023, including in Nigeria, Spain, and Turkey, and has already had an impact on elections in Taiwan and Indonesia in the first two months of 2024. These narratives often emanate from discourse pushed by politicians and candidates, before being amplified by both organic and inauthentic users – a behaviour which is likely to continue over the coming year.

Disinformation targeting the integrity of elections can influence dangerous real-world behaviours, including disrupting democratic processes and triggering post-election violence. This has been witnessed over the past year in countries such as Brazil – where supporters of former President Jair Bolsonaro stormed Congress in January 2023 alleging institutional election fraud.

HATE SPEECH

Hate speech perpetrated by extremist organisations and political parties in online spaces will likely pose a significant risk to elections across the world, particularly in the US, Europe, South Africa and India.

These entities will likely exploit polarised information environments and target wedge issues – such as immigration and religion – to seed hateful discourse towards minority groups, as well as to recruit and mobilise users in less-monitored digital spaces. These behaviours are often perpetrated by extremist organisations and are amplified organically by their online supporters. These actions will likely be seen during the campaigning period ahead of the June European Union elections, particularly in light of the growing popularity of ultra-nationalist ideologies and politicians across the continent in 2023.

There is also a significant risk of ideologically motivated real-world violence around election periods. Ahead of the February Indonesia general election, heightened levels of anti-Rohingya discourse online triggered violent confrontations between protesters and refugees. Similarly, in India, the Hindutva ideology – which has millions of supporters and has incited hatred against civilians and political candidates belonging to minority religious communities both online and offline – will likely impact the April-May general election.

Hate speech does not usually manifest in an isolated environment and is normally embedded with other behaviours including misinformation, harassment and violent extremism. Around the October US election in particular, we are likely to see an increased presence of extremist groups and armed militias who claim to protect electoral integrity while sharing ultranationalist viewpoints and encouraging civilians to take up arms.

FOREIGN INFLUENCE

Foreign state-backed influence operations (IOs) targeting elections are highly likely to be a persistent and significant threat in 2024. The aim of foreign IOs targeting elections is to create a divisive and distorted information environment. This in turn triggers confusion and fuels voter polarisation, while instilling public distrust in leaders and the electoral process.

The US and EU elections will likely be primary targets for foreign IO campaigns originating from hostile states such as Russia, Iran, and China. These operations often use inauthentic online assets to amplify content, as well as co-opting domestic media entities and journalists, who either authentically launder narratives from the hostile state or are explicitly directed to do so. Recent reports have outlined how Russia and China linked IOs have targeted the US to exploit domestic socio-political divisions. Similar state-linked campaigns will likely increase in prevalence in the coming year, capitalising on wedge issues, such as US spending on Ukraine, to sow discord ahead of the October US election.

AI-GENERATED CONTENT HAS HAD LIMITED NEGATIVE INFLUENCE ON ELECTIONS UP TO NOW

Foreign IOs will also likely target governments with an overlapping ideological alignment in an attempt to strengthen bilateral relations. For example, Russia will likely build on the popularity of the regional branches of RT and Sputnik in Latin America to spread narratives aimed at destabilising politics in elections in Mexico and Brazil. Similarly, there is an increased risk of Russian interference targeting the upcoming May elections in South Africa. Covert influence operations have already been found to inflame inter-racial and intra-African National Congress tensions, as well as promote pro-Russian propaganda in relation to the war in Ukraine.

AI-GENERATED CONTENT

AI-generated content will likely play a greater role in elections in 2024 as threat actors and political campaigners continue to embed AI techniques within their content-producing toolkits. AI-manipulated and generated media will likely be used by inauthentic entities to deceive voters, as well as by official election campaigns as promotional material.

Threat actors certainly have the ability to weaponise AI effectively and convincingly, which has been demonstrated on numerous occasions over the past year. For example, in April 2023, the Republican Party in the US released an ad with AI-generated images visualising a 'dystopian world' with a re-elected President Joe Biden. Similarly, in December 2023, Moldovan President Maia Sandu was forced to refute claims made in a Russia-made deepfake video of herself.

However, the successful use of sophisticated AI-generated content and technically manipulated media in sowing distrust in candidates and electoral processes will likely be limited; the majority of such content

being low quality and easily discernible by ordinary online users. In Indonesia, for example, while many media reports highlighted the proliferation of AI-generated media during the 2024 election campaigning period, this content was merely an extension of official political campaigning and did not have nefarious intentions.

THERE IS A SIGNIFICANT RISK OF IDEOLOGICALLY MOTIVATED REAL-WORLD ELECTION VIOLENCE

As a result, the risk of AI to elections in the medium term is often overstated. The vast majority of elections in 2023 saw AI-generated content have a limited influence and current disinformation campaigns are succeeding organically by exploiting societal rifts. As such, the present risk of AI to elections is centred more on the intrinsic uncertainty of its potential, rather than on its current impact.

HARASSMENT AND DOXXING

Heightened levels of targeted harassment and doxxing are likely in 2024, following a spike in threats against election workers and politicians over the past year in countries including New Zealand, Sweden, the US and Japan. Going forward, targets of online harassment campaigns are likely to include political candidates, election workers, journalists, activists and members of the judiciary. This is most likely to manifest in highly polarised political environments.

These threats will likely entail the dissemination of Personally Identifiable Information (PII) online – such as targets' home addresses, family members and phone numbers – as well as online harassment campaigns designed to undermine their legitimacy. In the US, this has manifested in a phenomenon known as 'swatting' – a form of harassment where false calls to law enforcement trigger an armed police raid on the target's house. A recent example of this saw Secretary of State for Maine, Shenna Bellows, targeted in December 2023.

Digital forms of harassment can also be a precursor to inciting physical violence against journalists and civil society members. These behaviours are often instigated by high-level politicians who legitimise the harassment. We have already seen this in the recent 7 January 2024 election in Bangladesh, where Awami League supporters attacked reporters at voting stations. Similarly, in Mexico, high-profile politicians and criminal groups frequently attack and harass media workers, making it one of the most violent countries in the world for journalists.

As we navigate the 2024 election landscape, it is important to acknowledge the digital activities that threaten our democracies in the real-world. From misinformation and disinformation to hate speech, doxxing and foreign influence operations, threat actors are seeking to exploit vulnerabilities and sow discord. The proliferation of AI-generated content also adds another layer of complexity, albeit with limitations that may not yet match the anxieties surrounding its potential impact.

However, by understanding the multifaceted nature of these threats and facilitating a reasoned, rational and fact-based conversation, we are able to begin countering their influence. Collaboration between governments, tech companies, civil society and individuals is essential in fortifying our digital defences and preserving the integrity of our democratic institutions ●

Beth Hepworth is Director of Protection Group International.

False narratives are likely to target voting systems and the integrity of electoral institutions globally

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**

WARNING SIGNS

Patrick Rea *examines the mental health challenges facing the security sector*

The mental health of security personnel in the UK is under unprecedented strain, a situation brought into sharp relief by a landmark 2020 study by Professor Mark Button, Professor of Criminology at the Institute of Criminal Justice Studies at the University of Portsmouth. This extensive survey, the most comprehensive of its kind, revealed that 40 percent of the 750 security officers involved displayed symptoms indicative of Post Traumatic Stress Disorder (PTSD).

The findings also highlighted the routine dangers these individuals face: 43 percent of respondents reported threats of violence at least once a month, with 10 percent getting threatened on a daily basis; more than 30 percent reported some kind of physical assault in the workplace at least once a year. This vulnerability is worsened by a nationwide surge in violent crime, particularly impacting the retail sector. The British Retail Consortium's 2024 report offers a stark illustration of the escalating threat, with daily violent incidents against retail workers jumping to 1,300 in the 2022/2023 period. This represents a nearly 50 percent increase from the previous year, underscoring a disturbing trend that poses risks not only to physical safety but also to mental well-being.

Many of those drawn to roles in security are veterans of the armed forces who bring their considerable skills and experience to the civilian workforce. However, this

Picture credit: AdobeStock

A high proportion of ex-services people are employed in the security industry, from some 2.4 million veterans overall in the UK

demographic may be susceptible to PTSD stemming from their service. Recognising this, mental health charity PTSD Resolution collaborates closely with professional associations within the security industry, such as ASIS UK and the Worshipful Company of Security Professionals (WCoSP), aiming to address and mitigate the impact of trauma in the security community.

While there is a growing awareness of mental health issues by employers in the sector, there is generally a lack of resources and professional support available to them. Symptoms may go unrecognised, leaving affected individuals without the treatment they need. This oversight can lead to negative outcomes, including increased absenteeism, deteriorating job performance and even suicide.

The situation presents a clear call to action: to safeguard those who secure our public and private spaces and retail environments, we must first ensure their mental health needs are met. It is against this backdrop of heightened risk and insufficient support that the initiatives spearheaded by PTSD Resolution and its industry partners become critical.

PTSD Resolution was set up in 2009 by co-founder and chairman Tony Gauvain, a therapist and retired Colonel of the Cheshire Regiment, to provide free therapy to address the mental health challenges faced by veterans, reservists and their families in the UK.

Accredited by the Royal College of Psychiatrists, this charity has been instrumental in providing free, effective mental health support to the veterans community. With over 4,000 referrals to date, PTSD Resolution delivers Human Givens therapy that typically concludes within an average of seven sessions, ensuring timely, targeted assistance.

The introduction of Trauma Awareness Training for Employers by PTSD Resolution marks a significant advancement in broadening the scope of support for trauma-affected individuals. This initiative acknowledges the critical gap in employer awareness and engagement concerning mental health issues. By equipping company owners, line managers and HR staff with the knowledge and tools to recognise and address trauma, PTSD Resolution is pioneering a shift towards more compassionate, informed workplace environments.

"The need for such mental health programmes is highlighted by the distressing challenges faced by security staff and veterans within the workplace. The worrying increase of PTSD and other trauma-related conditions underscores the importance of specialised support and intervention," says Graham Bassett, a security recruitment specialist and trustee of PTSD Resolution. "PTSD Resolution's approach, focusing on accessibility, confidentiality and efficiency, ensures that those in need receive help without undue delays. We can do more to support and care for those that keep us safe".

This collaborative effort is crucial in creating a culture of care and resilience, where the well-being of security personnel and veterans is prioritised, destigmatising PTSD and building a more supportive, empathetic society for those who have served, says Bassett.

A high proportion of ex-services people are employed in the security industry, from some 2.4 million veterans overall in the UK. This offers many benefits to employers, says Jonathan Thomas, a partner at Assist Security Group (ASG) Protect. He brings insights as an army reservist and former Royal Marine and is convinced of the unique strengths that veterans contribute to the sector:

"From their forces' training and experience, veterans bring discipline, trustworthiness, operational capability and a strong work ethic. However, it's their adaptability and problem-solving skills that are most crucial."

Veterans, accustomed to dealing with complex challenges with limited resources are adept at dealing with the often unpredictable nature of security work. Their military training has honed their ability to pre-empt threats and adapt to changing circumstances, skills that are directly transferable to civilian security roles. The British forces encourage creative problem-solving, enabling vets to bring innovative solutions to the table.

THERE'S A CONCERTED EFFORT TO DESTIGMATISE MENTAL HEALTH AND PROMOTE OPEN DIALOGUE

Moreover, the integration of veterans into civilian security teams introduces a valuable blend of perspectives, says Thomas. The combination of personnel backgrounds creates a balanced environment that creates effective problem-solving and team cohesion. Despite some veterans facing challenges such as PTSD, their overall contribution to the workforce is overwhelmingly positive. Their resilience, honed under the pressures of military service, equips them to excel in a range of operational environments.

"Veterans' adaptability is invaluable in ASG's work in forecasting emerging threats, controlling risks, and formulating a managed security solution, tailored to the specific environment of our clients to ensure effective risk management and security. PTSD isn't the plague, it's a state of mind that is increasingly well-managed. Also, there is a debt of gratitude and social responsibility in the industry and wider community to service personnel," says Jonathan Thomas.

MARK'S STORY

Mark is an army veteran who served two tours in Afghanistan. Working as a security officer in Manchester, he was caught up in an attempted robbery at the store he was guarding. Mark's manager Karen kept a close eye on him after the incident knowing trauma could appear later. She soon noticed changes – irritation, edginess. Though Mark denied a problem, it was clear to Karen that he was struggling.

Karen approached him and expressed concern, reminding Mark of their company's commitment to helping staff impacted by trauma on the job. She stressed that such reactions are normal and treatable. Mark finally opened up that he was reliving the incident and not feeling himself.

Mark agreed to meet with a therapist at PTSD Resolution, the security company partners for staff counselling and advice. Sitting down with a local trauma specialist made all the difference. With a first appointment within a fortnight and over two months of therapy, Mark learned new coping techniques and felt symptoms like anxiety and hyper vigilance begin to fade away.

Karen saw the positive changes in Mark after he accessed care through the company's employee

assistance programme. Company policy to promote openness about trauma and with a pathway to effective support has measurably increased staff morale and resilience, and impressed and reassured clients of the business too.

DAILY VIOLENT INCIDENTS AGAINST RETAIL WORKERS JUMPED TO 1,300 IN THE 2022/2023 PERIOD

The experience of trauma, characterised by symptoms such as aggression, anxiety, depression, and vivid flashbacks, can significantly alter a person's behaviour and mental state. These changes not only affect the individuals suffering from trauma but also have wider implications for their work environment, personal relationships and overall quality of life.

The onset of trauma symptoms can be immediate or delayed, often manifesting in ways that disrupt daily functioning and personal well-being. Recognising and addressing these symptoms early is crucial to prevent longer-term psychological damage.

PTSD Resolution's initiative to provide trauma awareness training for employers is a critical step towards bridging this gap. By educating employers and HR professionals about trauma, its symptoms, and effective interventions, the charity fosters a more supportive and understanding workplace culture. This training is essential for recognising trauma and facilitating timely and appropriate support for affected employees.

The collaboration between PTSD Resolution and professional associations marks a significant stride towards addressing mental health within the security industry. These partnerships amplify the reach and impact of mental health initiatives, creating a network of support.

Letitia Emeana, Chair of ASIS UK's Board of Directors, notes: "The expertise offered by PTSD Resolution provides great value to our members. Through this partnership, we not only directly support those in need, but also drive a culture shift – both across the security sector and more widely – encouraging staff at all levels to be more open about their mental health without fear of stigma."

Emeana says that while security roles come with inevitable stresses, a high incidence of PTSD and trauma-related issues should never be an accepted norm. ASIS UK's partnership with PTSD Resolution signifies a zero-tolerance approach to the lack of mental health provision, aiming to build psychologically safer, supportive and resilient security teams across the country.

James Sarson is a police officer and member of the Worshipful Company of Security Professionals. He adds: "Every year, WCoSP holds an AGM where mental health in the security sector is a high priority. It is reiterated how involved the company is in supporting charities and organisations that provide mental health assistance across sectors like police, military, retail and private security. In addition to financial donations, the company supports these groups through the work of its over 500 members."

By integrating PTSD Resolution's expertise with the professional and operational frameworks of these associations, there's a concerted effort to destigmatise mental health issues, promote open dialogue, and ensure a supportive environment for all security personnel. Through such partnerships, the industry is taking crucial steps towards not only enhancing the well-being of its members but also improving operational effectiveness and public safety ●

Patrick Rea is a Trustee and Marketing Director of the mental health charity PTSD Resolution.

The experience of trauma can significantly alter a person's behaviour and mental state

PTSD RESOLUTION ACTION POINTS

- Promote a responsible, supportive company culture rather than a 'macho' or dismissive attitude towards mental health.
- Educate line managers and staff about trauma and the importance of monitoring their mental health, such as through PTSD Resolution's half-day trauma training course.
- Regularly check on employees who have experienced traumatic events for changes in behaviour that may indicate a need for support.
- Reassure affected individuals that experiencing trauma is a normal reaction and not a sign of weakness.
- Initiate conversations about recovery preferences with employees not returning to their usual state after a few weeks.
- Encourage open discussion about trauma, but emphasise the necessity of professional treatment over talk.
- Partner with organisations like PTSD Resolution that are experienced in treating severe post-traumatic reactions for effective interventions.
- Recognise the cost-effectiveness of treating trauma early to prevent more significant issues and support employee well-being.

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

SIGINT, TSCM AND ARTIFICIAL INTELLIGENCE

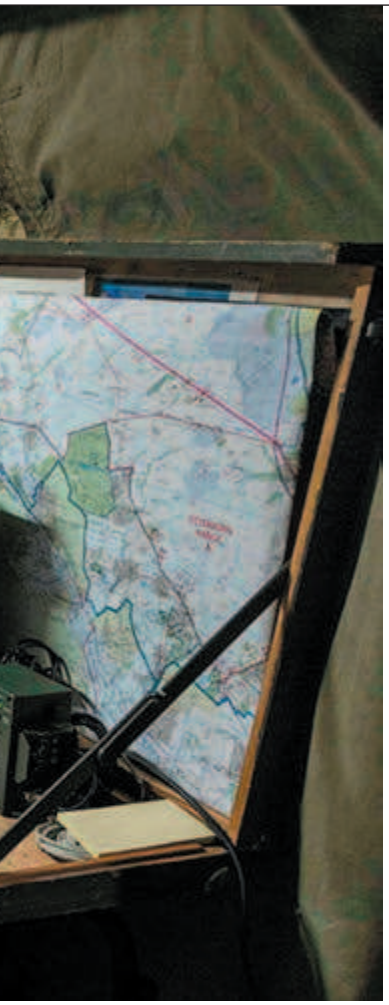
Paul D Turner *examines the growing role that AI plays in signals intelligence and technical surveillance countermeasures*

Perhaps dangerously overused and misunderstood, AI plays a significant role within SIGINT/TSCM across administrative and deployment-oriented signal analysis, analytics and reporting, as a path to clarity of large intelligence data subsets. AI and Machine Learning (ML) can be deployed to autonomously surface subtle and deeply buried intelligence-bearing signal events and identify trends and activities.

SIGINT/TSCM sub-systems have shifted to embrace machine learning and in reality adopted an emerging measure of artificial-intelligence and/or machine learning technology that can train the platform to detect more relevant signals faster than coded algorithmic responses alone. It perhaps needs to be pointed out that AI and coded-algorithms are heavily integrated processes and still require a profound measure of human operator-intellect to accomplish the task successfully.

When the spectrum is being processed at Terahertz (THz) sweep speeds well into the Millimetre (mmWave) band, as a norm, it is simply beyond the realm of human eye-sight to be able to visually extract all signals of interest. This is where AI can make a difference by detecting illusive

Picture credit: Crown Copyright



Noise filtering and on-the-fly adaptive signal processing techniques can support the removal or minimisation of unwanted spectral images and artifacts

signal events that may not be presented to the human operator across a comparatively slow user-interface. AI can process dataset visualisation; including differential vector measurements across a massive amount of mission-critical intelligence, at greater sweep speeds or within a real-time Intermediate-Frequency Broadband (IFB) or IQ streaming mode, becoming a core focus point in the AI/ML discussion.

AI is an umbrella catch-all that can describe a highly organised and standards-based process that can be used for powerful SDR feature development, and for the analysis of comprehensive datasets at a fundamental level – including display-oriented event labeling, emerging feature development and merging of feature components, big dataset generation and management to better facilitate the AI workflow process.

Anomaly detection is generally a long and difficult task for the technical analyst. ML can be used to better train the SIGINT/TSCM platform to recognise existing differential events and more accurately detect subtle anomalies deep within massive spectral datasets across a global collection strategy.

Collection is accomplished by a combination of AI-based machine-learning and predictive logic, across many thousands of perfect, not so perfect, and even very poor-quality samples to achieve a high-degree of accuracy. AI brings promise of more relevant, mission-oriented signal processing sub-systems at the source-code level, for emerging signal types and complexities. AI provides the opportunity to identify and flag standard, non-standard and modified modulation (non conformity) and classify outside of the expected norm.

AI and machine learning can assist the technical operator and software engineer with developing new tools that can predict and adapt to a wide range of changing situations; help optimise system performance, filter signals in real-time, hand-off high-probability events to a human operator or invoke additional analytical resources to surface exploitable intelligence.

Real-world wireless signals and extracted signal-level intelligence are often of poor signal quality – noisy and unreliable, sometimes by threat actor design – and cannot be relied on for high-quality intercept applications, radio direction-finding and ultimately, localisation. Advances in AI allow automatic signal quality metrics to be processed far beyond the ability of the human operator.

Noise filtering and on-the-fly adaptive signal processing techniques can support the removal or minimisation of unwanted spectral images and artifacts, resulting in cleaner and more reliable intelligence-bearing data within a shared spectral environment where many layers of ambient signal events can mask the one hostile signal, the operator needs to identify.

The use of predicative modelling across the signal processing environment touches the core of many advanced algorithmic models, used within the greater SIGINT role, to facilitate event time prediction, anomaly detection, image and speech recognition patterns, and the separation of ambient signals from potentially hostile signal events outside of the trained spectrum parameters.

SIGINT/TSCM platforms utilise AI at the signal analysis level, but can also be employed at the detection and capture level to manage the storage and hand-off of more relevant intelligence that directly assists in the clarification of big picture analytics. This important function is accomplished by identifying trends and patterns, based on and within the dataset that might not be immediately apparent to the SIGINT operator.

This big picture is more effectively disseminated across the intelligence network faster and more confidently, and is used to make more informed decisions, identify strategic opportunities and facilitate exploitation possibilities or proactively resolve complex challenges across various interoperable stake-holders.

AI and machine-based learning are interrelated and uniquely distinct concepts that are deeply imbedded and co-exist, within a SIGINT/TSCM sub-system for use as a Remote Spectrum Surveillance and Monitoring (RSSM) platform.

THE AI ENGINE SHOULD BE ABLE TO RECOGNISE AND LEARN FROM PREVIOUSLY UNKNOWN SIGNAL EVENTS

AI tends to be a much talked about catch-all process that refers to the use of technology solutions to build SDR and controllers that have the ability to mimic cognitive functions associated with human-intelligence and applied human-intellect. This allows the machine to see beyond the dataset, intuitively understand, and analyse spectral elements not only at the signal and band level, but also, classify, identify patterns, correlate significant events and process informed recommendations or assess the relevance of the intercept.

AI is thought of as a self-supporting sub-system within a larger mission platform with unique requirements. AI is a powerful set of technologies (AI engine) implemented within a SIGINT/TSCM platform allowing it to reason, learn and act to solve seemingly complex real-world challenges faster and more accurately across a globally connected radio-frequency environment.

As a comparatively equal partner, the Machine Learning process is a subset of AI that automatically enables a machine or system to learn and improve from experience (lots of experience)! Instead of hard-coding, machine learning uses algorithms to analyse large amounts of spectrum data (referred to as explicit programming, ironically), by learning from thousands or tens of thousands of iterations of every possible variable to then process an informed decision beyond the source-code.

Competent machine learning algorithms improve performance over time as they are trained by exposure to vast amounts of unique layers of spectral signal-level datasets, acquired from many different time periods, geographic locations, type of SDR hardware and a wide range of operator defaults and setting variables.

Machine learning provides the process; not to see a perfect world spectral environment – which arguably does not exist – and more accurately see and learn the spectrum, from a less than perfect, typical operator-deployed viewpoint, which tends to be the norm.

ML is a combination of the ability to structurally morph the best spectra, poor-quality spectra, interfered with spectra, captured in less-than-optimal conditions spectra and other factors such as different radio hardware, antennas, geographical locations and distances

from emitters, power levels, modulation schemes, software features, settings and operator experience.

AI is the concept of enabling a machine or system to sense, reason, act or adapt like its human counterpart. ML is the application of AI that allows machines to extract imprinted knowledge from real-world datasets and learn from it autonomously.

An AI engine's structure can vary depending on the specific application, but generally it includes several key considerations and elements. The driving algorithms can be simple instructions or complex mathematical computations; calculations and coded rules that are used to solve a problem or analyse a dataset.

The purpose of spectral-based machine learning as an AI technique is that it uses algorithmic mathematical computations to build a predictive model at the software level. A coded algorithm is used to parse datasets and then learn from that data by identifying and correlating spectral patterns discovered to generate interpretive models. Taking this concept even further, deep learning is a type of machine learning that can ultimately determine on its own whether its predictive result is accurate.

AI uses artificial neural networks, consisting of multiple layers of applied algorithmic functionality. Each layer of the algorithmic neural network analyses spectral data and then performs an independent analysis, and processes a correlated output that other layers of the neural network can interpret and process.

Neural Networks are a large array of algorithms that closely mimic the operations of the human brain and are used to recognise relationships within a large spectral dataset. This is critical in a deep learning context and uniquely designed to interpret and respond to sensory input data via machine perception, rendered labeling or clustering of raw input spectral energy patterns within a total energy capture environment.

Data preprocessing resources are tools used to filter and transform large amounts of raw data into a format that can be understood by the AI engine and travel efficiently across the neural network. Training and validation resources are tools used to train the AI engine using a large dataset of good, bad and ugly datasets, and then validate the accuracy of the engine's predictive solutions. Analytical metrics are necessary to measure the performance of the AI engine and adjust it over time as the ambient radio-frequency spectrum changes, new threat technology emerges or never-before-seen technology is introduced.

The AI engine should also be able to recognise and learn from previously unknown signal events, but will only be able to classify the signal as unknown. This is a positive and desirable response, rather than rendering a false classification. This implied limitation can be overcome with third-party integration resources that allow the AI engine to draw from a larger, more expanded dataset; integrate and learn from other datasets, software or platforms. All of the key elements work together to enable the AI engine to analyse data, learn from it, make predictions and improve over time in a cyclic approach.

The care and feeding of a neural network is fundamental in populating an AI engine via a machine-learning approach. There is no easy route or substitute for a highly focused and scientific approach to populating a competent dataset. When shortcuts are taken the engineer or operator will have no idea of what the expected outcome will be and cannot have any measure of confidence in the capability of the platform.

We have seen all too often within the TSCM environment competitive interests rushing to market with only a financial prize as the primary goal. Taking shortcuts and half measures at the technology level is a very short-sighted business model and tends to fool almost everyone concerned, except the threat actors!

When it comes to an AI solution within a SIGINT/TSCM role, we are seeing competitive interests simply rebrand their respective products with implied TSCM/SIGINT capability, when in reality, this is simply a marketing ploy with limited compatibility, third-party products.

A circular 360° approach is essential to advancing the benefits of AI within a modern standards-based methodology. The development and implementation of a functional AI sub-system takes research, dataset development and competent implementation within a fully qualified software defined radio environment

Paul D Turner, TSS TSI is the President/CEO of Professional Development TSCM Group Inc., and is a certified Technical Security Specialist (TSS) and Technical Security Instructor (TSI) with 44 years experience in providing advanced operator certification training, delivery of TSCM services worldwide, developer of the Kestrel TSCM Professional Software and manages the Canadian Technical Security Conference (CTSC) under the operational umbrella of the TSB 2000 (Technical) Standard.

AI can be deployed to autonomously surface subtle and deeply buried intelligence-bearing signal events and identify trends

Picture credit: AdobeStock

MESA 2.0 Advanced WiFi Detection Just Got Better!

Detect, analyze and locate WiFi devices.

New Firmware Update Delivers New Capability.

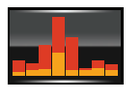
MESA 2.0

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

GRINDING TO A HALT

Joseph Carson *addresses the growing cyber threats to critical national infrastructure*

In an era where digital connectivity underpins the very fabric of society, the security of our Critical National Infrastructure (CNI) has never been more important. In recent years there has been a surge in sophisticated cyber attacks targeting these vital systems, including energy grids, transportation networks and water supply systems. Analysis from Microsoft in October 2023 found that 41 percent of all the threat alerts it sent out in the last year concerned CNI operators.

It's a threat that is being taken seriously by most governments around the world as regulators double down on measures to protect essential services and their connected supply chains. For example, in 2023 the NIS 2 Directive came into effect for member states of the EU, with new requirements for essential and important industries to tackle rising cyber threats.

In the UK, the NCSC has flagged an: "enduring and significant" threat to critical infrastructure in its 2023 annual review, and as the country is now the third for number of cyber attacks, it's no surprise that the Science, Innovation and Technology Select Committee recently launched an inquiry into the cyber resilience of the UK CNI, considering its critical role in supporting and growing

The UK is at high risk of a catastrophic ransomware attack that could bring its CNI to a standstill

the delivery of public services. All organisations within the sector and those in their supply chain must fully understand the nature of the threats they are up against and pursue strategies for enhancing their resilience.

The criminal groups targeting the critical infrastructure are formidable opponents. The head of E.ON one of Europe's largest energy suppliers, recently stated his firm has been continually attacked by high-level adversaries and called for states to do more to protect the sector. In the UK a parliamentary report has stated that the UK is at high risk of a "catastrophic" ransomware attack that could bring the country's CNI to a standstill, bringing further scrutiny on the cyber security challenges and measures needed to safeguard these essential services.

The work of nation-state actors has been linked to numerous cyber incidents targeting CNI. The NCSC highlights China, Russia and Iran as the main perpetrators, with objectives ranging from espionage to cyber warfare. Cyber attacks have become a standard element of geopolitical manoeuvring, used for espionage to acquire political and economic secrets. Microsoft's research indicates there has been some decline in destructive attacks in 2023 in favour of more subtle and persistent espionage tactics. Nonetheless, attacks designed primarily to disrupt essential services remain a prominent threat, often serving as an extension of traditional warfare – as we have seen with the conflict in Ukraine.

State-backed groups have the assets and capital to employ advanced persistent threats (APTs) that are complex and stealthy. APTs are designed to infiltrate networks undetected, allowing attackers to maintain a long-term presence within the target infrastructure. This approach enables them to gather intelligence, monitor activities and potentially disrupt operations at a time of their choosing.

While these groups are a grave threat, the UK's CNI also faces threats from criminal gangs motivated primarily by financial gain. To this end, ransomware has now become one of the most common tactics used by these groups, encrypting an organisation's data or systems and demanding payment for their release, or in other cases exfiltrating data and selling it on the Dark Web. They increasingly view CNI as a lucrative target for these attacks as the essential nature of the services allows for significant leverage in ransom demands.

The nature of critical national infrastructure creates many unique challenges that leaves it vulnerable to attack, and one of the most significant is relying on an ageing and legacy technology.

Many systems that are in use across our national infrastructure now interface with modern technologies, creating a patchwork of old and new that is challenging to secure comprehensively. This juxtaposition of legacy systems with modern IT assets introduces unique vulnerabilities, making them attractive targets for cyber adversaries.

The convergence of traditional IT and Operational Technology (OT) further complicates the security landscape. Many organisations across all CNI sectors – from energy providers to water companies, telecoms companies and emergency services – heavily depend on OT assets such as industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems, and programmable logic controllers (PLCs) that were designed in a pre-digital era. And where Internet of Things (IoT) devices – such as smart sensors in energy grids or automated control systems in water treatment facilities – have been deployed, in many cases they offer minimal security features. These systems are rarely designed to mesh with standard security controls. As organisations within the CNI embrace a programme of digital transformation as it is beneficial for operational efficiency, the boundaries between IT and OT blur, leading to an expanded attack surface, with critical systems exposed and unprotected devices that can be exploited as entry points into broader network systems.

Addressing these key risk factors requires a security approach that is as dynamic and multifaceted as the sector's threats.

THE CONVERGENCE OF IT AND OT SYSTEMS HAS EXPANDED THE THREAT LANDSCAPE

Although CNI security strategies must encompass a comprehensive approach addressing both technological and human factors, a strong cyber security posture in CNI involves building good foundations, including regular vulnerability assessments and penetration testing, particularly focusing on the interfaces between IT and OT systems. Ensuring that security patches are applied promptly, and systems are kept up to date is vital, as well as implementing network segmentation to limit the spread of a cyber attacks within the infrastructure.

Of course, getting the fundamentals right is not enough and organisations should explore more advanced technology opportunities, such as integrating AI and automation into their cyber security strategies. For example, AI-driven tools can help monitor networks for unusual activities, detect anomalies and predict potential threats based on data patterns and algorithms. Automation aids in rapidly responding to incidents, reducing the time between detection and remediation.

The speed and precision of automated, AI-powered tools are particularly valuable for managing CNI's often complex and sprawling IT environments. However, it is essential to maintain a balance as an over-reliance on automated systems without human oversight can lead to gaps in security.

In this AI-era it is worth noting that the human element in cyber security still plays a crucial part in prevention. In fact, Verizon's Data Breach Investigations 2022 Report has stated that 82 percent of all data breaches involved a human element. Training staff to recognise and respond to cyber threats is fundamental, which includes building their awareness of phishing attempts and understanding the importance of strong password policies. Equally important is establishing a culture of cyber security within the organisation, where security is firstly and foremost seen as a collective responsibility that stems from internal practices. Finally, even with well-layered defence, no system can ever be fully impenetrable, so having a well-defined incident response plan is essential. This should outline clear protocols for responding to different types of cyber incidents, roles and responsibilities during an incident.

By combining these strategies, CNI organisations can create a resilient defence against the evolving landscape

of cyber threats. This resilience is not just about preventing attacks but also about having the capability to quickly recover and restore normal operations in the event of a breach.

Effectively applying these security measures hinges on organisations' first identifying and prioritising the most critical assets in their IT environment. This requires mapping the network infrastructure to understand where the most sensitive and essential data and services reside. Once identified, these assets require stringent protective measures, including advanced encryption, access controls and continuous monitoring for potential threats.

The next step is identifying and neutralising the most prevalent threats to them. Regular penetration testing, especially in OT environments, identifies vulnerabilities that might not be apparent in day-to-day operations. Given the unique challenges in OT environments, such as legacy systems and the need for uninterrupted operations, a specialist approach to penetration testing is required. This ensures that security assessments are thorough yet do not disrupt critical processes.

Similarly, the convergence of IT and OT systems has expanded the threat landscape. Establishing better security for both environments requires both technological integration and a unified approach to risk management. This includes shared policies, procedures and a common understanding of the risk landscape. IT and OT teams need to be in regular communication, working together to spot any necessary changes or issues with their infrastructure, rather than the heavily siloed approach that is common today.

One of the most important factors is managing how these environments are accessed. Both Identity and Access Management (IAM) and Privileged Access Management (PAM) are critical in controlling network systems and data access. IAM ensures that only authorised individuals have access to specific resources, while PAM provides an additional layer of security for accounts with elevated access privileges. Implementing these systems helps mitigate insider threats and risks from compromised user credentials.

CNI operators should also be prepared for the worst-case scenario of a major breach and transparency in identifying and reporting cyber incidents is vital for all organisations within this sector. The forthcoming NIS2 directive requires a 24-hour turnaround for severe incidents, for example.

Disclosing incidents responsibly also demonstrates to stakeholders that cyber security practices are being followed and threats are being taken seriously. CNI sectors would also benefit from a more open approach to sharing lessons learned with the wider community to prevent similar attacks.

As the NCSC's review has flagged, environments with increasing levels of digitisation and complexity progressively become highly vulnerable to attack and more must be done on a national level to safeguard the UK's infrastructure.

All critical infrastructures face an evolving landscape of cyber threats, carried out by sophisticated, well-resourced nation-state actors and increasingly agile, brazen criminal gangs. Defending them requires individual operators and central government having a concerted, proactive and dynamic approach to security, based on fortifying defences and fostering a culture of vigilance and continuous improvement. Given that any attack on these vital services has the potential to bring a country to a standstill, operators also need full national support in defending against these threats. Governments must continue collaborating with security leaders to share intelligence, best practices and adapt regulatory frameworks to keep up with increasingly bold and devious adversaries ●

Joseph Carson is Chief Security Scientist (CSS) & Advisory CISO at Delinea.

CNI faces threats from criminal gangs motivated primarily by financial gain

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)

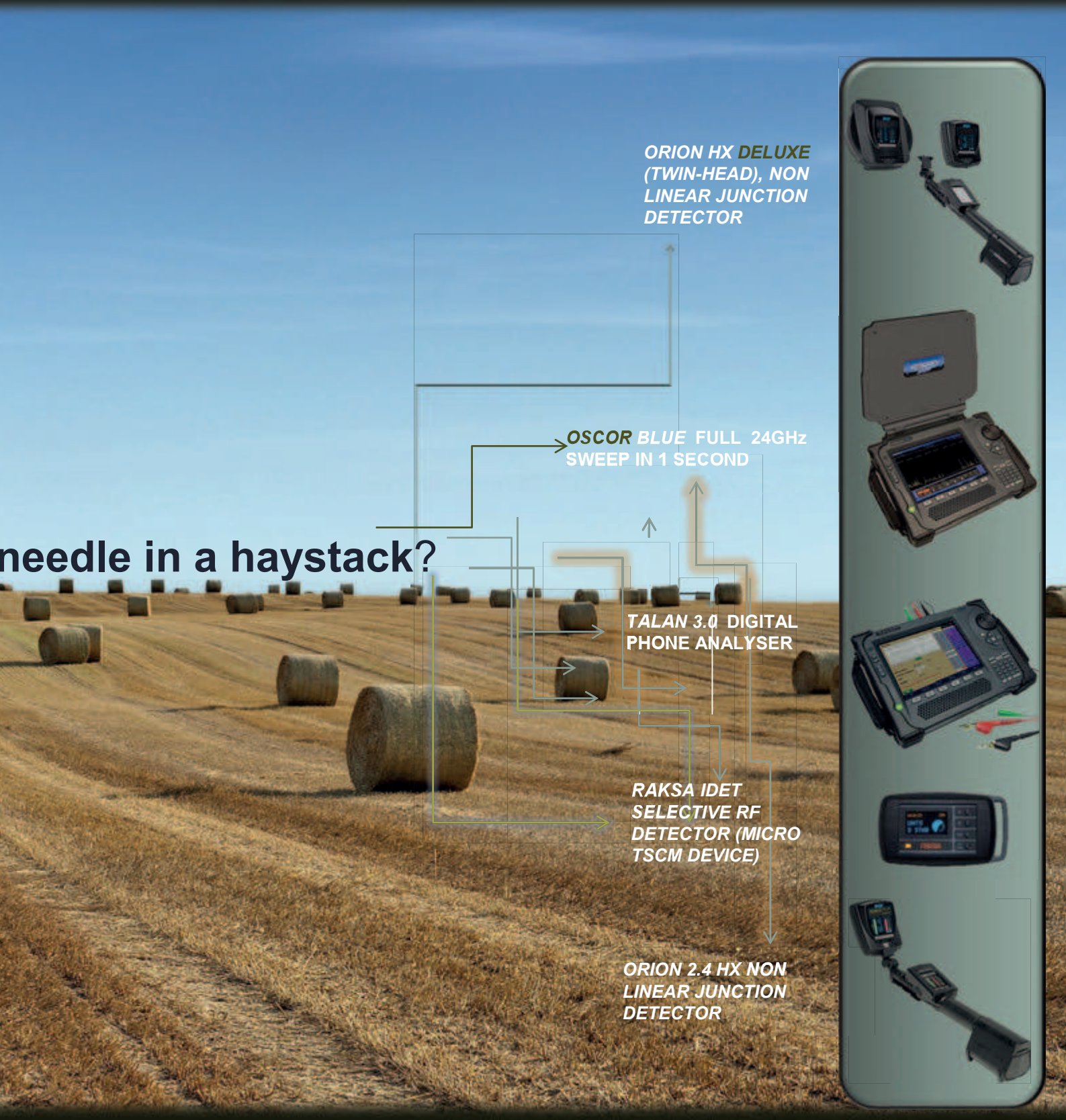
TSCM TRAINING
COURSES &
CERTIFICATION
UK/US/GLOBAL

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.



TSCM Equipment supply, training and de-bugging services

The preferred choice of Government & Law Enforcement Agencies worldwide.

Web: **www.intpro.com**

UNLOCKING A NEW ERA

Eugenia Marina *explores the role of biometrics in education: navigating the path to a secure and inclusive learning environment*

In light of the urgent global problems, education is a lighthouse for hope that will bring about change. Like any other aspect of our daily lives, the education sector is not unexposed to the effects of technological changes. As we look into the world of biometrics, especially facial recognition technology, we start seeing not only the ways it can influence access and security, but also find out how it has contributed to securing one's peace through knowledge and inclusivity. Biometrics as part of this symbiotic relationship provides a pathway towards a secure, more accessible and harmonised education system.

These days, biometric technology is widely used in the education industry. Its many uses change the security and convenience of the students and education facilitators. Modern protocols have reduced even the hazards that came with employing traditional biometric techniques. The most widely used biometric technologies in educational institutions are face recognition and contactless fingerprint or palm recognition. Because of their utilisation, biometrics are gaining more and more trust.

Exam boards and educational institutions may also use voice, iris, fingerprint or facial recognition technology to confirm test taker identities. This has been demonstrated to improve academic integrity.

One of the most liked and effective uses of biometrics in education is attendance monitoring. Administrators can identify truancy issues more easily, thanks to the automatic function of biometric attendance monitoring, which also removes the hassle for needless roll calls before courses.

Verifying each person attempting to enter a university or school with biometric-enabled access control can significantly boost safety. Restricted biometric security access can also be used to secure areas that are off-limits to students.

Biometrics can play a very significant role in activity tracking. In fact, it can be used to track various activities. On the other hand, employing manual reporting

Exam boards and educational institutions can use voice, iris, fingerprint or facial recognition technology to confirm test taker identities

Eugenia Marina is Business Development Director, MENA region, at RecFaces.

procedures to record activities can be time consuming. Instructors can use biometrics to keep an activity diary and generate quick reports as needed.

The contactless and user-friendly nature of facial recognition technology makes it a superior biometric modality compared with others, such as fingerprints. The seamless nature and non-intrusive property of facial recognition makes it a much more convenient and hygienic alternative for usage in an educational facility. The major difference between fingerprint scanners and facial recognition is that the latter provides a touchless experience in accordance with contemporary requirements, which increases general user satisfaction. The scalability, as well as its ease of implementation and adaptability make facial recognition a better option in transforming safety and accessibility within educational settings providing superior security and comfort.

The implementation of facial recognition technology into campus security systems brings many benefits, the most significant of which is the increased time and resource efficiency for students. This technology provides better identification and access control processes which are faster and more streamlined, thereby enabling a more convenient and efficient on-campus experience. Students have swift facility and event access, thus enabling them to utilise more of their time on academics or other productive activities. The fully automated check of faces in daily activities can increase the overall convenience and offer a modern and advanced solution to campus security. This positive trend towards efficiency encapsulates the potential for facial recognition systems to be both an added layer of security as well as enrich the quality of student life on campus.

The emergence of facial recognition technology in the campus security systems brings forward inspiring possibilities for the provision of customised campus services and offers a bright and progressive perspective. Through applying facial recognition, institutions can provide student-centric experiences, which can ensure enrichment of students' time on campus and help them grow holistically. The application of this technology allows the tailoring of campus resources, which leads to providing students with access to the facilities and services that match their tastes and requirements. Moreover, in the coming years, facial recognition will be capable of enabling intelligent event recommendations that provide students with suggestions aligning with their interests and previous activities. This will contribute to a richer campus life and an environment where community involvement is a constantly present value. Besides, target news will be delivered immediately and students will be informed about the latest campus news and upcoming engagement events. This change manifested in the form of personalised activities is inspired from the positive effect brought about by the application of facial recognition technology. This is indicative of the paradigm shift towards responsive and student-centric approach to education.

The campus security envisaged with face recognition systems integration constitutes a contrasting narrative speaking of biases and discrimination, with both justified concerns and positive implications featured in the discourse. The evolution of facial recognition systems for accuracy has been followed by the unfortunate possibilities of appearance biases. This subsequently resulted in industry-wide efforts to enhance the systems performance continually and establish a more legitimate system. Over the years, the facial recognition algorithms are being continually updated and reformed to be neutral to gender, appearance and racial differences, and eliminate chances of biased recording and alerts. This promotes inclusivity in the educational environment where the technology is more than efficient in accurate identification without promoting bias and discrimination of any kind, helping create a positive learning ecosystem.

In the world of rapidly changing educational technology, facial recognition systems represent a revolutionary force in relation to accessibility, security and inclusion within these institutions. The safety of students and staff is an issue that educational facilities all over the world have in common. Biometric systems, incorporated into access points of dormitories and laboratories, add another layer of security. Using facial biometrics, the authentication of online learners also becomes very easy. This is a blessing for a large number of educational institutions providing online courses making education more accessible to those who live in remote areas or have mobility issues. It provides a low-cost alternative for students who are unable to move in order to complete their higher education.

VERIFYING EACH PERSON WITH BIOMETRIC-ENABLED ACCESS CONTROL CAN REALLY BOOST SAFETY

A secure campus enabled by facial recognition technology evolves to become an enriching environment in which learning thrives. In this connection, educational establishments equipped with technologically advanced security measures create an environment of safety that is universally pervasive creating a space where both students and teaching staff feel safe. A great security infrastructure is not only a shield, but also an accelerant of positivity. In a scenario devoid of security concerns, the positive attitude settles in, establishing an excellent atmosphere for learning and working together. Beyond immediate safety, the implementation of state-of-the-art security features acts as a catalyst, the embedding of advanced security mechanisms inside education transcends to all parts of the educational ecosystem. Facial recognition technology not only targets the security issues, but also their potential positive impacts contribute towards creating a technologically enriched tomorrow.

Besides the initial feeling of protection, the impacts of a positive learning atmosphere reaches far and wide. It serves as the foundation for student well-being, involvement and academic performance. When learners feel safe, they naturally want to engage in the learning process actively. This active involvement, therefore, forms a catalyst whereby the students' academic performances improve since they are likely to assimilate and retain knowledge in an environment best suited for overall development. Basically, the combination of strong security measures made possible by facial recognition technology and increased inclusivity results in an educated space that not only protects, but also drives students toward academic success as well as personal development ●

The budget further underlines the need for defence leaders to adopt agile approaches to security

Elaine Whyte is defence and security expert at PA Consulting

SPRING BUDGET 2024

Elaine Whyte *examines the UK security implications of the recent Spring Budget*

The geopolitical environment created a challenging backdrop for the Spring Budget, as the UK's role in promoting peace and security around the world, most pressingly in Ukraine, competed with fiscal challenges. The Government is holding the Defence budget at 2 percent of GDP until economic conditions allow an increase, potentially to 2.5 percent. However, the current geopolitical challenges and competing priorities are a strategy quagmire for defence leaders, who are expected to deliver a world-class and broad fighting capability within existing budgets, while threats are becoming increasingly sophisticated and variable.

Productivity is crucial for defence, particularly as the UK prioritises resupplying and rearming stockpiles that are depleted from substantial equipment loans to Ukraine in an increasingly fractious global arena. There is a clear need to collaborate across the sector and supply chain, as well as for ingenious new approaches to procurement and whole systems management, to achieve defence and security outcomes within the current budget. This can only be achieved through fundamental change to the way the defence enterprise operates.

For example, embracing the overarching architecture of capabilities and technical solutions at a higher level than today provides productivity gains that can unblock the route to delivering more capability faster and cheaper, using common 'platforms' to reduce cost and time overheads. The Chancellor's Budget underscores the need for defence leaders to transform their operational efficiency, by simplifying processes and adopting agile approaches – whether that be in process optimisation or handling data like a strategic asset in digital integration.

TAKE THE STRAIN

In an increasingly strained economic environment, the whole defence and security enterprise should also forge a path that deepens collaboration and accelerates innovation. This requires new strategic partnerships, talent strategies and harnessing the power of emerging technology as warfare enters the information era. This fundamentally different approach could have a considerable impact on the battlefield of data and information.

For example, collaborating with small and medium-sized enterprises could allow defence leaders access to emerging technologies, such as in artificial intelligence and digital engineering, from more agile suppliers that offer a different perspective. Don't forget that the AI ecosystem is wide-ranging – encompassing university spinouts, fast-moving start-ups and small-to-medium scale tech enterprises – and it is these organisations that hold many of the transformative, forward-looking solutions that will help the defence sector overcome its challenges.

In this respect, it is good news that the Budget encourages investment in new technologies and AI, positioning the UK as the new Silicon Valley at the forefront of next-generation challenges and solutions. The appetite for change in implementation must now match up to the ambition of the intent. Defence leaders cannot afford to be slow to adapt or overlook the potential that cutting-edge technologies have in giving them a strategic advantage.

On the talent side, the defence sector is not alone in finding it hard to attract and retain talent, particularly in tech. The importance of bridging the digital skills gap is undeniable: from countering cyber attacks to data-enabled battle planning, tech capabilities are key to giving defence enterprises a competitive edge. To address under resourcing, the industry should focus on working together and breaking down siloes. In practice, this could look like sharing technical personnel across the forces, creating common career pathways and aptitude testing or devising more joint selection frameworks. There is also an opportunity to encourage young people into the sector through coordinated campaigns in higher education, emphasising the value and purpose of this work.

Defence leaders stand at the confluence of complex threat landscapes and constrained budgets, and the outcome of the Spring Budget has renewed questions as to how they can do more with less. Leaders can navigate this, but must rise to these challenges by 'choosing and changing' – making hard choices about the UK's role, being efficient in the use of resources and preparing the enterprise to change with future threats much more quickly ●

Picture credit: Crown Copyright

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 !

MAINTAINING THE STATUS QUO

Simon Alderson *examines the role of security firms in managing activist protests*

The 'friendly threat' that activists pose to event disruption is often incredibly difficult for security firms to spot. Although security measures can be in place such as body searches and checkpoints, activists often can get around these by concealing banners and often small items such as glitter or glue that they use to cause disruption. A balance always needs to be struck between how intrusive searches are as it is almost impossible to ensure that all protesters are stopped before getting in. Furthermore, activists often employ diverse tactics, making it difficult for security teams to predict and counter their strategies effectively. From mounting stages, to running on sports fields to throwing glitter or paint, the nature of the protest and form it may take cannot always be certain, however effective security can mitigate such actions when they do occur with good planning.

The widespread use of social media in organising protests also amplifies the speed and reach of activist movements, making it challenging for security firms to stay ahead of developments and adapt their strategies in real-time. Part of the solution is to monitor social media conversations to spot when a protest might be planned and put mitigation techniques and protocols in place.

In my experience, event security has undergone significant transformation, surpassing the conventional roles of uniformed officers, access control and incident response. Present-day event security professionals operate as strategic thinkers, employing intelligence-driven risk-based models to proactively address threats by identifying and rectifying gaps and vulnerabilities. Successful event security planning adopts a comprehensive approach, encompassing the

Security guards need to be able to distinguish between peaceful protest and acts that jeopardise public safety

Picture credit: Crown Copyright

physical safeguarding of individuals and assets from explicit threats of terrorism and violence, as well as safeguarding the brand and reputation. There are ways we can mitigate if not prevent protests.

This includes meticulous planning, as mishandling a protest can not only overshadow the intended event, but also be the sole memorable aspect, indeed, the desired purpose of the protesters.

Contingency planning for both planned and spontaneous protests is often lacking in event security strategies. Even when protest planning is included, key elements may be overlooked or inadequately addressed. Before delving into the strategies for effective management, it is essential for security officers to comprehend the context and motivations behind the demonstration. A comprehensive understanding of the issues at hand can aid in developing a nuanced approach that respects the rights of protesters while maintaining public safety. A well-coordinated strategy is vital for successful management. Security guards should collaborate with local police, emergency services and relevant stakeholders to develop a comprehensive plan that addresses potential risks and challenges. Coordination ensures a unified response and facilitates the efficient deployment of resources to maintain public safety.

Moreover, a proactive approach to security is essential in managing protests. Security firms can work closely with organisers and local authorities to conduct thorough risk assessments, identifying potential flashpoints and vulnerabilities. By understanding the dynamics of the crowd and anticipating issues, security teams can implement preventive measures such as crowd control barriers, access control and security checkpoints. The goal is to create an environment that deters disruptive behaviour and fosters a sense of safety for all.

Effective communication is also a cornerstone of successful security. Security firms can facilitate open lines of communication between event organisers, police and protest organisers when they are known to be present. Establishing a dialogue helps to understand the expectations and concerns of all parties involved for a more cooperative atmosphere. Clear communication channels can also be instrumental in disseminating information about safety and potential changes in the protest dynamics. Security companies can also utilise communication technology to ensure seamless coordination during the event. Timely and accurate information exchange is crucial for responding promptly to emerging situations.

PRESENT-DAY EVENT SECURITY PROFESSIONALS MUST ALSO OPERATE AS STRATEGIC THINKERS

It is also vital that security personnel undergo training to handle protests in a professional and respectful manner. Training programmes should cover conflict resolution, de-escalation techniques, and an understanding of legal boundaries. The ability to defuse tense situations through effective communication and understanding can prevent confrontations from escalating into violence. Training should focus on cultural sensitivity and the psychology of crowds, enabling security personnel to make informed decisions under pressure.

Advanced surveillance technologies can assist security firms in monitoring the crowd and identifying potential threats. CCTV cameras, drones and other monitoring devices can be strategically deployed to provide real-time insights into the crowd's behaviour. This allows security teams to detect and respond to unusual or suspicious activities promptly. The use of technology also contributes to the documentation of events, aiding in post-event analysis and the identification of lessons learned for future security planning.

Respecting the right to freedom of expression is a fundamental aspect of protest management. Security guards must be trained to distinguish between peaceful assembly and acts that jeopardise safety. Proportional responses to threats, avoiding the use of excessive force and protecting the rights of protesters contribute to a more positive and cooperative environment. Security firms must operate within the framework of the law and respect individuals' rights to peaceful assembly and free expression. Understanding the legal parameters of managing protests is crucial to avoid unnecessary confrontations and legal consequences.

The goal is to strike a delicate balance between maintaining public safety and upholding the principles of free expression, fostering an atmosphere where diverse voices can be heard within the bounds of civil discourse creating an environment where citizens can express their views without compromising public order. A thoughtful and respectful approach to protest management not only safeguards democratic principles, but also fosters trust between security officers and the communities they serve ●

Simon Alderson, CEO of First Response Group

Paul Mason is Managing Director for Redline Assured Security, with over 25 years of aviation experience.

Behavioural detection awareness skills play a significant role in achieving preparedness

EVOLVING THREAT

PREPAREDNESS IN AN EVOLVING THREAT

Paul Mason *considers how the security community can work together to deliver Protect Duty legislation.*

As identified in the Manchester Arena Inquiry (the recommendations from which inform Martyn's Law), a lack of preparedness and inadequate response to suspicious behaviour, enabling the terrorist to carry out his attack with tragic consequences, were amongst the key shortcomings and missed opportunities in the provision of security at the arena on 22 May 2017.

The threat of terrorism has evolved with an increase in the occurrence of attacks on crowded spaces. With more than 650,000 spaces in the UK being defined as 'crowded' it is imperative for approaches to security and risk management planning to evolve, too. While it will never be possible to eradicate terrorism altogether, with better preparedness comes more powerful deterrence and greater protection.

Preparedness is unquestionably a key tool in the arsenal of prevention activity, yet it is a fundamental missing piece in the jigsaw of security provision. Furthermore, according to a report carried out by Blerter and Event Risk Management Solutions, most event organisers rely on annual or one-off risk management planning, with only 18 percent having a risk management plan that is less than 12 months old, with 21 percent who don't have a plan at all.

Recommendations from the Manchester Arena Inquiry call for higher levels of preparedness, including calls for greater alertness to the threat level of a terrorist attack, robust procedures to counter the threat of a terrorist attack, and prompt action in response to reports or observations of suspicious behaviour that are out of sync with the expected pattern of life at such events. Furthermore, continuous assessment of evolving risk, ongoing training in how to intervene in a potential risk situation and continuous quality assurance all have a role in taking preparedness to a higher level to mitigate risk.

Behavioural detection awareness skills play a significant role in achieving preparedness across the security sector. A workforce that is trained in detecting unusual behaviour, such as individuals working later or starting earlier than normal, a person loitering outside a venue over the course of a few weeks, someone carrying a bulging rucksack or someone who looks nervous, jumpy, overly concentrated or unusually focused in a public space, acts as a powerful force against the threat of terrorism. Behavioural detection awareness training enables security personnel, venue stewards, information desk staff and cleaners to recognise early indicators that something could be awry and suspicious through careful observation of the behaviour of people as they go about their day-to-day activities.

VITAL SKILLS

Essentially, all personnel who encounter people, who are located close to vehicles outside a venue, or who sit behind a CCTV camera, should undergo behavioural detection awareness training (as a minimum) to, firstly, equip them with the observation skills to identify potential hostile reconnaissance, preparatory assessments or dry runs and, secondly, to sharpen their instincts to share suspicions with their superiors. For example, a cleaner may come across a dubious package hidden somewhere in a venue, potentially revealing a test set by a potential terrorist designed to assess the robustness of the venue's security eco-system. Without the proper training to know instinctively to act and clarity on the channels of communication to escalate suspicions, the test will fail and potentially be the green light for a fatal attack.

Many aspects of suspicious behaviour are common sense to recognise, but until they are brought together in a professional discipline across the entire workforce at a venue and the wider events industry behaviours will continue to go unnoticed or not be acted upon. It is therefore critical to embed a more proactive and pre-emptive approach to security that positions security as everybody's business to increase the likelihood of criminal activity being intercepted.

> **IT IS IMPERATIVE FOR APPROACHES TO RISK MANAGEMENT PLANNING TO EVOLVE**

Behavioural Detection Awareness training provides a low cost, high impact solution to making venues more secure. The minimal level of training can be implemented for all personnel in roles related to an arena, with 20 or 30 specific security personnel being more highly trained as behavioural detection officers, Meanwhile, ongoing quality assurance as the threat landscape evolves means that all personnel undergo rehearsals and observation during live events to embed skills that are crucial to preparedness and better risk management planning in an expanded holistic security system. A more positive security culture will result in greater resilience against future threats while addressing key weaknesses in the security sector ●

INTERNATIONAL SECURITY EXPO

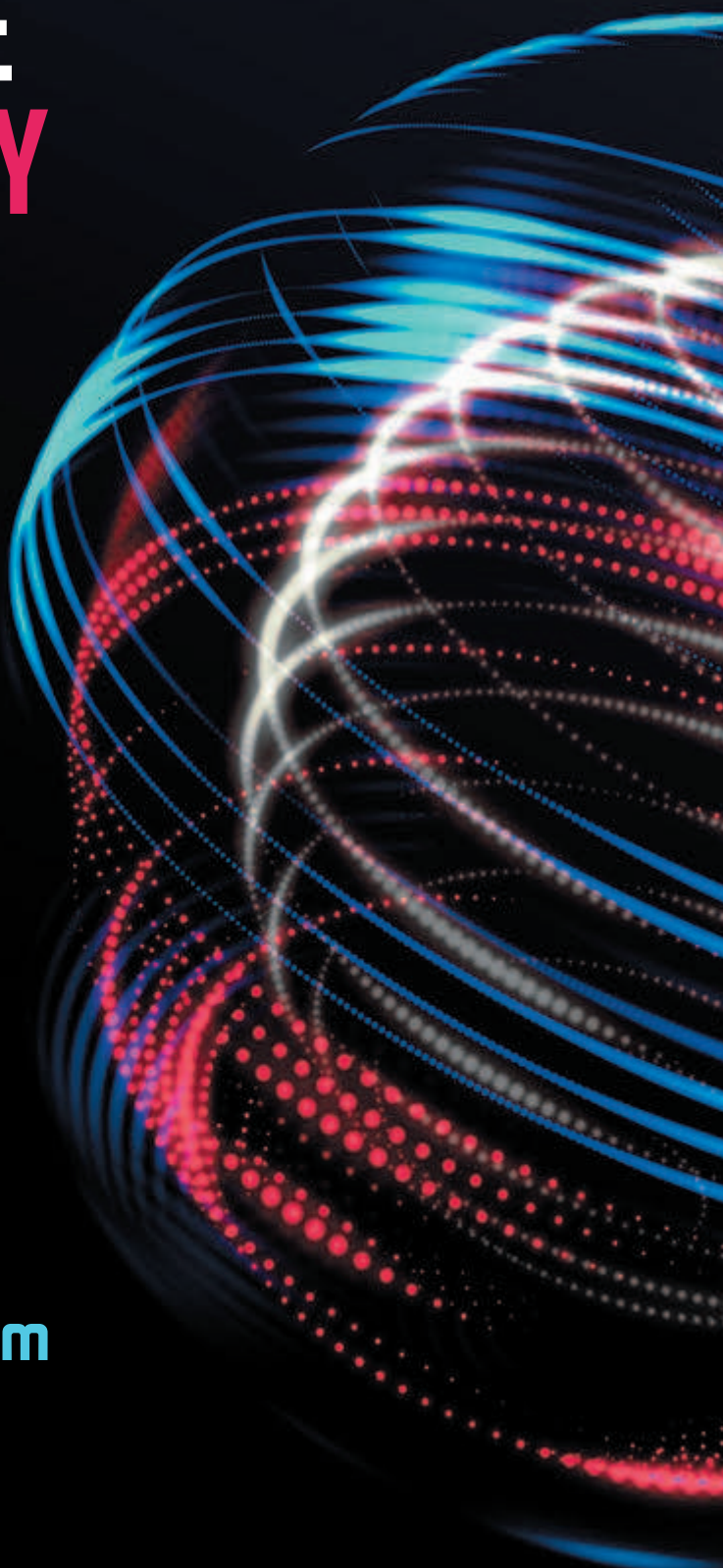
24-25 SEPT 2024
OLYMPIA, LONDON

CONNECTING THE GLOBAL SECURITY COMMUNITY

10,000+
HIGH-LEVEL SECURITY DECISION-MAKERS

300+
INTERNATIONAL EXHIBITORS

SECURE YOUR STAND TODAY



internationalsecurityexpo.com
+44 (0)20 8947 9177
info@internationalsecurityexpo.com

Picture credit: Getty

TRAVEL SAFELY

Rodger Cook, Kate Fitzpatrick *and* **Frank Harrison**

examine the current security challenges facing the global traveller

International travel in 2024 is at a pivotal crossroads, eagerly anticipated by travel enthusiasts, businesses and governments alike, yet facing greater risk and uncertainty than in living memory. Travelling teams face numerous risks in today's dynamic landscape. Economic instability, environmental risks, geopolitical factors and societal shifts all present uncertainties. Cyber security threats like data breaches and ransomware attacks also pose financial losses and reputational damage. The impact of these risks varies across industries, locations and organisations' circumstances.

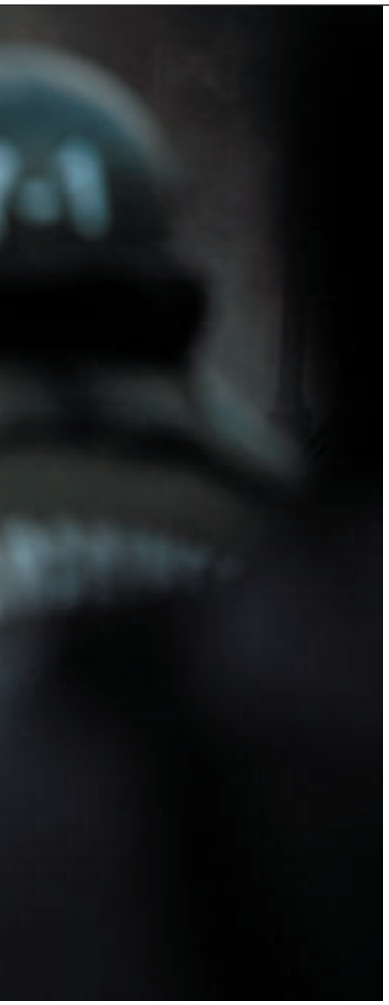
In this complex global security environment, the importance of diligent research and preparation prior to embarking on travel has never been more critical. Assessing the security and political landscape of destinations and equipping travellers with useful knowledge about potential dangers are essential steps in minimising risks to ensure that business critical travel can continue seamlessly.

The resurgence of right-wing politics, hybrid conflicts and geopolitical uncertainties add complexity to international travel. Misinformation campaigns are also a growing tactic in hybrid warfare, prompting the need for travellers to stay informed about geopolitical developments using reputable sources.

For instance, Houthi attacks in the Red Sea and territorial disputes in the South China Sea are causing uncertainty and diplomatic disquiet. Around 90 percent of global goods travel by sea, but the risk of geopolitical disruption to maritime routes is extreme.

Border tensions, sanctions and diplomatic disputes can all disrupt travel plans, emphasising the need for robust security measures, up-to-date intelligence and contingency plans for all travellers.

Last year has been confirmed as the warmest since records began, driven by climate change, causing increased frequency of natural disasters. Already this year, we've seen wildfires in Chile, Argentina and Columbia, a powerful earthquake in central Japan, tornadoes in the United States and volcanic eruptions in Iceland. Extreme heat is set to continue in 2024. From hurricanes to floods, these events pose threats to travel schedules, safety and finances.



Protests, civil unrest, terrorism and political instability can cause potential harm and disrupt plans

It is important that, where possible, travel plans have contingency measures in place to safeguard travelling teams to alert them to potential dangers of extreme potential weather or natural disasters.

Emerging needs for new resources to support the energy transition, supply chains and manufacturing have led to a shift in the destinations that business travellers must consider. Places once regarded as high-risk or no-go zones are now unavoidable destinations for many. Travellers and organisations must make informed choices and plan safe journeys to destinations that may have seemed unconventional in the past. While the desire for unique and immersive experiences remains a driving force, we recognise the critical need to ensure safety and security while navigating these evolving landscapes.

Local expertise and experience is key to mitigating the risk when visiting these destinations. Not only should this prepare the traveller for what they can and should expect, it should also include a cultural and society briefing including how to behave, body language and respecting the culture of the destination, the potential risks and ways to avoid them.

Organisations face a constant risk of cyber attacks, particularly when they are on the move, including rising cases of state-sponsored attacks, identity theft, financial fraud data breaches, ransomware targeting critical infrastructure and AI-driven phishing campaigns. These threats can result in significant financial losses, reputational damage and regulatory penalties.

For example, when using public wi-fi networks in airports, hotels or cafes, travellers are at risk of data breaches and identity theft. Hackers can intercept sensitive information, such as log-in credentials or financial details, leading to losses and privacy breaches.

Smart cities, which use technology to improve efficiency and quality of life for residents, are also vulnerable to cyber security threats. For instance, hackers can exploit vulnerabilities in smart city infrastructure, such as traffic lights or public transportation systems, to cause disruptions or accidents. This poses risks to residents and travellers visiting these cities who may rely on these systems for transportation or navigation.

To mitigate cyber security risks while travelling, travellers should use secure networks, such as a Virtual Private Network (VPN), to protect their data. They should also avoid clicking on suspicious links or providing personal information online. Additionally, organisations should educate their employees about cyber security best practices and provide them with the necessary tools to protect their devices and data while travelling.

Health crises, exemplified by the COVID-19 pandemic, have brought forth several risks and changes in travel dynamics that continue to impact travellers in 2024. The pandemic has upended traditional travel practices, making once-popular activities like crowded events, large gatherings and public transportation riskier due to the potential for virus transmission.

The impact of staff shortages in all aspects of the travel ecosystems also remains with chronic delays, restricted customer-facing services and rapid adoption of technology to fill these gaps creating further traveller frustrations and disruptions.

The pandemic has also highlighted the importance of agility and preparedness in swiftly responding to health crises. Future health crises could disrupt business operations, supply chains, and economies, underscoring the need for organisations to have robust contingency plans to ensure business continuity and financial stability.

Physical safety remains a paramount concern from theft and pickpocketing to robbery and mugging. Protests, civil unrest, terrorism and political instability can also cause potential harm and disrupt travel plans. Travellers need to stay vigilant and well-informed to navigate such situations and safeguard their mobile and computing devices that are often their primary forms of financial transactions, travel itineraries and communications. Keeping valuables at home and dividing cash and credit cards across multiple pockets or bags are simple ways to reducing the risk

SECURITY STRATEGIES MUST BE ADAPTIVE, FORWARD-LOOKING AND HOLISTIC

The human factor in travel security encompasses the need for a security-aware culture within organisations and the crucial mental health aspect for travelling workers and teams. Travellers may face a range of stressful experiences due to the uncertain nature of travel, therefore establishing and maintaining support systems which prioritise mental health and well-being is essential.

For example, being caught up in a natural disaster, dealing with a health emergency or facing a security threat, like a terrorist incident, while travelling can be highly stressful and traumatic. Travellers need access to assistance support that can provide safety protocols, access to medical facilities and evacuation support.

To conduct a comprehensive travel risk assessment for employees, start by determining the trip's purpose, destination and activities. Organisations must know their travellers, their travel experience, and their resilience. Research the country's or region's safety and security conditions, considering factors like political stability, crime rates, terrorism threats, health risks, natural disasters and local laws.

Organisations also need to understand the activities the traveller will perform and if those activities pose a risk from a legal, customary or local cultural perspective.

Check official government travel advisories and review corporate travel policies. Evaluate the employee's personal risk profile, transportation mode, trip duration and communication options. Consider the employee's unique requirements or vulnerabilities and consult local contacts for first-hand information.

Analyse the impact on work responsibilities and establish risk mitigation measures. Communicate risks and strategies to the employee, monitor the situation and provide ongoing support to ensure travellers on the ground are kept informed about potential threats and the impact on their safety is constantly evaluated.

Travellers should also be informed on local laws, customs and cultural norms to avoid misunderstandings or conflicts, and they should prioritise their health and safety by staying updated on vaccinations, carrying necessary medications

and following basic hygiene practices. They should also be prepared for emergencies or have access to travel assistance services. Engage and have the right stakeholders involved. Remember, involving relevant stakeholders, such as human resources, legal teams and security personnel is crucial in the travel risk assessment process to ensure comprehensive and well-informed decision-making. Also conduct a post-travel evaluation for improvement and involve relevant stakeholders throughout the process.

While this year presents unique global travel challenges, travellers equipped with the right knowledge and tools should be able to confidently navigate these uncertainties. Security strategies must be adaptive, forward-looking and holistic. Security leaders should adopt a multidisciplinary approach, collaborating across sectors and borders to address emerging threats effectively. This collaboration is essential for enhancing security and fostering innovation, resilience and ethical considerations in the face of global challenges.

It is crucial to have a Travel Risk Management framework in place to ensure organisations recognise and mitigate traveller, destination and activity risks. By implementing these frameworks, organisations can better mitigate the risks inherent in today's global travel landscape and protect their travellers. For instance, this includes staying updated using trusted travel advisories, leveraging technology for cyber security, and understanding local customs and laws to ensure a safe and enriching travel experience.

The world is more interconnected than ever, offering unprecedented business opportunities, cultural exchange possibilities and personal growth scenarios, and with the right preparation and support, informed travel is safe travel ●

Rodger Cook is General Manager – Global Security Services, **Kate Fitzpatrick** is Security Director EMEA and **Frank Harrison** is Security Director Americas, at World Travel.

WHAT SHOULD A TRAVEL RISK ASSESSMENT INCLUDE?

Security leaders need to understand who their travellers are as well as where they are going and what they are doing to identify and manage risk exposures. Once the potential risks are identified, businesses should use the model of Educate, Locate, Communicate to prepare the Travel Risk Management programme.

Travel Risk Assessment Inclusions:

Destination Analysis: Identify specific travel locations, considering political, social and economic stability, ongoing conflicts, civil unrest and natural disasters.

Current Situation Assessment: Evaluate destination stability, including health risks, healthcare availability, vaccination requirements, recent outbreak, and epidemics.

Security Analysis: Assess crime rates, terrorism threats and overall safety.

Transportation Risks: Evaluate safety and reliability of local transportation options.

Cultural and Social Factors: Understand local customs, traditions and cultural norms.

Environmental Risks: Assess weather conditions, climate patterns and geographical features.

Legal and Regulatory Considerations: Understand local laws, regulations and customs impacting travellers.

Infrastructure Assessment: Evaluate essential services like communication networks, electricity, water supply and emergency response systems.

Emergency Planning: Develop contingency plans and protocols for emergencies.

Communication and Reporting: Establish communication channels for travellers to report whereabouts and safety.

Personal Considerations: Consider the specific needs and vulnerabilities of individual travellers.

Insurance Coverage: Review travel insurance policies for adequate coverage.

It is vital that travel plans have contingency measures in place to safeguard teams to alert them to potential dangers of extreme potential weather or natural disasters

Picture credit: Getty

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

2 March, London – UK
Two women were injured by shotgun pellets after a suspect dropped a firearm and it accidentally discharged during a police pursuit in Clapham.

3 March, across the country – Belgium
Belgian police arrested four youths over messages they exchanged allegedly plotting a jihadist attack.

3 March, Karabulak – Russia
Six members of the Islamic State group barricaded themselves in a third-floor apartment and were killed in a shootout in Russia's volatile North Caucasus region.

3 March, Cornwall – UK
An unexploded bomb was discovered on a beach in Falmouth by a member of the public. An explosive ordnance disposal team was brought in to safely deal with it.

5 March, Berlin – Germany
Leftwing extremists claimed responsibility for a dawn arson attack on an electricity pylon at a Tesla car factory, which bosses said would halt production until the end of the week.

5 March, across the country – Turkey
Police detained 51 people across 12 cities suspected of having links to the Daesh/ISIS terror group.

5 March, Pristina – Kosovo
A man was sentenced to three-and-a-half years in prison for contacting a person in Saudi Arabia to learn how to create bombs he planned to use against an LGBTQ+ march in the capital.

Americas

2 March, Hopkinton – USA
A 20-year-old man was arrested and charged with detonating a device after a loud explosion caused over 100 concerned inhabitants of the Massachusetts town to call emergency services. No one was hurt.

3 March, Philadelphia – USA
A 27-year-old man was killed by another passenger moments after they both got off a bus. Witnesses said the two had argued, but a motive remains under investigation.

4 March, Philadelphia – USA
A 17-year-old student was killed and four other people were wounded when gunfire erupted at a bus stop. The victims included two women who were riding on a bus.

4 March, USA
A security failure at a third-party vendor exposed an unknown number of American Express card numbers, expiry dates and other data to persons unknown.

5 March, Philadelphia – USA
A passenger on a bus got into an argument with another man and fired two shots from a 9mm handgun. The victim died shortly afterward at a hospital.

6 March, Philadelphia – USA
Eight high school students waiting to board a city bus after classes were wounded by gunshots from suspects who jumped from a car and opened fire, the fourth shooting on the transit system in as many days.

Asia

1 March, Bengaluru – India
At least eight people were injured when a suspected home-made bomb exploded during lunch hour at a cafe in the country's technology hub.

2 March – Red Sea
An Italian warship participating in the EU naval protection force in the Red Sea was forced to shoot down a Houthi missile in a rare engagement by the country's navy.

4 March, Surabaya – Indonesia
At least 10 personnel were injured following an explosion in the Indonesian police's Mobile Brigade headquarters in East Java.

5 March, Karnataka – India
Multiple bomb threats were sent to the chief minister, deputy chief minister, state home minister and commissioner of Police via email threatening to blow up crowded areas in the state. A ransom of $2.5 million was demanded to prevent further blasts.

5 March – Red Sea
Three cables under the Red Sea that provide global internet and telecommunications were cut. At time of going to press, Yemen's Houthi rebels are suspected of being responsible.

5 March, Faizabad – Afghanistan
An explosion shook a Taliban military base next to the airport in, the capital's North-Eastern Badakhshan province. No one has yet claimed responsibility.

6 March, Auckland – New Zealand
Police carried out a controlled detonation of a home-made explosive device found at a reserve near Seabrook Avenue.

6 March, Rawalpindi – Pakistan
The Punjab Counter Terrorism Department and local police apprehended three men near the jail where Imran Khan is held. From Afghanistan, they were reportedly going to carry out a terrorist attack in the area.

10 March, Peshawar – Pakistan
A motorcycle packed with explosives went off in the North-Western Pakistani city, killing two people and severely injuring another.

Africa

2 March, Heidelburg – South Africa
A hijacking suspect was shot dead in the town to the East of Johannesburg during a high-speed chase by police, after two suspects hijacked a vehicle.

3 March, Ngala – Nigeria
Boko Haram insurgents reportedly abducted female internally displaced persons numbering between 113 and 319 depending on sources from the Borno State town.

4 March, Kurfi – Nigeria
The Nigerian Army killed a man reported to be the second-in-command in the hierarchy of terrorists in Katsina State, under the leadership of another terrorist known as Modi Modi.

8 March, Kuriga – Nigeria
More than 280 students were kidnapped from their elementary school and one was shot by unknown assailants on motorcycles in Kaduna state.

9 March, Gidan Bakuso – Nigeria
Gunmen forced their way into a school in the Sokoto village in the North-West of the country, and started firing shots before kidnapping 15 children in a dawn raid.

10 March, Mogadishu – Somalia
Explosives caused a huge fire that gutted a section of the capital's biggest market, Bakara, killing one person and destroying several stores .

12 March, Indian ocean
A group of Somali pirates hijacked a Bangladeshi cargo vessel and took 23 people on board hostage before heading in the direction of Somalia.

14 March, Mogadishu – Somalia
Al-Shabaab terrorists attacked a hotel frequently used by government officials for meetings in the capital following bomb explosions and gunfire. Several people were injured.

14 March, Malawi
Malawi's government regained control of the passport system, weeks after a cyber attack. The system was hacked by unknown "mercenaries" who demanded a ransom.

NEWS

Europe

Security plans for Paris Olympics stolen from train

A bag containing potentially sensitive security plans for the Paris 2024 Olympic Games was stolen from a train at the Gare du Nord station. Police sources revealed that the bag in question belonged to a 56-year-old engineer from Paris City Hall. A bag containing his work computer and two USB drives, with data including the municipal police's organisational plans for securing the Olympics, was stolen. To enhance security during the Paris Olympics, due to start on 26 July, exceptional measures will be implemented in France, including the utilisation of intelligent, algorithmic video surveillance. The comprehensive security strategy will involve a daily deployment of approximately 35,000 security force personnel, with 2,000 municipal police officers specifically assigned to safeguard the event. Paris' military governor has revealed plans to deploy a temporary camp of 10,000 military personnel in the Bois de Vincennes public park located in Eastern Paris, as part of security arrangements for the Olympics. As a result, residents will only be able to access certain zones via QR codes, along with other security restrictions.

Germany accuses Russia of information war after leak

Germany's defence minister accused Russia of conducting an "information war" aimed at creating divisions within the country, in his first comments after the publication of an audio recording of a meeting of senior German military officials. In early March, Russian media published a 38-minute recording of a call in which German officers were heard discussing weapons for Ukraine and a potential strike by Kyiv on a bridge in Crimea, prompting officials in Moscow to demand an explanation. A couple of days later Germany called it an apparent act of eavesdropping and said it was investigating. "The incident is much more than just the interception and publication of a conversation… It is part of an information war that Putin is waging," defence minister Boris Pistorius said. The Kremlin has repeatedly denied accusations of spreading false or misleading information. A Russian foreign ministry spokesperson said the country was demanding an: "explanation from Germany," without detailing its particular concerns. On the leaked call, participants discuss the possible delivery of Taurus cruise missiles to Kyiv, which Chancellor Olaf Scholz has so far publicly rejected. The discussions also covered the use of long-range missiles provided to Kyiv by France and Britain – and the training of Ukrainian soldiers.

Norway, Sweden and Finland host Nato military exercises

A first-of-its-kind training exercise involving more than 20,000 soldiers from 13 countries was launched across Northern Norway, Sweden and Finland as the region prepared to become a fully Nato territory. The joint defence exercise, which ran until 14 March was held in recognition of Finland's recent membership of the Western military alliance, and with Sweden expected to join imminently. The training exercise across air, land and sea – which also included soldiers from the UK, US, Denmark, France, Germany, Italy, Spain, the Netherlands, Belgium and Canada – incorporated a cross-border operations exercise to demonstrate "a unique level of cooperation and interoperability as they cross borders on land, sea and air".

Researchers awarded £4.2 million to build a secure world

Researchers in Manchester are on a mission to tackle some of the UK's most challenging resilience and security problems. Backed by a £4.2-million funding award from UK Research and Innovation's building a secure and resilient world strategic theme, the university team will drive a Research and Coordination Hub to confront "pressing risks and threats online and in the world around us". Led by Dr Richard Kirkham, Deputy Director of the Thomas Ashton Institute for Risk and Regulatory Research at The University of Manchester, the project known as SALIENT (Secure And ResiLIENT), will bring Manchester academics together with partners from the universities of Bath, Exeter and Sussex to catalyse, convene and conduct research and innovation in support of the UK's national security and resilience. Dr Kirkham added: "Our approach will promote a culture of genuine interdisciplinarity, co-production and citizen engagement, ensuring that the research we do is relevant, timely and represents value for money."

Rishi Sunak: extremist are growing threat to UK democracy

UK prime minister Rishi Sunak claimed that extremist groups in the UK are: "trying to tear us apart", in a hastily arranged Downing Street statement in early March. The claim was made from a podium outside 10 Downing Street – something normally reserved for major announcements such as a general election – after divisive MP George Galloway won a byelection in Rochdale. The prime minister condemned what he called: "a shocking increase in extremist disruption and criminality" after the 7 October massacre by Hamas and the Israeli invasion of Gaza. He also went on to claim democracy itself was a target, as he condemned the election of Galloway, who easily won the seat in Rochdale on a platform that focused on anti-Israel sentiment over Gaza. In a sometimes rambling and seemingly contradictory 10-minute address, Sunak made points likely to anger MPs on the right of the Conservative party such as Suella Braverman and Robert Jenrick, who themselves have sought to stoke up recent tensions as being almost entirely the responsibility of Islamist extremists.

NEWS

Americas

US to discover if Chinese cars pose national data security risk

The United States has opened an investigation into whether Chinese vehicle imports pose national security risks and could impose restrictions due to concerns about "connected" car technology. The US Commerce Department probe is needed because vehicles: "collect large amounts of sensitive data on their drivers and passengers (and) regularly use their cameras and sensors to record detailed information on US infrastructure," the White House said. As vehicles could: "be piloted or disabled remotely" the probe will also look at autonomous cars. "China's policies could flood our market with its vehicles, posing risks to our national security," President Joe Biden said. White House officials told reporters it was too early to say what action might be taken and said there was no decision on a potential ban or restrictions on connected Chinese vehicles. Biden called the effort an: "unprecedented action to ensure that cars on US roads from countries of concern like China do not undermine our national security". There are relatively few Chinese-made light duty vehicles being imported into the United States. Commerce Secretary Gina Raimondo said the administration was taking action before they become widespread and: "potentially threaten our privacy and national security".

US Government expands role in software security

The White House Office of the National Cyber Director (ONCD) has released a report written for developers and engineers stating that the nation needs to create a new balance of responsibilities for defending cyberspace and better incentives for companies to invest in the cyber security of their products. The ONCD has called on technology manufacturers to shift to memory-safe programming languages – such as Python, Java and Rust – which can eliminate up to 70 percent of the vulnerabilities, and to develop better ways of measuring the security of their products. The current ecosystem places too much burden on the people least able to afford the costs needed to secure critical infrastructure and systems against attackers, National Cyber Director Harry Coker said in a video statement. "A system that can be brought down by a few keystrokes needs better building blocks, a stronger foundation. We need to expect more of those most capable and best positioned to defend cyberspace, and that includes the federal government," he said.

Florida to deploy state troopers during spring break

Florida's Republican governor Ron DeSantis will deploy state troopers to help with crowd control during the spring break season, warning that the Sunshine state would not: "tolerate lawlessness". About 140 state troopers will be sent across Florida to assist 17 law enforcement agencies, as thousands of college students make their way en masse to popular spring break destinations. At least 60 of those officers will be stationed in South Florida, mostly in Miami Beach, the Tallahassee Democrat reported. Spring break hotspots such as Daytona Beach and Panama City will also have an increased police presence, DeSantis said. DeSantis warned potential visitors that there would be consequences for lawless behaviour, warning: "We're a law-and-order state," and: "You are going to pay the price and be held accountable if you're coming for reasons other than to have fun. That is not gonna fly in the Sunshine state." Bag checks and restricted beach access will also be in place in Miami Beach, as officials work to curtail chaos.

New York deploys National Guard to subways

New York's governor outlined sweeping new state efforts, including deploying the National Guard, to address surging subway crime in the city in early March. Gov. Kathy Hochul announced her new five-point plan, which includes surging state personnel to help with the NYPD bag checks, proposing a bill to allow judges to ban more violent offenders from the system, adding new cameras for conductor cabins, increasing prosecutorial and law enforcement coordination and deploying more outreach teams along with existing Safe Options Support (SOS) ones. The state personnel surge includes 750 National Guard members and 250 personnel from MTA and State Police, totalling 1,000, and the effort was underway the same day she announced it. The idea, Hochul says, is for people to have a: "felt sense of safety," she said.

US military simulation spending to exceed $26-billion up to 2028

The US is poised to significantly bolster its military simulation and training expenditure, surpassing $26-billion annually up to 2028. The allocation of resources into advanced training systems reflects the evolving geopolitical landscape and the imperative to optimise preparedness in the face of emerging threats, according to a GlobalData report. The findings reveal that the US military is investing heavily in its simulation and training systems to prepare its personnel. These investments cover practice air, land and sea systems and equipment. Overall, this sector is anticipated to value a total of $159-billion between 2023 and 2028. Its largest segment is projected to be land simulation and training, at $137.2-billion. Fox Walker, Defence Analyst at GlobalData, notes: "Military simulation and training is the largest sector of the US defence market. The US plans to spend at least $26-billion annually, highlighting the Department of Defence's commitment to building up the combat readiness within the armed forces."

NEWS

Asia

New Zealand extends terrorist designation to Hamas

New Zealand has announced the designation of Hamas in its entirety as a terrorist entity, expanding a previous decision from 2010 which designated only the Palestinian faction's military wing the Al-Qassam Brigades. In addition, the Pacific island imposed travel bans on: "extremist Israeli settlers" who have committed violent acts, calling the behaviour: "unacceptable" and reiterated its opposition to settlements as a: "violation of international law". "New Zealand is seriously concerned by the significant increase in extremist violence perpetrated by Israeli settlers against Palestinian populations in recent months. This is particularly destabilising in what is already a major crisis," New Zealand's Prime Minister, Christopher Luxon, said in a statement. Foreign Minister Winston Peters added: "Settlements undermine the prospects for a viable two-state solution. Recent statements by some Israeli ministers about plans for further settlement construction are of serious concern and will raise tensions further between Israelis and Palestinians". In terms of the Hamas designation, the prime minister said in a statement: "What happened on 7 October reinforces we can no longer distinguish between the military and political wings of Hamas. The organisation as a whole bears responsibility for these horrific terrorist attacks." The expanded designation, which began under a previous prime minister, freezes: "any assets of the terrorist entity in New Zealand. It also makes it a criminal offence to carry out property or financial transactions with them or provide material support."

Peace talks with insurgents won't fail, says Thai PM

During his ongoing visit to the Southern border provinces, Thailand's Prime Minister, Srettha Thavisin, has confirmed that peace talks between the government and a major insurgent group in the Deep South will not collapse with an aim to achieve reduction of violence and cessation of hostilities. The end of February marked the 11th anniversary of peace talks initiated by the Yingluck administration, which signed a general agreement with the Barisan Nasional Revolusi (BRN) – a major insurgent group active in the Thai South. The Thai government delegation and BRN representatives have agreed in a principle on a draft roadmap called the Joint Comprehensive Plan towards Peace. The plan includes public consultation, cessation of hostilities and finding a political solution to end the conflict. The Prime Minister reaffirmed that efforts for peace in the Southern border provinces are ongoing, with a focus on opportunities and a better future for people in the region and whether to revoke the emergency decree in the areas is subject to security considerations.

Vietnam lists overseas dissident groups as terrorist organisations

Vietnam has listed two political groups operating in the United States as: "terrorist organisations", accusing them of orchestrating attacks and promoting a secessionist agenda. The groups are the North Carolina-headquartered Montagnard Support Group Inc (MSGI) and Montagnard Stand for Justice (MSFJ), which was established in Thailand. Both are accused of involvement in deadly attacks in the Central Highlands region in June 2023 that killed nine people, including four policemen. Montagnards are an ethnic minority from Vietnam's Central Highlands. Many are Protestant Christians who sided with the United States during the Vietnam War.

Schiebel Camcopter wins contract for South Korean navy

Schiebel, together with Korean-based defence solutions companies Hanwha Systems and UI Helicopter, has been awarded a contract by the Defence Acquisition Programme Administration (DAPA) for the development and delivery of the Vertical Take-off and Landing CAMCOPTER S-300 Unmanned Air System to be operated by the South Korean MOD. The contract was signed with Hanwha Systems for the supply of the S-300 for Intelligence, Surveillance, Target Acquisition and Reconnaissance missions for the South Korean Navy and Marine Corps. The Navy has been a Schiebel customer for over 10 years, and is understood to be reacting to North Korea's call for an expansion of it UAS fleet, adding larger and heavier UAS with greater capability.

Treason equals life sentence under Hong Kong security law

Hong Kong's government has released the draft text of a new security law that tightens control of the city and brings its laws closer in line with mainland China. The law, known as Article 23, defines and penalises crimes related to national security. The draft published in early March proposes sentences of up to life in prison for some crimes including insurrection and treason, and lengthens allowable periods of detention without charge from 48 hours to two weeks. Possessing a seditious publication could attract up to three years in jail under the law, which also gives police the right to search any premises to seize and destroy such material. The draft also introduces a crime of: "foreign interference", and of colluding with foreign forces. The sentence for sedition increases from two years to seven or 10 if found to have been committed in collusion with foreign forces. In other offences, such as revealing state secrets, limited public interest defences have been allowed and the bill notes Hong Kong's traditional freedoms. Police must also petition a magistrate if they want to hold someone without charge for longer than the current 48 hours.

HEALD®

DESIGNERS, MANUFACTURERS AND INSTALLERS OF AWARD WINNING PERIMETER SECURITY PRODUCTS

Secured by Design

PSSA

SafeContractor SafePQQ

OSPA WINNER 2022
Outstanding Security Equipment Manufacturer

MADE IN BRITAIN

Constructionline
Gold Member

SafeContractor

+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

NEWS

Africa

Insurgent attacks force thousands to flee in Mozambique

A series of attacks in the Northern province of Cabo Delgado by IS-linked armed groups has sent tens of thousands fleeing from their homes. Recent attacks by an Islamist insurgent group, known locally as Mashababos or al-Shabaab (not affiliated with the Somali al-Shabaab), have killed at least four civilians in villages of the Chiure district and 25 Mozambican soldiers in the town of Mucojo, which the Mozambican army had retaken only nine days earlier. Destruction of infrastructure, including homes, churches, schools and health centres in the fighting have also increased pressure on already degraded public services in the region. More than 70,000 people have fled from the embattled Northern districts of Cabo Delgado in the past two months, according to official estimates, with many seeking shelter at government camps in neighbouring Nampula Province. The insurgency in Cabo Delgado began in 2017 as militant Islamists and jihadists attempting to establish an Islamic state clashed with government forces. Nearly 5,000 people have died in the conflict, including more than 2,000 civilians, and 709,000 remain displaced by the ongoing violence. Massive LNG projects in the region have also been jeopardised by the fighting.

Cyber security breach at South Africa's business registry

The Companies and Intellectual Property Commission (CIPC) of South Africa, tasked with business registrations and intellectual property oversight has fallen victim to a cyber attack, exposing personal information of both clients and employees. The breach prompted immediate action, shutting down specific CIPC systems to contain potential damage. While the extent of the compromised information remains undisclosed, the agency assured ongoing investigations would determine and communicate the impact shortly. Established in 2008, the CIPC manages records of millions of South African companies, ensuring compliance with company and intellectual property law and facilitating business activities. The breach raises concerns about the exposure of directors' and owners' names, addresses and contact details, as well as those of patent and trademark holders. CIPC urged affected clients to closely monitor credit card transactions and authorise only known and valid requests.

Over 95 percent of insurgents with Boko Haram ideology dead

The Borno State Government has claimed that more than 95 percent of insurgents with Boko Haram ideology – especially the founding members of the group – are either dead or have already surrendered. Special Adviser to the Borno State governor on Security Affairs, Brig.Gen. Ishaq Abdullahi made the revelation in early March while addressing newsmen in Maiduguri, the state's capital. Abdullahi stressed that the leadership of the group was in disarray as only 10 of its founding members might still be alive. The governor's aide added that many top commanders of the sect have died from leadership tussles between ISWAP fighters and the Boko Haram insurgents loyal to the late Abubakar Shekau after his death. He noted that other leaders of the sect have also died from in-fighting among them due to leadership positions, especially after the death of the late leader of Shekau. He added that more than 90 percent of the die-hards with Boko Haram ideology died after Shekau's demise.

New pact to safeguard businesses from cyber threats

Cassava Technologies, Anthropic and Google are looking to tap into the growing Artificial Intelligence space in Africa and provide extra cyber security through a new partnership. The deal will see the companies offer advanced cloud, cyber security and generative AI capabilities to African businesses. This comes at a time that Africa is witnessing an increase in cyber-crime activities as organisations continue to become more digitised. Cassava Technologies, co-founder and executive chairman Strive Masiyiwa said: "We recognise the importance of responsible AI in enabling access to economic opportunities and empowering individuals and businesses across the continent. Our partnership will help us deliver AI-powered solutions that address the unique challenges and opportunities in Africa's digital transformation journey." Liquid C2 will enhance cyber security and cloud services across Africa, integrating Google Cloud's latest AI, data, collaboration and security solutions.

Kenya hopes to deploy 1,000 police officers to troubled Haiti

Kenya and Haiti have a security deal to try to salvage a plan for Nairobi to deploy 1,000 police officers to the troubled Caribbean nation to help combat gang violence that has surged to unprecedented levels. Kenya agreed in October to lead a UN-authorised international police force to Haiti, but the Kenyan high court ruled the plan unconstitutional in January – in part because of a lack of reciprocal agreements between the two countries. Kenya's president, William Ruto, said in a statement that he and the Haitian prime minister, Ariel Henry, witnessed the signing of the reciprocal agreements between the two countries in early March. It was not immediately clear how, or if, the agreements could circumvent the court's ruling. Gunmen shot at Haiti's main international airport and other targets, including police stations, in a wave of violence that caught many people by surprise. Separately, at least four police officers, including two women, were killed in an attack on a station near the community of Canaan in early March.

DIARY DATES

2024 Conference and Exhibition planner

8-10 April AUCSO 40th Annual Conference 2024
Liverpool, UK
Organiser: Association of University Chief Security Officers
www.aucso.org

9-12 April ISC West 2024
Las Vegas, USA
Organiser: The Security Industry Association
Tel: +1 301-804-4700
Email: info@securityindustry.org
www.discoverisc.com/west/en-us.html

16-18 April Expo Seguridad México 2024
Mexico City, Mexico
Organiser: The Security Industry Association
Tel: +52 (55) 8852 6000
Email: info@exposeguridad.com
www.exposeguridadmexico.com/

30 April - 2 May The Security Event 2024
Birmingham, UK
Organiser: Nineteen Events
Tel: +44 (0)20 8947 9177
Email: info@thesecurityevent.co.uk
www.thesecurityevent.co.uk

6-8 May GPEC 2024
Leipzig, Germany
Organiser: EMW Exhibition & Media Wehrstedt
Tel: +49 34 743 - 62 090
Email: info@gpec.de
www.gpec.de/

14-16 May Airport Show 2024
Texas, USA
Organiser: Clarion Events
Tel: +1 203 491 2400
Email: sales@bordersecurityevents.com
www.bordersecurityexpo.com

21-23 May Border Security Expo 2024
Dubai, UAE
Organiser: RX Global
Tel: +971 2 409 0300
Email: info.airportshow@rxglobal.com
www.theairportshow.com/

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

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

THE SECURITY EVENT

30 APRIL – 2 MAY 2024
NEC BIRMINGHAM UK

THE UK'S AWARD WINNING NO.1 COMMERCIAL, ENTERPRISE AND DOMESTIC SECURITY EVENT

SCAN TO REGISTER FOR YOUR FREE PASS

FIND OUT MORE: WWW.THESECURITYEVENT.CO.UK

Co-located with:

PROFESSIONAL SECURITY OFFICER LIVE

NATIONAL CYBER SECURITY SHOW

THE FIRE SAFETY EVENT

THE HEALTH & SAFETY EVENT

THE WORKPLACE EVENT

Lead Media Partner:

Security MATTERS

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

Durabook expands rugged tablet portfolio

Durabook has announced the availability of two rugged tablet models specifically designed for use in locations where gases, vapours, dust and other substances create a significant risk of explosion. The Durabook R8-EX and U11I-EX Windows 11 tablets are certified to meet the EU ATmosphères EXplosibles Zone 2/22 certification, meaning they can be used in environments where potential ignition sources include lightning strikes, stray currents, static electricity, open flames and mechanically generated sparks. Both models feature Coolfinity fanless cooling, which enables them to operate safely in hazardous industries where standard laptops and tablets cannot. By eliminating the need for a fan, Coolfinity also maximises reliability and battery life by removing a component that consumes power, is a potential point of failure and vacuums dust and other debris into the device. The new Durabook R8-EX and U11I-EX tablets are designed to meet those requirements and more with Intel 12th generation processors, Windows 11 with Secured-core technology to provide an extra layer of protection and Durabook's proprietary DynaVue display technology to ensure readability even in direct sunlight. The R8-EX has an 8in display and the U11I-EX features an 11.6in one. Both tablets' displays support four touch modes (glove, stylus, water, finger) and an optional digitiser.

Burg-Wächter unveils C-Line padlocks

Burg-Wächter has introduced its C-Line range of tough brass cylinder padlocks. Designed to the same exacting standards associated with German engineering, the range has been created to ensure that valuables are kept safe. The locks boast a tough solid brass body, hardened steel shackle – making it resistant to hacksaws – and its double-bolted mechanism. There are two options in the C-Line range to choose from; the 222 C-Line features a standard size shackle while the 222 HB C-Line incorporates an extra-long shackle. With the 222 C-Line coming in nine different sizes, ranging from an internal shackle height of 35-87mm and the 222 HB C-Line boasting three sizes, from 50-103mm, Burg-Wächter's C-Line range comes with two keys as standard.

GA-ASI'S Gray Eagle 25M UAV conducts first flight

General Atomics Aeronautical Systems, Inc. has conducted the first flight of the Gray Eagle 25M (GE-25M) Unmanned Aircraft System. The flight marked a significant milestone in the Gray Eagle modernisation programme as the US Army continues to develop the Multi-Domain Operations-capable GE-25Ms for US Army active duty and National Guard units. The first flight focused on flight critical operations, including the testing of the improved flight computer boasting 5x more processing capacity and 80x more data storage (with 10x more RAM) for increased computing power that enables processing at the edge, as well as meeting the demand for increased automation and autonomy. The flight tested the aircraft's new HFE 2.0 engine and power generation systems. Designed in cooperation with Project Manager Endurance Uncrewed Aircraft Systems, the new engine, gearbox and generator design decreases major maintenance actions and virtually eliminates the need for overhaul.

Sepura Broadband hand-portable device

Sepura has launched its SCL3, a rugged broadband hand-portable device to complement its SCU3 Hybrid Broadband Vehicle Device. The SCL3 reduces the risk and costs of migrating to Mission Critical Services (MCX) by providing hybrid solutions to help bridge the Transition. The device has the flexibility to be deployed as LTE only or as hybrid TETRA and 4G/5G, providing a powerful device to enable the migration to mission-critical broadband communication. The SCL3 is a 4G/5G rugged handheld device that addresses the requirements published by NCCOM Nordic operators. PPDR (Public Protection and Disaster Relief) users are accustomed to rugged TETRA devices with physical buttons for PTT, emergency calls; these requirements are carried forward into the SCL3 LTE and hybrid device. The physical characteristics of the device support frontline operation in all environments, which include shifting temperatures, humidity and wet conditions. A long lifecycle, with continuing support for hardware, chipset, battery and software are also an essential part of the SCL3 value proposition.

3DX-Ray launches cabinet-style mail screening X-ray system

3DX-Ray has announced that its established Axis-CXi system cabinet-style mail screening X-ray system is the first to fully integrate AI machine learning software functionality. Designed to revolutionise mail screening and building entrance security, the newly integrated AI software adds an intelligent layer to the AXIS-CXi cabinet X-ray system, providing unparalleled accuracy and efficiency in threat detection. Key features include enhanced threat recognition: the AI software employs cutting-edge algorithms to identify and analyse potential threats with an unmatched level of precision and confidence; efficient mail screening: the system streamlines mail screening processes, ensuring a rapid yet thorough examination of incoming mail for any suspicious items; building entrance security: with real-time threat assessment, the AXIS-CXi system contributes to bolstering security at building entrances, safeguarding against unauthorised or potentially harmful items, including firearms, ammunition, sharp objects and drones; and a user-friendly interface: the intuitive user interface ensures ease of operation, allowing security personnel to make informed decisions swiftly.

TSCM & SECURITY SOLUTIONS

Delivered globally by the world's largest TSCM company

TSCM solutions

- TSCM Inspections & Live Monitoring
- CYBER TSCM
- Equipment Design & Manufacture

  - *Sentinel, BlackLight & Lynx*
- Equipment Supply & Gap Analysis
- Accredited TSCM Training (govt only)
- Physical Security Reviews

Security solutions

- Cyber Forensics
- Drone Forensics
- Cyber Incident Response
- Physical Penetration Testing
- Protective Security Services
- Threat Briefings & Consultancy
- Secure Communications

About QCC

Founded in 1999, QCC has grown to become the world's largest TSCM company with capability unique to QCC. We provide a comprehensive global service to commercial and government clients worldwide.

We are serious about what we do, and adopt a partnership approach to directly reduce our clients risk exposure.

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

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

ISO 17025

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

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