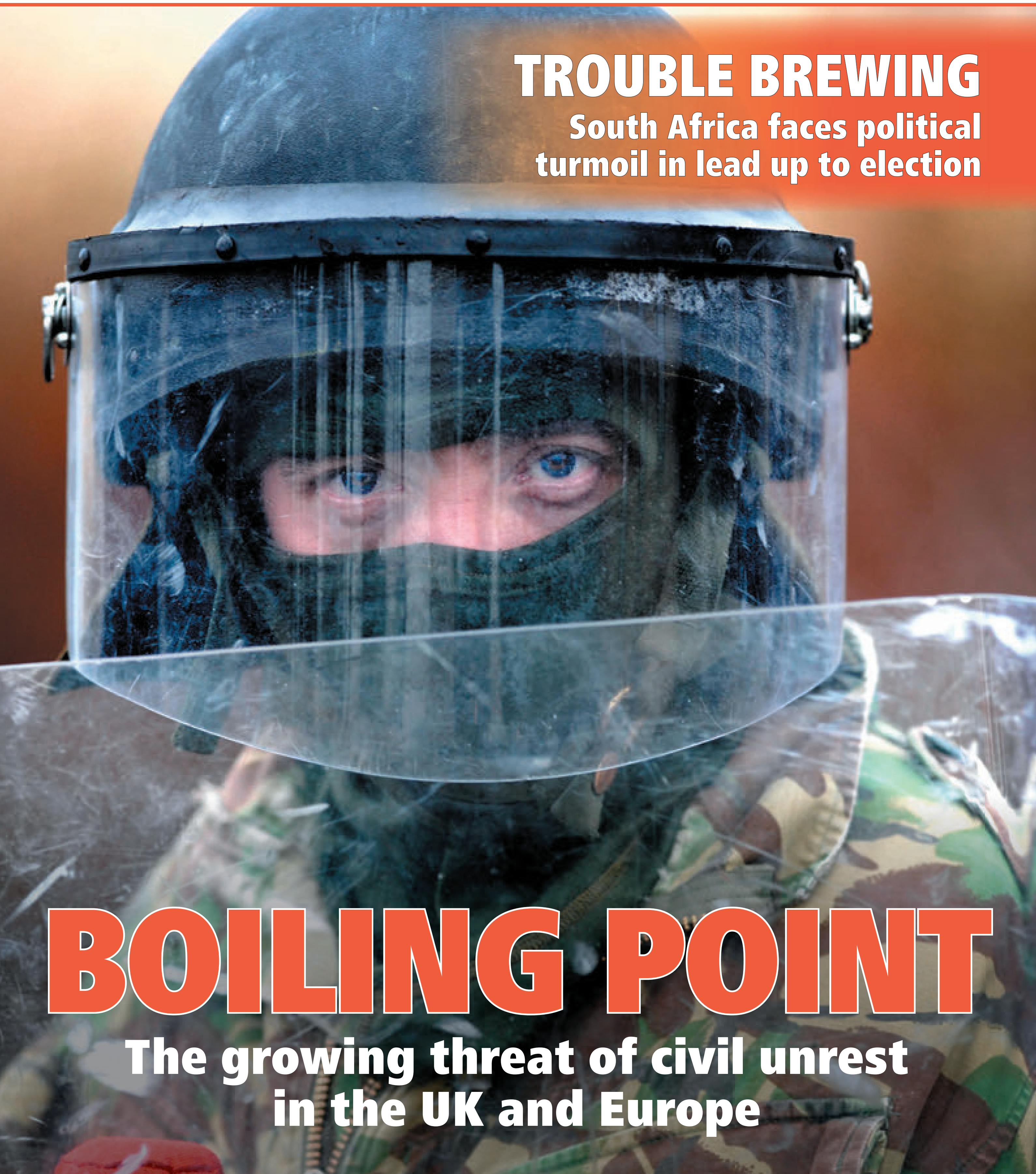
www.intersec.co.uk

intersec

The Journal of International Security

October 2022



TROUBLE BREWING

South Africa faces political turmoil in lead up to election

BOILING POINT

The growing threat of civil unrest in the UK and Europe

intersec

Volume 32 Issue 9
October 2022

Cover photograph: Crown Copyright

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

Cyber attacks against the UK's critical national infrastructure (CNI) are significantly outpacing current security budgets, according to research from UK cyber security services firm, Bridewell. The research saw the company survey 521 UK cyber security decision-makers in the communications, utilities, finance, government and transport and aviation sectors in March.

Firstly the good news: 70 percent of those questioned revealed that their company has increased its cyber security budgets over the past 12 months. However, despite rising investment in cyber security, 69 percent say it has become harder to detect and respond to threats, while 62 percent note that it takes their organisation too long to detect and respond to threats, and 60 percent admit to still struggling to understand how and why a breach occurred.

On average, UK CNI operators are now spending 39 percent of their IT budget on cyber security, with investment predicted to rise by a further 23 percent in the year ahead. However, the fact that many organisations are still struggling with the volume, sophistication and detection of cyber threats suggests cyber security investment is not being spent wisely.

Speaking about the results, Bridewell Director of Managed Security Services, Martin Riley, told *Intersec*: "It's encouraging to see that cyber security budgets are rising, however, without a strategic approach to cyber security transformation and investment, CNI operators risk wasting budget on tools and technology that fail to deliver the visibility and results needed. Operators must re-evaluate how they allocate and use their security budget, so that escalating cyber threats can be tackled with much more robust, proactive and holistic cyber security approaches, such as threat intelligence and detection and response."

Currently, only a quarter of those asked say that they have a managed detection and response (MDR) solution in place and even less (20 percent) have implemented extended detection and response (XDR) to enable detection and response capabilities across network, web and email, cloud, endpoint and most crucially, identity. Similarly, only a fifth say they have implemented threat hunting and cyber intelligence processes. Poor cyber security investment choices could also be causing problems with visibility. Seven in 10 CNI cyber leaders admit that they don't have sufficient visibility across the IT/OT boundary while 64 percent do not have sufficient visibility over all end user, networks and systems.

Problems could also be a result of over investment in security tools with 62 percent admitting the number of security tools within their organisation is unmanageable. On average CNI security teams are managing 33 security tools, with 35 percent managing over 40 tools. Not only does too many tools stretch security teams too thinly across disparate and poorly developed solutions, but it increases the complexity of monitoring, managing, operating and optimising a technology stack.

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: October 2022

CONTENTS

October 2022

www.intersec.co.uk

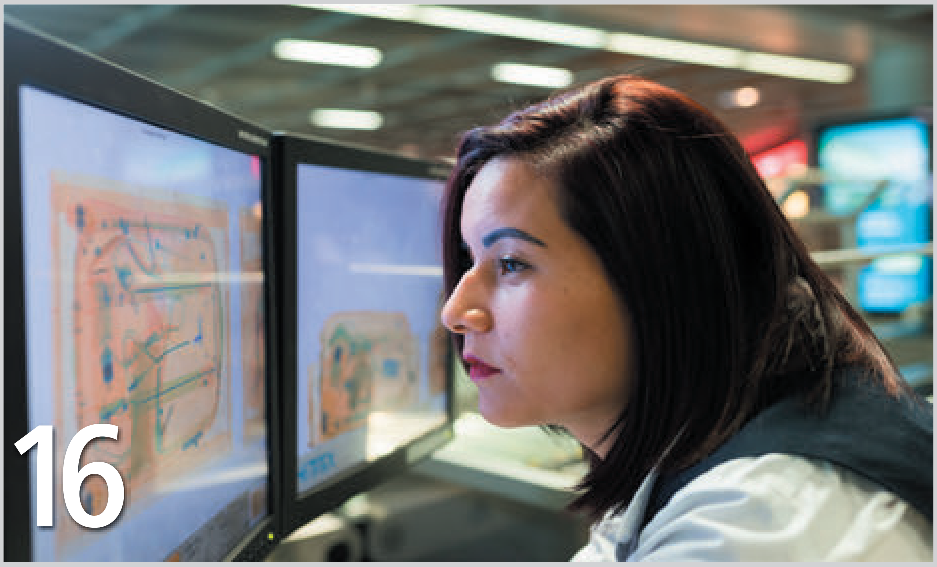
intersec

Features

Regulars

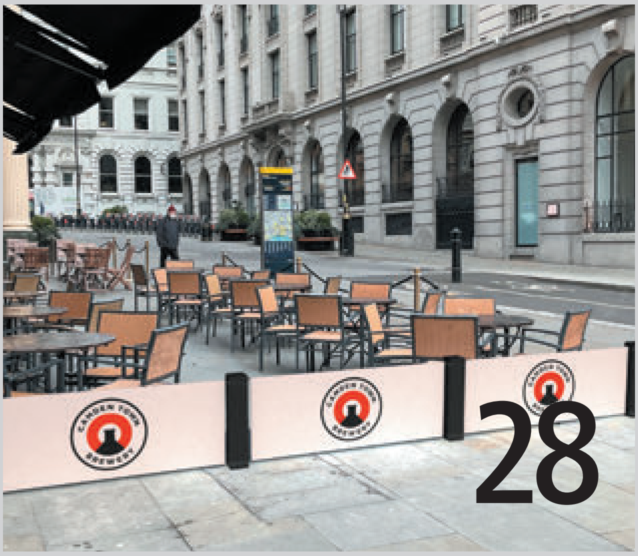
8

12



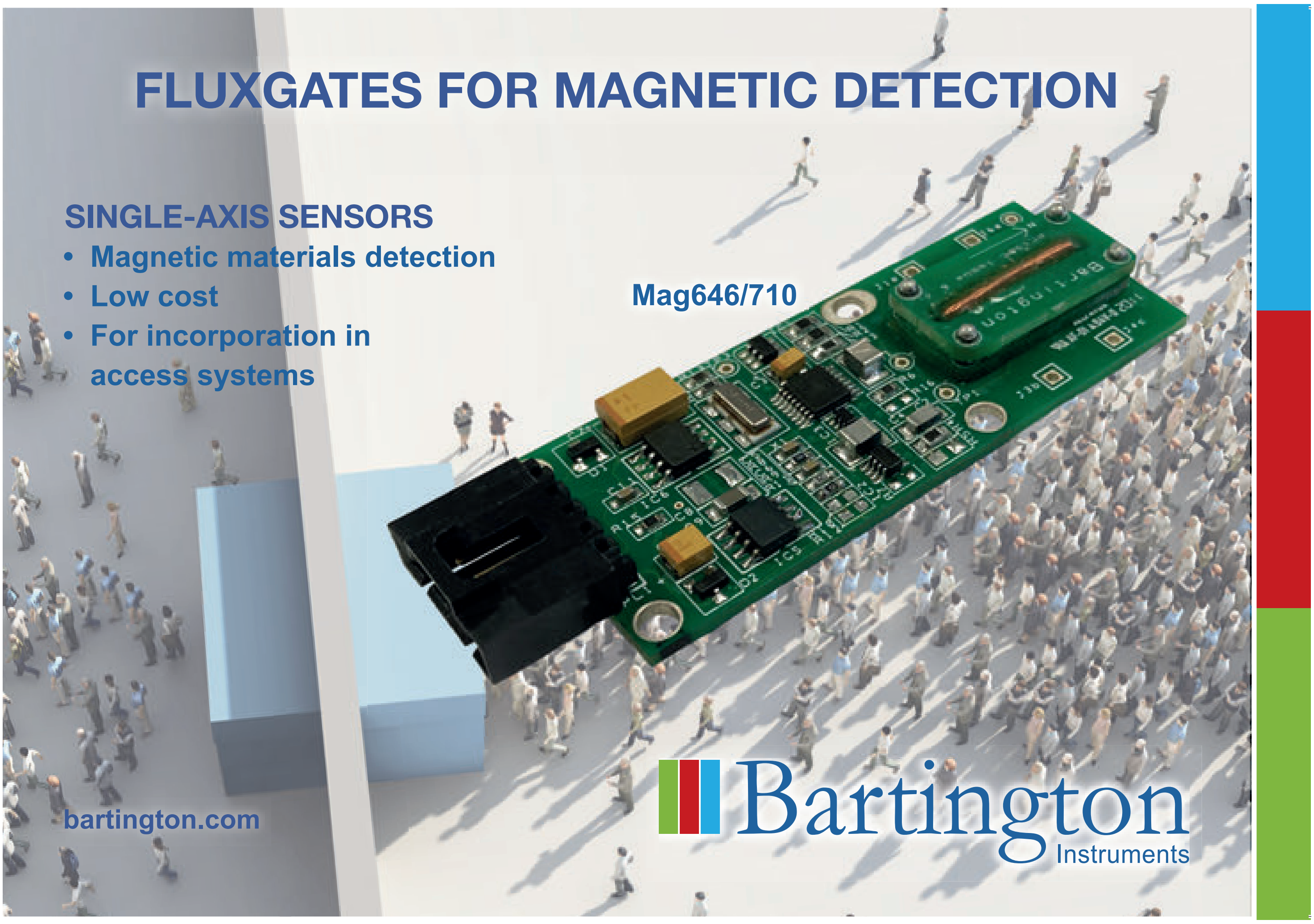
16

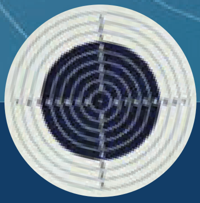
22

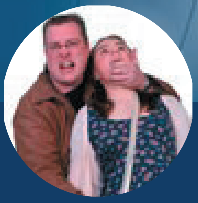

28

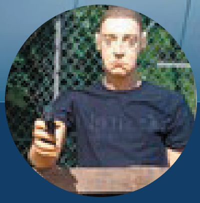
32

THE APP SCANS VARIABLE HOLOGRAMS
WITH HOLOGRAPHIC VARIABLE ENCRYPTED INFORMATION
SCAN
IDENTITY CARD
CARTE D'IDENTITE
ABROADIA
SMITH
SUSAN
Abroadian
07 02 1992
F
B80000012
25 11 2021
24 11 2031
Signature
BAUER +MÜCK
IDENTITY CARD
CARTE D'IDENTITE
ABROADIA
SMITH
JOHN
Abroadian
15 02 1985
M
B80000011
25 11 2021
24 11 2031
Signature
BAUER +MÜCK
36









Is Putin bluffing?

Major General Julian Thompson CB OBE Principal Consultant Editor

Media coverage of the war in Ukraine has recently been driven off the front pages by other events in Europe and the US. That said, enough information has been emerging to indicate that all is not going well for Russia both in the campaign and domestically. The Russian reaction to conscription is an indicator of the attitude of many Russians who hitherto supported the war. The way the draft is being conducted has attracted much criticism from several Russian governors who fervently supported the invasion of Ukraine. This domestic chaos is reflected on the battlefield. Putin has sacked the senior general in charge of logistics and assumed an increasingly hands-on role directing strategy, apparently telephoning frontline commanders and overriding their decisions. The deputy defence minister (four-star General Dmitry Bulgalkov has been removed for his poor handling of logistic support and replaced by Colonel General Mikhail Mizintsev. One of the major logistic challenges he faces is equipping, training and deploying 300,000 reservists who are being called up. At least seven more senior generals have been fired. Lieutenant General Roman Berdnikov lasted a mere 16 days as commander of the Russian Army's Western Military District after suffering a series of crushing defeats in Kharkiv.

Picture credit: US Dept Defence

Putin's announcement: "If the territorial integrity of our country is threatened, we will certainly use all the means at our disposal to protect Russia and our people... this is not bluff," has gained the attention of people in the West. Russia's tactical nuclear arsenal is limited in range to around 300 miles, with yields of around 10 kilotons (the atomic bomb dropped on Hiroshima had a yield of about 15 kilotons). It is assumed by all experts that Putin is threatening the use of tactical rather than inter-continental ballistic missiles with vastly greater ranges and yields.

Will he use his tactical nuclear weapons? Putin is clearly irrational and if cornered might do so. Professor Sir Lawrence Freedman, the eminent war studies expert at King's College London, has said: "The potential targets for limited nuclear strikes [in Ukraine] are those already identified for conventional strikes – critical infrastructure more than cities." He also pointed out in a blog post that Snake Island, which is uninhabited, could be used as a demonstration target to show Russia's power and to sow fear in Ukraine and the West.

Putin has the power under Russian law to launch nuclear weapons in the event of an existential threat. He is said to always have at hand a 'cheget', or nuclear briefcase, that connects him to the command-and-control centre of Russia's nuclear arsenal. But the cheget does not include a nuclear 'red button'. Instead, it transmits the order to the Russian General Staff or central military command. This central command has two ways of starting a launch: they can either send codes to weapons commanders or use a back-up system that bypasses all chains of command to launch land-based nuclear weapons. If Putin opens his cheget and gives the order to launch nuclear weapons on Ukraine or a NATO member, will the Russian Central Command obey, or will the order to launch nuclear weapons be a step too far for even his most loyal generals?

Putin has the power to launch nuclear weapons in the event of an existential threat

Western leaders have mostly dismissed his threats as bluff, despite his explicit insistence to the contrary and with some nuclear analysts pointing to a subtle shift in Putin's comments. Andrey Baklitskiy, an expert at the UN institute for disarmament research noted that Putin's statements go beyond Russian nuclear doctrine, which only suggests Russian first use in conventional war when the *very existence* [author's emphasis] of the state is threatened. But Baklitskiy has added: "Putin includes 'territorial integrity' and the very abstract protection of people, independence and freedom in the term existence". Which coming from a person, Putin, who has the sole decision-making power regarding nuclear weapons, must be taken seriously.

During the Tory party leadership contest, Liz Truss said she was ready to push the nuclear button even risking global annihilation. She is now Prime Minister of the UK, and statements made in political contests might be modified in the cold light of reality. The President of the US quite rightly has refused to elaborate in detail on his response to a potential chemical or tactical nuclear strike.

If radiation from a nuclear bomb in Ukraine spread to European allies such as Poland, this could trigger Article Five, which in turn could see UK and the US coming to Poland's defence. But how Germany, Italy, France and others would react is unclear. Would they really agree to a nuclear exchange over four provinces in Eastern Ukraine? Doubtful.

Recent remarks from China suggest that they are distancing themselves from the conflict, urging a: "ceasefire through dialogue". Some nuclear experts have stated that any move by Russia towards tactical nuclear attacks will lose them their most valuable ally, China. Possibly.

Picture credit: Getty

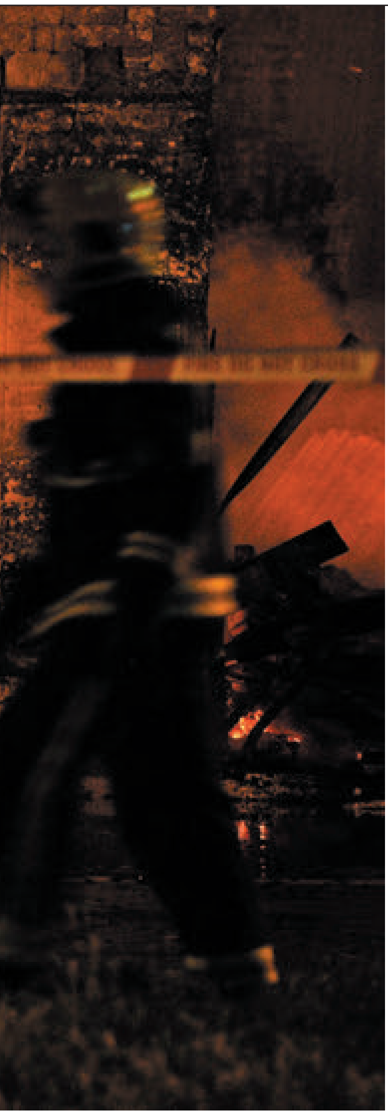
RISING TENSION

Robert Hall *questions whether or not we are in for civil unrest as we appear to face the winter of discontent to end all winters of discontent*

Mark Twain is reported to have said that: "History doesn't repeat itself but it often rhymes". This is true of civil unrest in many contexts and the echoes in modern Britain are less than harmonious. We are today facing a perfect storm of lights and livelihoods. Societal pressures – economic, health, environmental – are forcing many citizens to face going backwards in terms of living standards and opportunities.

Even with the financial help being offered by the new government, this winter is looking particularly bleak for many families with rising food and energy prices. It is therefore perhaps unsurprising that the spectre of societal unrest is rearing its ugly head. This may go beyond co-ordinated protest marches and include an uptick in acquisitive crime such as shoplifting, burglary and vehicle/fuel theft as well as online fraud and blackmail. Contingency planning by police chiefs is said to be underway to deal with any unrest.

The UK has been here before in various guises even in the past half-century. With the oil embargo of 1973, when the oil price increased by 300 percent over six months, a



Almost half of Britons surveyed fear riots this winter

three-day week was introduced and there was a 50mph speed limit on motorways. Coupled with a series of strikes by coal miners and rail workers over the winter of 1973-74, the oil shock became a major factor in the defeat of Heath's government in the 1974 general election. The subsequent Labour government told the country to heat only one room in houses over the winter; today, the suggestion of an extra pullover is deemed condescending.

The so-called 'Winter of Discontent' of 1978-79 was characterised by widespread strikes by private companies and later public-sector trade unions demanding pay increases of up to 17 percent, well above the 5 percent government ceiling. The unrest led to the fall of the Callaghan government.

The poll tax riots of 1990 were a turning point for the Thatcher government. One protest theme was 'Don't Register, Don't Pay, Don't Collect'. During the early months of 1990, over 6,000 anti-poll tax actions were held nationwide, with demonstrations in cities around England and Wales drawing together thousands of protestors. London witnessed some violent scenes.

The riots of 2011 following the police shooting of Mark Duggan in Tottenham quickly spread across the country. They were mainly focused in London where property losses were estimated to total £100-million. Besides the specific response to the shooting (the spark that lit the flame), social factors such as racial and class tensions, economic decline and the unemployment that decline had brought were strong causes, and challenged the Big Society idea of the Cameron government.

Economic pressures are frequently behind popular displays of discontent. Today is no different. The gloomy economic outlook and energy crisis combine to make for uncomfortable parallels with yesteryear. In general, internal factors are more of a motivator for civil unrest than external ones but when they come together, as with the energy crisis, then the repercussions can be powerful. Recent government action to ameliorate the energy challenge may help to take the sting out the short-term situation but will not remove it for many: over 14-million households are already struggling to pay their energy bills.

Campaigns like Don't Pay UK, Enough is Enough and We Can't Pay can be expected to continue and may herald the prospect of wider popular discontent. Furthermore, current industrial unrest in several sectors is unlikely to dissipate with inflation projected to be 10 percent or more. Even though trade unions' membership has dropped from 52 percent in 1980 to 23 percent in 2021, there is today an appetite for wider, possibly co-ordinated support for protest against the fall in living standards and the disparity in wages.

The prospect of violence cannot be discounted. According to a poll commissioned by *The Independent*, more than half of Britons think non-payment of energy bills are "justified" while almost half fear riots: some warn this winter could see a 'poll tax moment' for government. In another survey, over a quarter (29 percent) believe violent disorder is appropriate given the circumstances. Among 18-to-24-year olds, nearly half think rioting is "justified", and even among 35-to-44-year olds it is over 40 percent.

The challenges are widespread. One risk consulting firm, Verisk Maplecroft, sees a rise in civil unrest as 'inevitable' in middle-income countries which were able to offer social protection during the pandemic but will now find it difficult to maintain that level of spending as the cost of living surges. The consultancy's 'Civil Unrest Index' indicates that 75 countries will likely see an increase in protests by late 2022 resulting in, for example, a higher frequency of unrest and more damage to infrastructure and buildings. Finland is projected to experience the 16th biggest rise in protests globally over the next two years, followed closely by Sweden (21st) and Norway (34rd), all countries one would not normally associate with civil disorder.

In France we have seen disruption caused by the gilets jaunes movement, while officials in Germany have warned of an 'autumn of rage by extremists to exploit the cost-of-living crisis. In the capital of the Czech Republic, 70,000 demonstrators gathered recently to protest at soaring energy bills and demanded an end to sanctions against Russia over the war in Ukraine. Further afield, we have witnessed in Sri Lanka the overthrow of a government because of high prices and shortages of basic commodities and medicines.

CONTINGENCY PLANNING BY POLICE CHIEFS IS SAID TO BE UNDERWAY TO DEAL WITH ANY UNREST

The UN Secretary-General said in March that the destabilising potential of disrupted supply chains and surging commodity prices caused by the conflict in Ukraine is planting the seeds for political instability and unrest around the globe. According to the head of crisis management at the risk consultancy arm of Allianz: "civil unrest increasingly represents a more critical exposure for many companies than terrorism" and: "Incidents of social unrest are unlikely to abate any time soon, given the aftershocks of COVID-19, the cost-of-living crisis and the ideological shifts that continue to divide societies around the world".

The US consultancy OnSolve has revealed that while global protests increased only slightly from 2020 to 2021 (+4 percent) they increased by 59 percent in the US and 76 percent in the UK over the same period. The consultancy estimates that a single, large two-day protest occurring outside the headquarters of a Fortune 1000 company ($2-billion in revenue) costs $548,000. The disruption to the construction of the HS2 line by protesters has already cost £126-million.

The response to the challenges lies not just with the police and government. Businesses, both large and small, have a key role to play. The response can be considered at two levels. The first relates to practical, tactical measures to keep the business safe and able to continue to operate. The second relates to the wider social engagement that connects businesses to their employees, customers, communities and wider stakeholders through good stewardship and governance – elements of the so-called ESG (environmental, social, governance) agenda.

On the first point, civil unrest can affect travel, operations, supply chain and even share price. Organisations should therefore view current events as a catalyst for evaluating best practices and policies, including preparing office locations and employees for

▶

potential disruption. The COVID-19 experience has provided useful preparation for certain measures like working from home where possible. Risk assessments, security reviews and resilience planning should be refreshed as a priority. Businesses need to be alert to the indicators and designate clear pathways for de-escalation and response which anticipate and avert the potential for personnel to be injured and/or damage to business and personal property.

Security measures in the face of protesters could include: ways to ground lifts quickly in the event of invasion, tools to cut chains and remove glue, video recording of actions and reactions, digital and loudspeaker messaging. In terms of trespass on to company property, people who become disruptive through verbal or abusive actions can be deemed to be trespassing through nuisance and be asked to leave.

CIVIL UNREST CAN AFFECT TRAVEL, OPERATIONS, SUPPLY CHAIN AND EVEN SHARE PRICE

On the second point, there is a growing expectation on business to do more to address societal problems, especially when trust in government (and the media) is declining. The Edelman Trust Barometer 2022 marks these trends and says that: "Societal leadership is now a core function of business". Business needs to work with other organisations, institutions and communities to foster innovation and deliver impact. If this doesn't happen, and leadership and trust deficits arise in both the public and private sectors, then it could rupture the ties that bind a democratic society together, and with potentially dangerous consequences. A weakening of the social contract, unless halted, will make the task of decision makers that much harder in the face of mounting domestic pressures, not just with energy. It is the degree of erosion to national solidarity and the loss of a unifying purpose that will determine the scale of the problem.

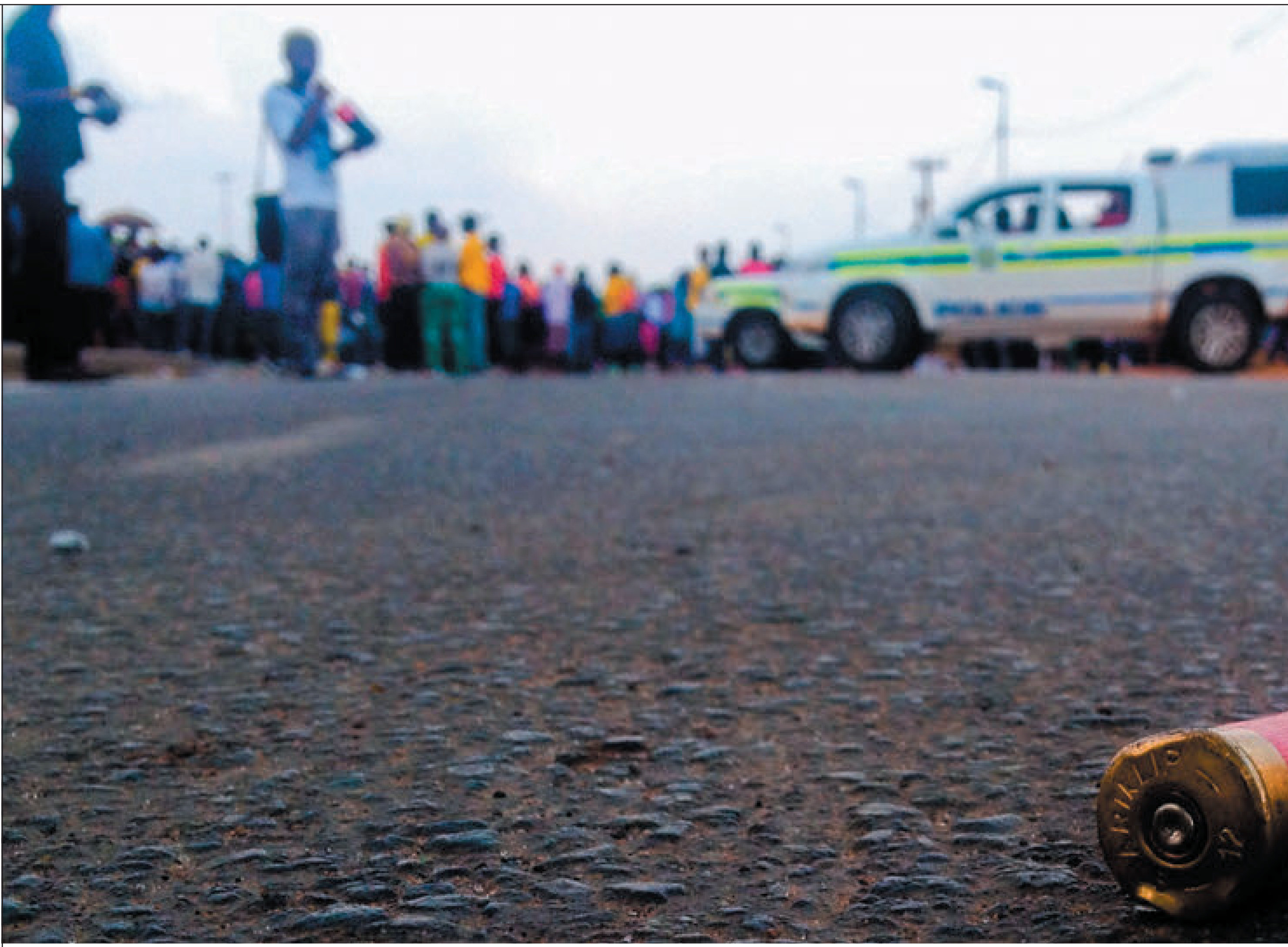
Hence, business should do more to help build the resilience of its workforce and the communities in which they and customers live. The John Lewis Partnership, for example, has decided to give free meals to all staff this winter to support them during the cost-of-living crisis. Many of the supermarkets already help with local food banks, while others support schools, youth clubs and care homes. More and wider engagement is needed. The activities can have a payback in terms of enhanced brand reputation, better customer loyalty, community cohesion, better awareness and improved diversity and inclusion. Additionally, potential employees and staff are now looking at the track record of organisations when deciding whether to join or stay. Those organisations that can demonstrate good resiliency measures are more likely to have a dedicated work force that will remain loyal and motivated. Importantly, they will also attract wider investment as the financial markets view ESG action plans as an indicator of success. While individual corporate actions may not remove the wider causes of civil unrest, they can help alleviate the worst direct effects.

The growing strength of special interest groups, a loss of trust in politicians to find solutions, social fragmentation and a diminution of societal responsibilities all contribute to a darkening picture. If a large swathe of the population cannot afford to heat its homes or to feed itself, or both, then vociferous, even violent, opposition may not be far around the corner. This is true for not just the UK as strains are appearing worldwide. Societal resilience may be tested as never before (short of war) and we need to pay attention to ways of strengthening it. President Putin may readily take advantage if we do not ●

Robert Hall is an independent consultant on resilience. He is the former Executive Director of Resilience First and has worked in the security and resilience domains for a number of FTSE100 companies. His book *Building Resilient Futures* will be published in late 2022.

Verisk Maplecroft's 'Civil Unrest Index' indicates that 75 countries will likely see a higher frequency of unrest and more damage to infrastructure and buildings before the end of the year

Picture credit: Getty



Picture credit: Bonging Ngcobo

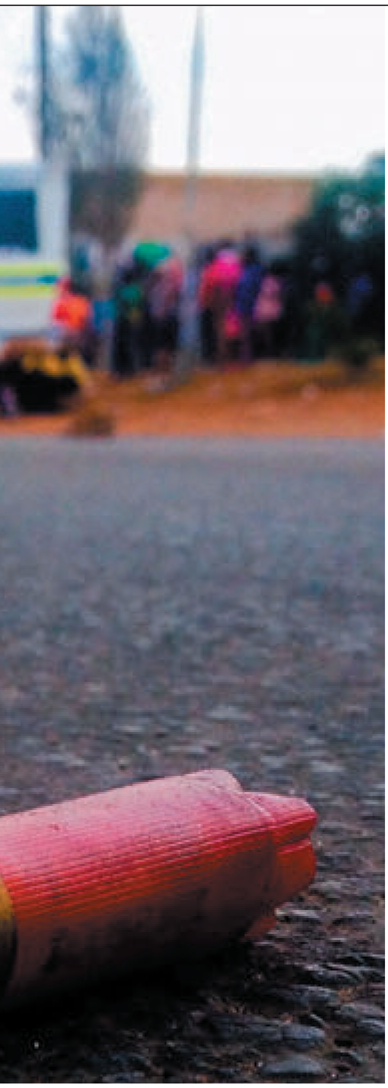
TROUBLE BREWING

Tamara Naidoo *explains how fragmentation within the ANC could lead to political turmoil in the lead up to the general elections*

This July, former South African president Thabo Mbeki warned that South Africa will experience an Arab Spring-like uprising, due to dissatisfaction with rising living costs and disillusionment with the political leadership. His comments naturally re-awakened business concerns about the country's long-term outlook; such dissatisfaction had already come to a head in July 2021 when a wave of unrest resulted in almost ten days of mass rioting and looting.

For now, those worries seem exaggerated and Mbeki's warning overblown, although it was a useful way to prompt South Africans to focus on systemic governance issues. While there are seemingly constant protests, most fall far short of the widespread unrest of 2021 and typically only cause localised disruptions for businesses. Since the unrest last year, the government and businesses are employing mitigation strategies, which seem to have worked well. So even though the unrest is unlikely to worsen, it's unlikely to get much better either – for now.

Trouble is on the horizon. South Africa is due to hold general elections in 2024 and the governing party, the African National Congress (ANC), is likely to lose its majority in



There were 1,178 protests in South Africa between January and July 2022

parliament for the first time in 30 years. This will result in a far more unpredictable terrain for businesses.

When the ANC successfully negotiated the end of the Apartheid regime in 1994 this was only the beginning of its mammoth task to rectify severe inequality in South African society. Over the decades since, South Africa benefited immensely from the ANC's ability to channel diverging political stances under its broad church. The party led the restructuring and liberalisation of the South African economy. This was made possible as it brought together both powerful unionists and business leaders from its membership to strengthen policy debate and facilitate compromise.

But while the ability to compromise was once its strength, now the party's emphasis on negotiation has become its curse. This is because polarisation within the ANC has resulted in political indecision and delays that have both elevated strategic risks for businesses and accentuated the drivers for protests in the country; these are primarily relating to economic hardship, poor service delivery and political infighting.

In recent years, political and community-based activists have frequently organised protests in central urban areas and the low-income periphery of cities. Data from the Armed Conflict Location and Event Data Project (ACLED) shows that the frequency of these has consistently increased; there were 1,178 protests nationwide between January and July 2022, up from 876 during the same period in 2019. Most demonstrations occurred in Gauteng, Kwa-Zulu Natal and the Western Cape and were relatively small, causing minimal disruptions for businesses. Community protests typically attract up to a few hundred people and pockets of violent protesters often attempt to block roads and throw stones at security forces.

Protest data shows that the three drivers often run concurrently in any given protest. Economic hardship was already worsening in the country prior to the pandemic in 2020. This fed a high frequency of protests well before the subsequent global economic slowdown. Poverty and stubbornly high rates of inequality were partly caused by systemic policy failures. For example, poor policy led to unnecessary delays in national electricity provision reforms, and this has similarly led to sub-standard infrastructure on a municipal level. For businesses, this has meant that their day-to-day operations are an ongoing challenge due to deteriorating water and road maintenance.

Then there's the ANC's internal politics. Far from its initial role as mediator, today's ANC has become a driver of protest. The ANC has always had factions. But in recent years infighting between the two factions, those aligned with ANC president Cyril Ramaphosa and those aligned with former ANC president Jacob Zuma, have increasingly used subversive tactics, such as stirring protests. The risk of these is most acute over the short-term in the run-up to the ANC electoral conference this December where party members elect the 'top six' positions in the party, including the president (of both state and party).

As this draws closer, jockeying between rival factions in the ANC is likely to prompt more frequent protests in major metropoles along with increased incidents of targeted political violence in Kwa-Zulu Natal, Eastern Cape and Mpumalanga. In previous ANC elections politicians or hired thugs have instigated anti-government protests to boost their profile for nomination at the ANC electoral conference. In low-income areas these would probably turn violent, for example in July protesters burnt two trucks in Pietermaritzburg. Still most violent incidents would be unlikely to spread because the instigators tend to have highly localised support bases.

However, this fragmentation in the ANC presents businesses with greater risks including those pertaining to violent rioting and wildcat strikes. The potential for security incidents of this kind is related to two dynamics. The first is the use of subversive tactics by competing factions and the second is the governance risk emanating from the ANC's alliance with worker unions breaking.

THE FRAGMENTATION OF THE ANC IS SET TO UNDERMINE BASIC BUSINESS PRACTISES

The widespread rioting of July 2021 stemmed from competition between the Ramaphosa camp and the Zuma camp. Official state and media-led investigations have suggested that high-level ANC affiliates orchestrated the July unrest to pressure the Ramaphosa government into halting criminal proceedings against Zuma. Based on this precedent, the ANC electoral conference is an important monitoring point.

A clash between factions is unavoidable because several high-level cadres associated with Zuma's faction, with open criminal cases against them, are ineligible to compete in the December elections. So it's possible that these excluded members would at least attempt to instigate a more coordinated campaign of local riots in an effort to undermine both Ramaphosa's popularity and his credibility as a leader, before December. For now though, aside from Zuma there is no other single convenor capable of mobilising inter-provincial riots like those that happened last year; so any such riots would probably remain local.

The second dynamic that has emerged with the fragmentation of the ANC is the increasing likelihood of wildcat strikes. These can have a debilitating impact for industrial players. Until now wildcat strikes have only been occasional due in part to the ANC's internal negotiation capacity with trade union members. But many unionists seem to feel unrepresented by union leaders as the leadership is increasingly perceived to be in cahoots with unreliable ANC leadership. Unionist distrust of the official ANC alliance has prompted more brazen unionist action in recent months. In August unionists interrupted electricity supply in major economic hubs for several days due to a wage dispute. And within weeks of this, trucker unionists blocked a major freight route over the employment of foreigners.

Still there have not been signs to suggest union leaders would follow through on threats to break the ANC alliance. This implies some discipline among lower-rung unionists is likely to be maintained and with that the ANC would earn the largest proportion of parliamentary seats in the next election.

Where protests do break out, the government seems intent to adhere to its strategy of negotiation along with reinforcement from security forces, equipped with tear gas and water cannons. However, with the breakdown in ANC leadership and the salience of other protest drivers, these efforts would at most shorten disruptions, rather than reduce the number of strikes and protests. They are unlikely, however, to retain their majority, which makes the 2024 elections a game-changer for both the general political environment and for businesses.

Based on Ramaphosa's popularity in opinion polls, the ANC will keep Ramaphosa as president of the party for the election, irrespective of factional battles. Ramaphosa has so far struggled to uphold the business-friendly approach for which he is known. But a strong Ramaphosa camp in the ANC would stick to their initial mandate of increasing private sector participation in the economy, along with other needed reforms such as sprucing up anti-corruption measures, removing barriers for new businesses.

ECONOMIC HARDSHIP WAS ALREADY WORSENING IN THE COUNTRY PRIOR TO THE PANDEMIC IN 2020

Nonetheless in the scenario where there is strong representation of Zuma's camp in high-level ANC decision-making, Ramaphosa's pro-business approach would be challenged by those pushing for radical policies, related to nationalisation and land expropriation. Such attempts in 2023 would be tempered by the current parliament, but post-2024 this would depend on the political values of an entirely new governing coalition.

With shifting factional battles ongoing in the ANC, it is not yet clear who would be selected to partner in a coalition government. If the Zuma camp has a strong presence in ANC leadership, it would likely partner with the third most popular party in the country, the Economic Freedom Fighters. This is a leftist, disruptive party that would assist the Zuma faction to push for radical economic policies to dismantle the 'capitalist monopoly'. Though there are signs that socioeconomic pressure would probably make this more difficult for the coalition to carry out, the threats of such policies would shake investor confidence further.

Even if a strong Ramaphosa camp is elected at the ANC conference in December and the ANC selects the second-most popular party – the liberal Democratic Alliance party – the outcome would be the same. Prolonged policy debate and political deadlock is inevitable, meaning there will be a period of policy uncertainty for several months at least.

Based on the current deterioration of national and local government administration, after the 2024 general elections most South African institutions would not be robust enough to adequately respond to protest triggers such as spiralling living costs or politically instigated unrest without clear guidance from the central government. And this would have a negative impact on systemic issues such as corruption and critical infrastructure because any pre-2024 government plans would be re-evaluated by the new coalition government, causing delays. As such a far more challenging operational environment awaits businesses after 2024.

Going forward, the fragmentation of the ANC and factional infighting between the Ramaphosa and the Zuma camp is set to undermine basic business practises in the country. And instead of mitigating the impact of ANC infighting, the general elections will only embroil another set of political actors in policy discourse and execution. As a result, businesses will have to contend with an even more unstable government in addition to an already high frequency of protests. This will stifle the economy, escalate protests and deepen the litany of issues which the country is already grappling with – not least, as far as businesses are concerned – the security risks of unchecked and increasingly brazen attacks by sophisticated criminal networks. Civil unrest, therefore, may prove to be a distraction from South Africa's larger problem, which is the breakdown of its political leadership ●

Tamara Naidoo is an intelligence analyst for the Africa desk at Dragonfly, a geopolitical and security intelligence service for professionals who guide decision making in world leading organisations.

Jockeying between rival factions in the ANC will cause more frequent protests in major metropoles

NEW TTK TACTICAL TSCM KIT

The TTK weighs approximately 25lbs/11.3kg - for easy transport.

MESA® hand-held Spectrum Analyzer

ANDRE® Broadband Detector

ORION® 2.4 HX
Non-Linear Junction Detector

CMA-100 Countermeasures Amplifier

Compact, Portable, Tactical

The TTK Tactical TSCM Kit is packaged for mobility in a durable hard shell carry-on case that includes necessary tools for an effective TSCM sweep.

- Locates hidden electronics, transmitters, microphones, and illicit surveillance devices
- Includes Spectrum Analyzer, Broadband Detector, NLJD, Audio Amplifier, *thermal industrial multimeter, and accessories
- Double layered custom foam
- Retractable extension handle
- Quiet rolling stainless-steel bearing wheels
- Weighs approximately 25 lbs/11.3 kg

*Kit contents may vary

International Procurement Services (Overseas) Ltd
118 Piccadilly London W1J7NW
Phone: +44 (0)207 258 3771
Email: sales@intpro.co.uk

REI®

www.reiusa.net

Picture credit: Smiths Detection

THE X-FACTOR:

Matt Clark *explains why the versatility, effectiveness and ever evolving nature of X-ray makes it the cornerstone security screening technology*

It is a sobering reality that we face an array of complex and evolving security threats, presenting real danger to lives and putting assets at risk. The good news is that there are multiple layers of security that can be applied to effectively tackle these threats. These approaches range from everything from trained sniffer dogs to manual inspections by security personnel and X-ray scanners. Each method has its benefits, but X-ray security equipment is the most commonly deployed due to its accuracy, ease of use and operational and cost effectiveness. By reducing manual processes, it increases efficiency and boosts security outcomes. Indeed, X-ray has been central in threat detection for many decades and with technological advancements enhancing the capabilities of X-ray based solutions, it continues to future proof security operations.

Put simply, X-ray detects hidden threats without intrusion. It uses radiation at safe levels depending on the application and environment, and is extremely versatile – in terms of its applications, scalability and the choice of low/medium/high energy levels in line with requirements. In essence, X-ray comes in many different shapes and sizes to answer different needs – and while some applications require certified systems, some don't. It is used for screening, mail and parcels, personal bags at checkpoint security, baggage or freight in containers, vehicles and trains. It helps with identifying explosives, dangerous goods, weapons and contraband in many different kinds of environment – and is safe, causing no harm to people or baggage.

X-ray security screening has developed since its inception. Early iterations of baggage screening systems

CT scanners eliminate the need to take liquids and electronic devices out of luggage, creating a more frictionless experience at the security checkpoint

had only a single stationary X-ray detector and were lower resolution – and while this is still the standard for many applications, increasing computing power has improved single-view system performance, while dual and multi-view systems have been developed to enable more sophisticated screening methods.

Advancements in X-ray technology have solidified its essential role in screening for security threats. Computed Tomography technology is one such advancement for X-ray based security screening. CT has enhanced X-ray scan images – enabling high-definition, 3D, rotatable, full-colour imagery. The benefits of CT are wide-ranging – it speeds up evaluation time, delivers more accurate outcomes, low false alarm rates, minimises touch points and relieves operator burden.

Let's take airport security as a case study for the potential of CT-enhanced X-ray scanners. When it comes to the airport passenger journey, the security screening process is typically seen as one of the most stressful points. With the removal of shoes, belts and jewellery, having to separate belongings into trays and taking electronics and liquids out of bags, queues tend to build and so does passenger impatience. That's where computer tomography comes in. Typically employed in the medical sector, and as mentioned, CT technology generates 3D, volumetric x-ray images. In the context of airport security, CT scanners enable security operators to inspect baggage from every angle. The growing adoption of this technology by airports around the world is great news for passengers, with CT scanners eliminating the need to take liquids and electronic devices out of luggage, drastically cutting queuing times and creating a more frictionless experience at the checkpoint.

In the US for example, the Transportation Security Administration (TSA) is working to implement CT technology and has already installed over 300 scanners, allowing passengers to keep laptops and electronic devices in their carry-on bags to minimise touch points during the screening process. CT scanners – which are being adopted around the world – also support the enhanced health and safety measures implemented at airports, by decreasing the level of contact between passengers, screeners and surfaces, such as trays. With automatic detection capabilities and low false alarm rates, unnecessary interaction between passengers and operators is reduced and physical distancing among travellers can be more easily implemented with quicker screening. With liquids and laptops being allowed to remain in bags during screening, the number of trays handled by both staff and passengers is drastically reduced.

Further enhancements to X-ray capabilities are being unlocked through the deployment of artificial intelligence (AI), which can enable automatic object recognition. Through machine learning and its subset deep learning, algorithms can be developed that imitate the way the human brain processes data and identifies patterns based on examples to inform decision-making.

In this way, AI-based algorithms can detect prohibited or contraband items such as weapons, dangerous goods, currency or cigarettes and support operators in making fast and accurate decisions. This not only boosts operational efficiency, but also the security outcome. For the development of deep learning algorithms for security scanners, a library of X-ray images is shown to the algorithm so that it can learn to identify patterns in the shape of items, such as guns, gun parts, ammunition and knives or other potentially dangerous prohibited items such as lithium batteries. While the list of objects that AI algorithms can detect is ever expanding, deep learning is currently limited in that it cannot yet detect substances or items which are inconsistent in shape. However, traditional material property discrimination-based techniques, when combined with machine learning, can be powerful for detecting such objects. The use cases for AI-based algorithms are wide ranging. They can be deployed for screening systems at airports, in urban environments or public spaces and at ports and borders.

CT SCANNERS ENABLE SECURITY OPERATORS TO INSPECT BAGGAGE FROM EVERY ANGLE

AI algorithms are particularly helpful for less experienced image analysts. As algorithms cannot get tired or distracted and are impartial, they reduce the risk of human errors, resulting in improved security outcomes. More automated screening processes can also reduce operational expenditure, as with greater screening efficiencies and productivity fewer staff are required. By increasing throughputs and reducing manual processes requiring physical contact, the security screening experience becomes significantly less stressful for those being screened.

With a very high level of detection, these AI algorithms also drive down false alarm rates. There is also potential to combine the automatic explosives detection capability of a scanner with object recognition to enable 'alarm only viewing' of X-ray images, further accelerating throughput.

Another critical enhancement for X-ray based scanners is centralised networking or remote image evaluation. Although well established for airport hold baggage screening systems and border control, remote screening is not yet widely used for airport passenger checkpoints and cargo – and is particularly beneficial for major hubs, with high volumes of traffic or cargo. When a security network spans regional outposts – which see fluctuating volumes of either goods or traffic – it is advantageous to link all outlying locations to a centralised hub where volumes are more stabilised. This enables more efficient operator resourcing, meaning that staff do not have to stay onsite at smaller locations around the clock. At borders, a centralised screening and management system can allow X-ray images and associated data to be analysed online in a remote-control centre. On-site operators can therefore focus on the scanning process and completing the relevant dataset information, such as customs declarations and vehicle licence plates.

On a country-to-country or even continental level, image sharing via Wide-Area Networks (WANs)

▶

can be deployed to facilitate the real-time sharing of images between different sites, enabling greater resource prioritisation and operational efficiency. WANs enable detailed data analysis across global security networks to enhance security levels, with one set of scanned images for both outbound security and inbound customs clearance at the destination. As security outcomes can never be compromised, it is necessary for wide networks to be secure, with sufficient bandwidth for real-time distribution of the images. Establishing a viable, robust WAN is therefore no mean feat, with back-up solutions needed in the event of network failures.

> **X-RAY DEVICES HAVE BEEN CENTRAL IN THREAT DETECTION FOR MANY DECADES**

At the most cutting-edge of X-ray systems development is Open Architecture (OA). OA allows security authorities to incorporate new security and technology components into their screening systems through 'standard interfaces', which means different systems can work in tandem. Principally, OA enables integration of third-party algorithms into X-ray based security scanners, delivering interoperability and system flexibility. This means different fleets can be updated with the most advanced and latest software to take advantage of new technologies, such as AI, to meet an ever-growing and changing list of potential threats. Not only does OA therefore have the potential to improve security outcomes, but also operational efficiency and the ability to meet evolving regulation. OA also can allow for screening results to be shared between different authorities, despite them having different fleets and service providers, and can enhance centralised image evaluation, enabling operators to review screening imagery in remote operator rooms, optimising the operator to scanner ratio through multiplexing. It should be noted, however, that best practices around OA are still to be universally agreed so that it can be deployed in a way which maximises its benefits and does not compromise screening data or system effectiveness.

Looking to the future, the introduction of X-ray diffraction scanners will enable more precise material analysis and further operational efficiency when scanning cargo and baggage. The use of diffraction as an orthogonal technology unlocks the benefits of a system of systems approach, vastly increasing scanning capabilities. The technology provides higher levels of accuracy in the material analysis and detection of substances, resulting in a reduction of manual intervention. This enables automated alarm resolution, so that operator resources can be more effectively prioritised. By extending the capability of scanners, diffraction can future-proof security operations against emerging threats and regulatory changes.

What is clear is that X-ray is here to stay. For many security operations designed to protect people, infrastructure and institutions, it is the most effective and efficient approach to tackling the threats of today – and with software and AI growing its capabilities, the threats of the future. With digital augmentation, X-ray will continue to be a cornerstone security technology – with increased automation paving the way to a fully contactless and highly efficient security process ●

Matt Clark is Vice President Technology & Product Development at Smiths Detection.

> **As algorithms don't get tired or distracted and are impartial, they reduce the risk of human error**

Picture credit: Smiths Detection

A DIFFERENT APPROACH

Why innovation is at the heart of Securiscape

Picture credit: Securiscape

He may have personally overseen every aspect of his company's product development programmes, but there is always one stage Securiscape managing director Mark Stone cannot watch – the impact test.

"In 18 years of running this company," says Mark, "I have never been able to watch the crash tests. "The night before them I'm a bag of nerves and my mind's full of thoughts about whether the product is good enough or what we might have left out. Then the next day I always crouch down behind a car until it's over because I don't want to see what happens. There's just too much at stake."

In the case of Securiscape's innovative Glide Bollard flexible HVM barrier system, he need not have worried. Released last year after a three-year R&D programme, the bollards underwent a series of successful crash tests to earn their IWA 14 rating, proving that they can withstand the impact with a 7.2 tonne truck travelling at 40mph.

In one memorable incident the truck had far more to fear than Mark did. In the aftermath of its test it was discovered that the truck had lost its front axle and its cab – and had flipped upside-down. The bollards, meanwhile, were completely unscathed.

Mark set up Securiscape 18 years ago and the Glide Bollards are the latest product to have hit the market, with more new ones now in the pipeline.

Its innovation is what has made Securiscape its name in the industry, with the Glide Bollards acting as a perfect example of what it can do to serve customers looking to protect their premises without turning their close environment into a fortress or stopping people from going about their business.

There are currently three versions of the Glide Bollard on the market, the Glide Bollard 30, the Glide Bollard 40 and the Glide Bollard Nano. All of them comprise of a series of steel bollards fitted onto a rail that is embedded

Securiscape has installed its products in some of the best addresses in the country

▶

SECURISCAPE IS THE ONLY FIRM TO SELL AN IWA-14 RATED SAFETY FENCE

Glide Bollards can be installed in sites where deeper footings are not always possible

Picture credit: Securiscape

into the surface of a road or pathway. Depending on need, the bollards can either be immobile or they can be slid aside manually to allow a vehicle to gain access and pushed back into place to form an impregnable barrier.

What makes the systems different is the depth to which they are embedded into the road surface and the level of protection they can offer. The Glide Bollard 30 and 40 can stop a truck travelling at 30mph and 40 respectively, while their installation depth is 210mm for the Glide Bollard 30 and 240mm for the Glide Bollard 40. The Glide Bollard Nano can stop a vehicle such as a Ford Mondeo travelling at 40mph and where it scores highly is the shallowness of the trench needed to install it.

Incredibly, bearing in mind the forces that it is capable of withstanding, this measures just 130mm – the length of a standard pencil.

It took many months and a significant investment for Securiscape to achieve this and the result is a system that is capable of being retrofitted in sites where there is a danger of disturbing underground services by excavating too deep. It also causes minimum fuss, takes less time and is more cost-efficient – three considerations that underpin everything that Securiscape does.

The company was born out of Mark's previous company, which designed and rented out award-winning floral street planters. In 2016, in the wake of the vehicle-borne terrorist attack on Glasgow International Airport, it received a request to design a planter which could double as a defensive installation to stop further attacks on other sensitive buildings.

It produced its first prototype within a couple of years and, after selling his previous firm in 2016, Mark has concentrated on Securiscape full time and now works alongside his daughter, Chloe.

Street planters are still a major part of what the company does – it has installed them outside railways stations, banks and council offices – but it also supplies temporary street barriers for outdoor events, its bollards and a range of pedestrian guardrails which are capable of protecting people from vehicles being driven onto the pavement and used as weapons.

In all of these cases, just like the original street planters, the products have been developed to order, often in the wake of a spate of terrorist incidents where lives have been lost.

The temporary street barriers – called SecuriPods – were developed following the attacks on the Berlin

Christmas Market in 2016, while the guardrails – which can also be installed on bridges – were produced following the attack on pedestrians on Westminster Bridge the following year.

Like the Glide Bollards, they are available in different versions and are IWA-14 rated, while they are also capable of being installed in sites which are unsuitable for products which require deeper footings or cannot be used on a slope.

"The Glide Bollards were also created in response to a customer inquiry," Mark explains. "He got in touch to ask us if we sold a barrier system that could control vehicle movements but which didn't impede the progress of pedestrians.

"The same is true of the guardrails, which came out of a request from a faith school which wanted to protect its students as they queued up on the pavement to enter the school gate each day. That's not an easy undertaking because the space we had to work with was limited and there was also the issue of planning permission and so on, but it's just the sort of challenge we love to take on."

Securiscape holds eight separate patents and its product development is definitely the side of the job that Mark likes the most. In particular he is proud of the way in which he is able to solve customers' problems and also create products that, in some cases, have never been seen before.

This includes the manual glide bollards but also Securiscape's pedestrian guardrails, which were his answer to the inquiry from the faith school and are now in position. Understandably, they are different to normal roadside pedestrian guardrails, which are not designed to withstand a collision. Securiscape's are and they can achieve a whole lot more, thanks to ground-breaking innovation that has revolutionised HVM technology.

Called the HVM Socketed Guardrail system, the product achieved its all-important IWA-14 rating after being subjected to a Highways England crash test involving a 2.5 tonne pick-up driven at 30mph at the vehicle testing facility MIRA in Leicestershire.

The successful test – it was yet another that Mark couldn't bear to watch – represented a huge step forward for Securiscape, which is the only firm to sell an IWA-14-rated safety fence, thanks to its unique ground-mounted socket system and SmartPost technology.

This makes it easy to install and, more importantly, super-shallow – the excavation depth of the guardrail is just 400mm, thanks to a design innovation which ensures that the force from any impact is dissipated along the length of the railings rather than the posts having to bear the brunt. This means the fencing can be installed with a minimum of fuss and relatively cheaply – and makes it ideal for protecting pedestrians using the pavements on busy road bridges.

Not only has its R&D underpinned its success over the past 18 years, it has earned Securiscape the opportunity to install its products in some of the best addresses in the country, including One Hyde Park, the luxury apartment block, which is famous for being the most expensive residential development in London.

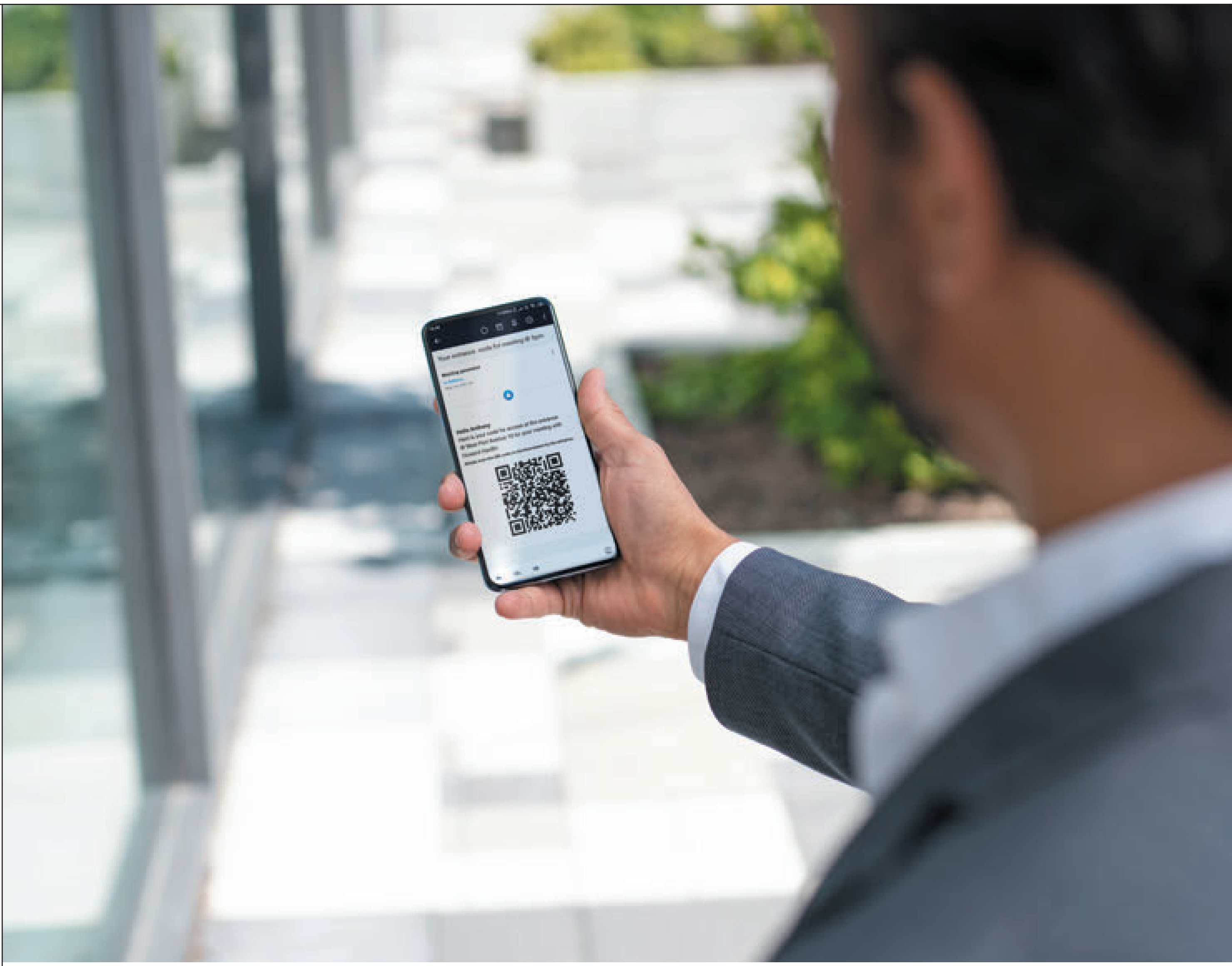
Its planters are also stationed outside UBS Bank in the City of London, it has recently completed an installation for Leicester Tigers Rugby Club and the mixed development close to Wembley Stadium also doubles as a showroom for Securiscape's products, with 54 Glide Bollards, dozens of planters and many metres' worth of Guardrail playing their part in keeping everybody safe.

"It's amazing when we think about where we install our products, but the best bit about the job for me is working with our designers on new ideas, learning new ways to solve people's problems and making what sounds impossible possible," Mark reveals.

"Nobody wants our streets to be turned into a fortress, which is why we make products that don't look out of place, and everything we do has to be practical and cost-effective. That's one of the biggest challenges to the sector. Like in other industries, costs are rising and people have budgets to protect, so much of what we do looks at how easy the products are to install and transport because we can save customers' money that way.

"That takes up a huge amount of my thinking time and our product development, but with Protect Duty on the way, many more organisations are going to have to look at installing perimeter security products and we in the industry have a duty to ensure that they are as affordable and effective as possible."

To find out more about Securiscape and its products visit **www.securiscape.co.uk** ●



CRACKING THE CODE

Derek Wang *explains why QR codes hold the key to access control*

Physical access control systems (PACS) are crucial for any organisation that wishes to secure access to its premises. While some small organisations may still opt for a traditional lock and key approach, the vast majority have decided to steer more towards keyless, contactless door entry for additional security and ease of use. This, of course, requires some level of identification measures in place to control and monitor access to company buildings, such as a plastic identification card or key fob.

Relying on these more traditional authentication options, however, doesn't come without its challenges. Whether that's the risk of losing an identification card or struggles with storing data, organisations are increasingly looking to digital solutions for access control. This is where the QR ('Quick Response') code comes in.

A QR code is a type of two-dimensional barcode that stores data that can be read and processed by the camera in a smartphone or a dedicated reader. QR codes are by no means new, having first appeared in the mid-Nineties. Despite this, it is only in recent

From a security standpoint, dynamic QR codes can more accurately monitor and track building access

years that they have become notably prominent, largely due to the rise in smartphone use.

More recently, their integral role in the global pandemic has brought the QR code offering much more to the fore, as organisations across all industries have been in search of low-touch solutions through contactless technology.

For organisations that wish to up-level their access control measures, they ought to consider the QR code as a more efficient way to control access to their businesses and premises than traditional counterparts.

When looking at existing access control systems, traditional plastic access cards or key fob-based access solutions remain the most common methods for controlling access to an organisation's premises. These traditional credentials, albeit simple, aren't necessarily the most effective form of access control today.

Plastic identification cards are powered by radio frequency signals emitted from the card reader, which has a limited range and relies on close proximity to function successfully, and key fob-controlled access operates in a similar way, utilising short-range electric signals to unlock a door in close proximity to the key fob.

KEEP IT SIMPLE

Compared with traditional access solutions, managing a QR code as a credential in an access control system is fairly straightforward. A unique, one-time entry QR code can be generated in a matter of seconds for any visitor, which can be sent directly to them via email or mobile app. At the entrance to a building or room, the visitor can display the code on their mobile device to be scanned by a QR code reader. The data within the code is shared with the access control system to confirm access rights in real-time, and the door is then unlocked automatically. Intercoms at the door can also double up to serve as a QR code reader, which further simplifies the access control process.

QR-controlled access is particularly useful for organisations looking to manage different visitor groups and zones with various access requirements, such as a university or a block of offices. QR codes can easily be set up with additional controls, such as allowing site access for a limited time period and number of uses, or restricting entry to specific doors or areas of a building, depending on who the visitor is and why they need to be granted access. This allows for more flexibility when it comes to visitor management than traditional credentials.

Though traditional access control methods provide some level of security, one of the main challenges that comes with using physical credentials is that it's difficult to control and monitor who is accessing premises, as cards or key fobs can often be misplaced, stolen or shared between visitors.

Integrating a dynamic QR code into access control solutions provides an extra layer of security for organisations. While a traditional QR code is static and cannot be changed or updated once created and distributed, a dynamic QR code can be updated and changed even after its creation and distribution. This is an important development as a static code is easy to copy, making it less ideal for high-security demands. Dynamic QR codes provide options to be changed and updated, even after distribution, while at the same time keeping all the aforementioned benefits of a QR code-based access control solution.

From a security standpoint, dynamic QR codes can more accurately monitor and track building access, providing a better overview of who is visiting an organisation's premises and when. This uplevels security measures for an organisation, as it not only enables security operators to keep track of who has entered a building and at what time, but it minimises the risk of credentials being obtained and used by another individual.

Dynamic QR code-based solutions also remove the risk of credential copy that some more traditional methods may be more susceptible to, since a screen copy, photocopy or video recording of the dynamic QR code will not be registered by the reader. Organisations can further enhance the security of the QR code-based solution by combining a dynamic QR code with a multi-factor authentication solution, such as a PIN entered at the same time as the code is scanned.

A QR CODE CAN BE GENERATED, DISTRIBUTED, UPDATED AND REVOKED RELATIVELY EASILY

This is not to lessen the role of network video cameras and audio in building security and access control. Combining QR codes with video and audio analytics is an effective strategy for organisations to further enhance their security measures. For example, in cases where physical identification may be needed, the network surveillance cameras on-site can enable security teams to monitor footage as an additional source of information and compare this with QR code access data.

A further use case in combining audio and video with QR-powered access is in a vehicle access system. License plate recognition can be used in combination with QR codes to control visitor access. When booking a hotel room, for instance, a guest can provide their car license plate number and receive a QR code which will securely grant access to the hotel parking garage. With the right systems in place, guests can then gain access when a camera picks up their license plate.

Adding network speakers can be useful to inform the driver that the access is denied, or that a QR code has expired. An alert can be triggered if necessary, allowing security personnel to intervene directly. If surveillance cameras are integrated into the system, a denied access or an alarm caused by a door that was forced open can also trigger the recording of the area, capturing relevant video evidence.

There are a number of additional benefits to using QR codes for access control outside of security measures, and one of the most notable is improving overall organisational efficiency.

The digital nature of a QR code means it is a cost-effective solution, particularly when comparing them with physical cards or key fobs. A QR code minimises the costs of purchasing, handling, printing, distributing and disposing of physical credentials.

▶

Not only this, but digital credentials save the cost of installation since organisations can utilise existing video intercoms or cameras as the QR code reader. By installing a QR code scanning application, which requires few components, organisations can reduce overall costs. This form of access control is easy to manage and maintain, and so has long-term cost benefits for organisations.

Carbon efficiency is also important for organisations to consider. Removing any requirement of plastic cards or key fobs, or even printed paper, also has a positive impact on the environment and plays a part in reducing company carbon emissions.

A QR CODE STORES DATA THAT CAN BE PROCESSED BY A SMARTPHONE CAMERA OR READER

An additional benefit of using a QR code as the credential is it can be helpful for improving the efficiency of managing access control systems. A QR code can be generated, distributed, updated and revoked, providing a highly efficient system management solution. It is also very convenient to use, suiting the priorities of the mobile-first workforce.

Typically, an external visitor can use a QR code to access a facility or parking area without having to stop at the front desk. This reduces dependency on building staff to check visitors in and so enables faster entry as well as a more reliable way to track those that enter.

Another typical use case involves the management of late deliveries when there is no staff present. When a supplier already has a QR code on their mobile device, they can simply display it in front of a code reader to gain access to specific areas at a facility. The use of dynamic codes is ideal in these situations, where security is ensured through the use of multi-factor authentication and ensuring against static codes being copied and used by others beyond those intended.

Advanced access control using dynamic QR codes and integrated QR code readers is providing organisations with the long-term solutions they need to address the challenges of managing access to facilities. Dynamic QR code-based access control is capable of addressing some of the core limitations and downfalls of traditional solutions such as physical cards and key fobs, and also brings a number of benefits – from enhanced security to organisational efficiency.

By implementing dynamic QR codes into an existing access control system, and combining this with building intercoms, network cameras and audio, organisations can look to a more efficient, frictionless and secure future for optimal access control. ●

Derek Wang is Global Product Manager at Axis

A unique, one-time entry QR code can be easily generated in a matter of seconds for any visitor

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!

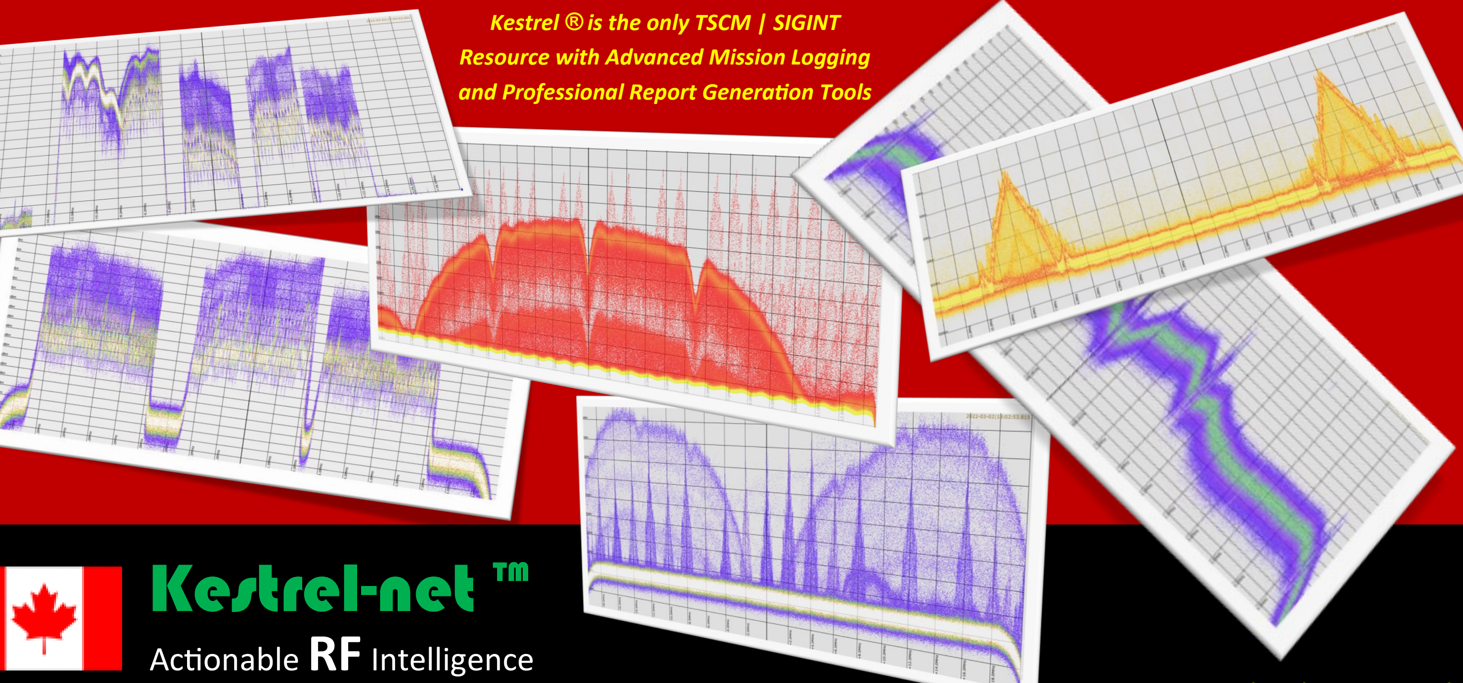
This is Not Just Another TSCM Spectrum Analyzer! | Now You Can Have Tomorrows TSCM | SIGINT Software — Today!

Kestrel TSCM ® Professional Software

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

Radio-Frequency, Power Line, and Optical Threat Technology Detection within a Standards-Based Software Defined Radio (SDR) Environment

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



Kestrel ® is the only TSCM | SIGINT Resource with Advanced Mission Logging and Professional Report Generation Tools

Kestrel-net ™

Actionable **RF** Intelligence

How Does Your Analytical Spectrum Stack-

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

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

It’s An Open & Shut Case.

Introducing the new TTK Tactical TSCM Kit

If your security issue is in the UK or abroad, the new TTK Tactical TSCM Kit is the most comprehensive mobile kit we have ever sold, it has the power to tackle hidden state of the art bugging devices with the mobility to go anywhere to find them - single handed. The durable hard shell carry-on case houses a Spectrum Analyzer, Broadband Detector, NLJD, Audio Amplifier, *Thermal Industrial Multimeter - all with accessories and it’s only available in the UK from I.P.S.

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

*Kit contents vary

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

IPS

THE HALLMARK OF SECURITY

Looking For The Most Extensive Mobile Sweep Kit Available?

Picture credit: Crowdguard

SAFETY FIRST

Keeping sites safer from hostile or errant vehicles. **Iain Moran** *discusses the importance of risk assessment and specification in protecting people and assets from hostile and errant vehicles.*

While weaponisation of vehicles is relatively rare, hostile vehicles can pose a significant threat to both people and assets. And terrorism is not the only risk. Thieves and protestors can also use vehicles to damage properties. Then there is the issue of drink and drug driving and, of course, simple human error.

The risks may be rare, but they are real. There needs to be a considered understanding of the nature of that risk and how it can be mitigated in a way that is both effective and proportionate.

Terror attacks at events and within busy urban centres are well-documented. Along with the organised gatherings targeted at the Berlin Christmas Market and Bastille Day celebrations in Nice, the London Bridge attack highlights the potential risk of terror attacks happening at any time and in any public realm environment.

Meanwhile, according to data collected in the US over the past decade by the Storefront Safety Council, there have been more than 24,000 storefront crash incidents in the past 10 years in the USA. This data has been scaled up by Lloyds of London, and the

There have been more than 24,000 storefront crash incidents in the past 10 years in the USA

scaled data indicates that storefront crashes occur globally as many as 100 times per day, with 46 percent of all incidents resulting in an injury, and 8 percent resulting in a fatality.

These storefront crashes include both accidental and malicious events. While a recent spate of coffee shop storefront crashes can be attributed to reckless driving, these incidents demonstrate the potential of such events to damage a brand, highlighting how intentional attacks could be used specifically as a tactic to cause reputational damage. For luxury brands, there is also a threat from ramraid attacks, where vehicles are used as a means of gaining entry to take high-value stock from the store; a practice that can cause significant damage to both the property and the brand.

In all of these scenarios, the consequences include safety risks to staff and customers – as evidenced by a recent incident when a driver mounted the pavement and hit a busy restaurant bar in Virginia, injuring 14 people, several of them seriously. But the commercial risk goes much further and includes the cost of repairs, the financial impact of business interruption and the effects on both insurance premiums and the ability to secure insurance cover.

Following an incident or in anticipation of potential increased risk, it's not uncommon to see a knee-jerk response, in the name of due diligence. But, although putting measures in place to reassure stakeholders and deter attacks is a positive step forward, only a detailed consideration of risk, coupled with a holistic approach to tailoring the right solution will really provide peace of mind that people and assets are protected.

Certified and tested hostile vehicle mitigation (HVM) systems, which have been correctly specified and installed, are a practical solution to mitigating risk. However, it is just as important to ensure that the systems chosen are suitable and proportionate for the specific level of risk for the individual environment as it is to mitigate risk. Over-specification not only inflates the cost of protecting the environment but can also over complicate or delay the installation, and can result in the measures becoming intrusive.

The anticipated UK Protect Duty legislation looks likely to recommend a threats, vulnerabilities and risk assessment (TVRA) approach to identifying risk. We recommend that this assessment be carried out by experts that can offer a turnkey approach to risk assessment, specification, supply, installation, deployment and servicing of HVM equipment. It's important that someone underwrites the risk and in this way event management companies, venues, local authorities and commercial business can outsource all due diligence to a single trusted and quality assured partner.

At Crowdguard, we have developed a rigorous TVRA process so that we are able to offer our clients this joined up approach and considered consultancy that takes account of commercial, operational and aesthetic factors, alongside safety and asset protection. This TVRA process involves an analysis of the threats for a particular location, building or brand; threats that may change. TVRA should not be seen as a one-off-exercise, therefore, but as a process that needs to be refreshed. Threats may include a change in the terror alert level, a revised road layout or threatened direct action from groups.

Threats should be considered in the context of the vulnerabilities inherent in a site's location, building, or brand. For example, potential vehicle access routes, existing security arrangements or controllability of all entrances and exits.

At Crowdguard, we include vehicle dynamics analysis in the TVRA process in order to enable the potential size and speed of hostile or errant vehicles to be considered, alongside threats and vulnerabilities, in order to assess risk. Only then can an optimised solution be designed to mitigate as much of that risk as possible.

It is an evidence-based approach to understanding risk and developing a solution that can be proven to mitigate specific threats, vulnerability and risk. The starting point for any HVM strategy should be knowledge and, armed with that knowledge, event managers, venue operators, local authorities and property owners can make informed decisions about the level of risk they are willing to accept.

THE GOAL IS TO HELP PEOPLE BE SAFER AND FEEL SAFER; NOT TO MAKE THEM FEEL UNDER THREAT

In some scenarios, it may be that the client is willing to accept a higher level of risk in order to balance risk mitigation with commercial and/or operational factors. However, where this is the case, the improved understanding of risk forms part of the defence against potential threats because the potential vulnerabilities to malicious or accidental safety or security issues can be built into safety and security practices.

At Crowdguard, our approach is to give the client our best advice for specification of a best-fit, proportionate solution, while providing potential alternatives with a summary of how the client's choices will affect their risk mitigation. We can do this thanks to our partnerships with a variety of HVM and perimeter protection product suppliers, enabling us to offer both temporary and semi-permanent solutions for a broad range of different applications.

Indeed, education and expertise are vital to both the client's decision-making and the level of protection offered by the final solution. A common mistake is for event organisers, venue operators and local authorities to assume that any IWA-14-1 HVM system will be suitable for their security requirements because it is certified. This is not the case. There is no such thing as a one-size-fits-all solution. The most appropriate solution needs to take account of factors such as the speed and force of a potential attack or accident, the ground conditions and the layout of the protected area.

The level of protection delivered by the HVM solution is also dependent on quality assurance processes and how closely the finished installation mirrors the 'as tested' performance of the HVM product. For example, Crowdguard's portfolio includes the RB50 system from Highway Care, which is installed in 4m arrays. This system was crash tested as a 4m array so it is almost always deployed in an 'as tested' configuration. For other systems, it is the expertise of the specification team that calculates any disparity between 'as tested' and 'as installed' performance, so that this can be factored into risk mitigation effectiveness. The difference between 'as tested' and 'as installed' should always be communicated in writing to the client so that they are fully aware of their level of risk.

Quality assurance processes are integral to effective risk mitigation because any non-compliance during installation and deployment can reduce the system's performance. The Hostile Vehicle Mitigation Installers Scheme (HVMIS) has been designed to ensure appropriate specification and correct installation of suitable HVM systems and requires installation of the HVM by a registered company. At Crowdguard, we have developed our own strict quality assurance processes. All operatives are manufacturer-trained and install the system as close to 'as tested' as possible, with a full understanding of impact test results. We ensure that they understand the foundation/ground conditions of the impact test and carry out all maintenance requirements. Following decommissioning and removal, all equipment is checked and maintained so that it is in peak condition for the next installation.

CERTIFIED AND TESTED HVM SYSTEMS ARE A PRACTICAL SOLUTION TO MITIGATING RISK

Alongside the safety and security considerations for best practice specification and installation, there are practicality and aesthetics considerations, because the right solution needs to enable the venue, property or location, and the occupier, visitors or members of the public to continue functioning as normal. Consequently, there needs to be a discussion about whether the HVM protection needs to be temporary – perhaps to address a specific risk – semi-permanent to provide flexibility, or permanent. Aligned to this is a consideration of whether the solution needs to be reconfigurable – are there varying levels and types of risk at different times of day, or times of year, for example?

Access is also important. The purpose of an HVM system is to protect people and assets from vehicles, but how will it affect pedestrian access and is a pedestrian permeable solution required for some or all of the installation?

The importance of aesthetics should not be underestimated either. The goal is to help people be safer and feel safer; not to make them feel under threat. It is possible to select HVM systems that can be customised, not only to look less invasive but also for branding, wayfinding, advertising or information. This should be considered both in the context of how welcoming the environment looks and any commercial value that can be leveraged by the need for safety protection. Indeed, advertising on HVM systems can become a revenue generator. Meanwhile, solutions such as the Unafor Core, which has recently been added to the Crowdguard portfolio, can be used to enhance the aesthetics of a location. This is particularly useful for streetscapes and public realm locations, where variants of the system with planters or street furniture enhance the environment, while making it safer.

With a TVRA approach, a safety specialist can recommend the most appropriate solution to mitigate risk for the site in question, but may also provide an alternative solution that takes into account any practical issues or stakeholder concerns. When choosing between the options, it is important to understand the risk gap and make an informed, pragmatic choice, which is why it's vital to work with a specialist ●

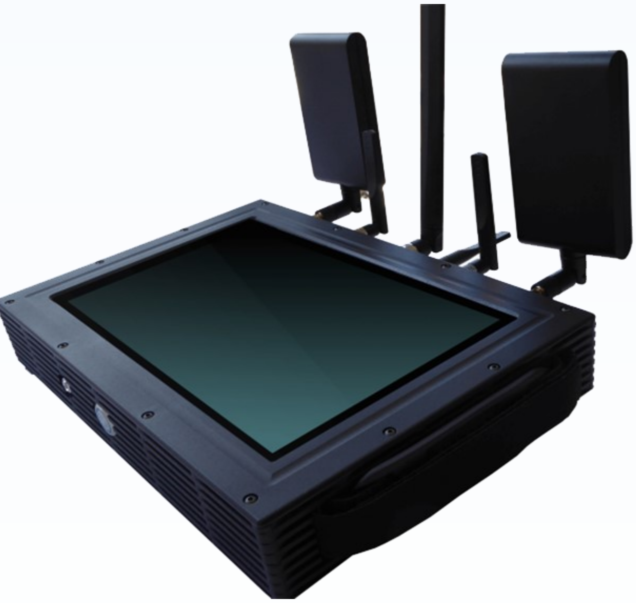
Iain Moran is Managing Director of Crowdguard, the specialist in safety and security solutions for the public realm, events and buildings.

The most appropriate solution needs to take account of factors such as the speed and force of a attack, ground conditions and layout of the protected area

Picture credit: Crowdguard

Sentinel

A TSCM BREAKTHROUGH



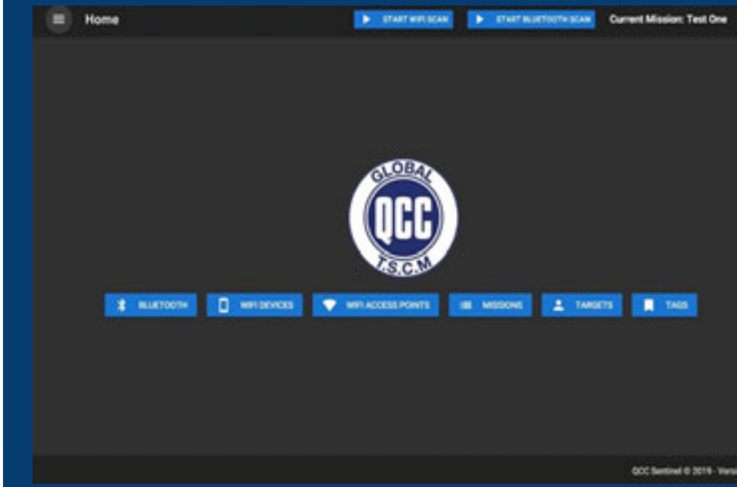
QCC Sentinel is the most advanced TSCM portable system for the detection & location of Wi-Fi 2.4GHz - 5GHz Devices & APs. Also with detection & location of all Bluetooth devices with full direction-finding. Software for TSCM & Tactical use.

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

Designed for TSCM Engineers by TSCM Engineers.

FEATURES

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



Current Mission: Test One

SENTINEL KIT INCLUDES

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

For further details: contact@qccglobal.com

LONDON

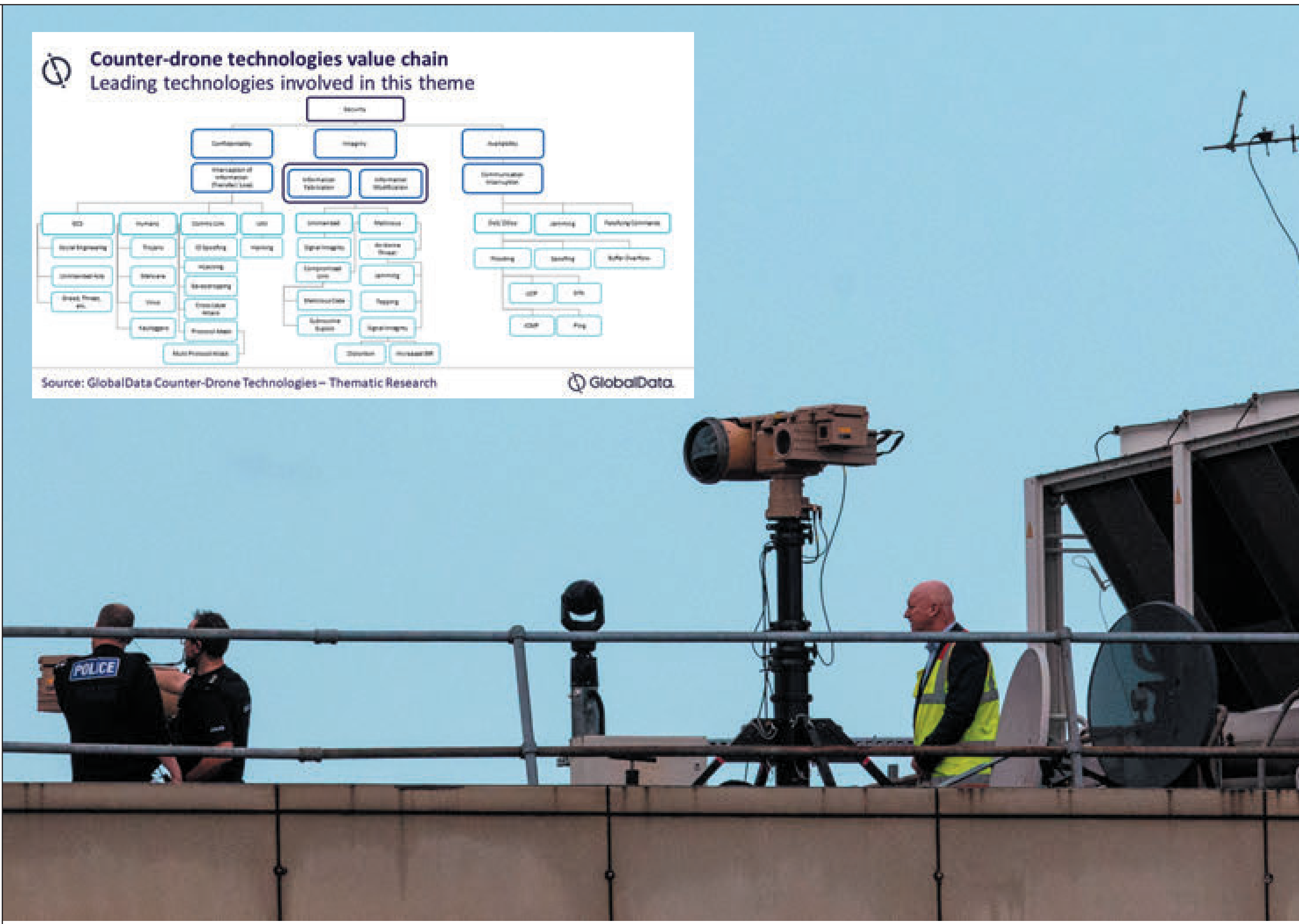
T: +44 207 205 2100
E: contact@qccglobal.com

SINGAPORE

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

ISO 9001 CERTIFIED
ISO 27001 CERTIFIED
ISO 45001 CERTIFIED
ISO 14001 CERTIFIED

"Keeping your business, *Your* business"



Counter-drone technologies value chain

Leading technologies involved in this theme

Source: GlobalData Counter-Drone Technologies – Thematic Research

Picture credit: Getty

SERVE AND PROTECT

Pinky Hiranandani *explains why drone security remains a critical factor as the market takes-off*

The widespread use of drones, particularly for commercial and military use cases, has increased the associated security risk. Drones interact with their base using unencrypted communication channels, exposing the sensitive information they collect. As more drones enter both public and private airspace, drone security will become paramount for national and local governments, law enforcement agencies, critical infrastructure and public venues. To counter this emerging threat, investments in Counter-Unmanned Aerial Systems (C-UAS) capabilities are essential.

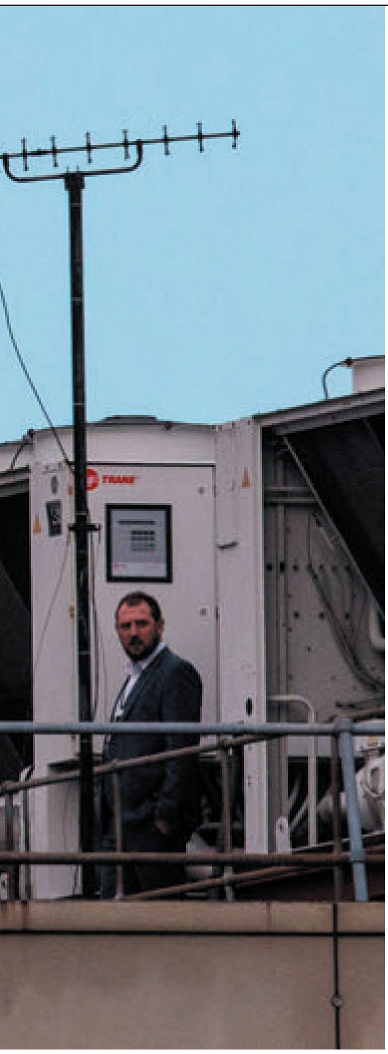
Malicious drone interference has compelled commercial end-users, including industrial conglomerates, universities, utilities and sports organisations to explore drone mitigation solutions. Against this backdrop, the focus of drone manufacturers has shifted to counter UAS systems.

Biological countermeasures, such as using eagles to detect and neutralise rogue drones in restricted airspaces, are also being explored. Commercial flights are already being disrupted by drones. For instance, in December 2018, Gatwick Airport was closed for 33-hours due to a perceived threat from drones. To help resume operations, Leonardo's Falcon Shield counter-drone system was used to detect, track and mitigate rogue drone threats.

Physical security includes the use of hardware for detecting, tracking and interdicting UAS threats, while software security refers to cyber protection against hackers. The counter measures deployed in the defence industry are more likely, but are not exclusively to be used for neutralising larger UAS platforms (High-Altitude Long Endurance (HALE) and medium-altitude long-endurance (MALE) drones). In the civil market, these measures are deployed to neutralise small unmanned aerial systems (sUAS).

Counter UAS physical systems fall under three broad categories: ground-based, hand-held and aerial based. Ground-based counter UAS systems are used to detect and track incoming drone threats, and include devices such as radar, radio frequency sensors, electro-optical (EO)/infrared (IR) sensors, combined sensors and acoustic. Hand-held devices used for interdicting drone threats include unconventional and conventional projectiles. The aerial-based counter UAS systems include jamming, directed energy, and cyber tools.

Of the various ground-based systems, radar is one of the most used C-UAS capabilities. Numerous radars, such as low-frequency pulse radar, have been designed to detect large metal objects like planes and helicopters, but are less suited for detecting small radar cross-sections and carbon body objects that fly lower to the ground, as such as UAVs in Group 1 (Max gross takeoff weight of <20lbs. and operating altitude of <1200 above ground level (AGL)) and Group 2 (21–55lbs. and <3500 AGL).



Radar is one of the most used ground-based C-UAS capabilities

One method that developers can use to increase the accuracy of their C-UAS systems, and reduce the frequency of false positives is to incorporate multiple detection and interdiction techniques into their systems. By corroborating different forms of data from multiple sensors, the system can accurately triangulate legitimate UAS threats and filter out false positives that otherwise would have been flagged.

Conventional projectiles are hand-held devices which include air-to-air munitions, surface-to-air missiles, and small arms munitions. Of these, surface-to-air missiles are perhaps the most traditional means of UAV interdiction, and for specific segments of the UAV population (Groups 3-5) they are the most effective. Cheaper interdiction methods such as small arms munitions, unconventional projectiles and DEW are a more appropriate choice for small drone interdiction.

Common unconventional projectiles include collision drones and nets. Other promising projectiles include water cannons, which the US Defense Systems Information Analysis Center regards as a low-cost defence option especially for aboard naval vessels. A water cannon was used at the 2016 US Air Force Research Laboratory's Commander's Challenge to successfully bring down a drone during a C-UAS exercise.

Under aerial-based systems, directed energy is used, which includes dazzling, lasers and high-power microwaves. Of these, lasers are a low-cost-per-shot option, requiring only electrical energy rather than chemically propelled munitions – making them an attractive choice for C-UASs.

Under jamming, RF and GNSS jamming systems are used as counter measures. RF jamming as an interdiction is being extensively used in many C-UAS products and will face more advanced threats from evolving UAS technologies. There are now commercially available UAS that utilise mobile LTE networks rather than conventional RF links.

Going forward, with the likely widespread deployment of drone swarms, jamming (RF and GNSS) and spoofing – where false GPS signals are broadcasted to UAS receiver – provide a cost-effective means of disrupting a swarm or a single UAS by preventing coordination among individual elements, collapsing the swarm so that it disintegrates into many disparate, uncoordinated elements and by preventing communication between the UAS and the operator.

The value chain graphic opposite highlights the technologies used for cyber counter drone security. Cyber-attack against UAS platforms include violations such as **data confidentiality** – where information is intercepted between the Ground Control Stations (GCS) and the platform; **data integrity** – where information is falsified in transfer between the GCS and the platform; and **data availability** – where communication between the GCS is disrupted**.**

DRONE SECURITY WILL BECOME PARAMOUNT AS MORE DRONES START TO ENTER INTO AIRSPACE

Spoofing devices deceive a GPS signal by broadcasting false GPS signals to the UAS's receiver. Spoofing is considered a step ahead of jamming since the latter can disrupt a receiver but not deflect or redirect it. Additionally, regarding collateral damage, spoofing holds an advantage over jamming. The use of spoofing is more common in communications and mechanisms which do not have a high degree of security. Companies like Dedrone, Sharper Shape, DroneShield, Drone Defense and SkySafe offer software-based protection against hackers.

The US recognises that UAS could provide its adversaries with a low-cost means of attacking or conducting ISR missions against US forces and that smaller UAS cannot be detected by traditional air defence systems due to their size, construction material and flight altitude. In light of this, in FY2023 the US Department of Defense (DOD) plans to spend at least $668 million on C-UAS research and development and at least $78 million on C-UAS procurement.

To counter UAV threats, branches of the US military have undertaken several development projects. The Air Force is testing high-powered microwaves and lasers for C-UAS missions. For example, in October 2019, the Air Force received delivery of a vehicle-mounted C-UAS prototype, the high-energy laser weapon system (HELWS), that will undergo a year-long overseas field test. The Navy is also investing in the development of DEWs, with ODIN being installed on USS Dewey in 2020 and on USS Preble in 2021.

China is the second-largest C-UAS producer in terms of the number of product designs. One of the primary factors driving Chinese investment in C-UAS technology is awareness of US investment in drone technology. State-owned China Aerospace Science and Industry Corporation (CASIC) has reportedly developed a C-UAS system consisting of multiple weapons, including land-based rockets and UAS-hunting UAS that can shoot net-based projectiles, along with capabilities in development regarding vehicle-based adaptions and small-UAS detection devices.

China has also reportedly developed rifle-shaped interdiction devices, which send out jamming signals that disrupt UAV functions, resulting in either a forced

▶

landing or diversion of the intruding UAV. At Airshow China 2018, CASIC also showcased a vehicle-based laser weapon called LW-30, which can use a directional emission high-energy laser to quickly intercept aerial targets, such as photoelectric guidance equipment, UAVs, guided bombs and mortars.

DATA FROM MULTIPLE SENSORS ALLOWS THE SYSTEM TO TRIANGULATE LEGITIMATE UAS THREATS

China is also using artificial intelligence in C-UAS products, with reports surfacing that the country is already in the process of evaluating prototypes for a C-UAS platform that leverages AI to detect and destroy intruding UAVs. In China, jamming systems appear to be the most popular way to detect and counter UAVs.

Israel has continuously worked in association with the US to make progress in the C-UAS sector. The growing accessibility and affordability of sUAS systems for personal use translates into a growing threat of terrorist organisations deploying improvised drones in attacks. Additionally, adversary states in the region, including Iran, are actively expanding their drone fleets. These incentives will drive Israeli investment in C-UAS going forward to ensure that it is capable of countering drone threats of every scale. Israel unveiled an Advance UHF AESA radar system, which is designed to search, detect and track low observable aircraft, UAVs and missiles.

C-UAS systems may not always be legal. There is significant confusion and ambiguity as to the exact legal dimensions of C-UAS technology use. This is because the technology is often subject to overlapping laws that were drafted to address other technologies, long before counter-drone technology existed.

In the US, in general, whether a detection or tracking system implicates federal criminal surveillance laws, such as the Pen/Trap Statute and the Wiretap Act, depends on whether it captures, records, decodes or intercepts, in whole or in part, electronic communications transmitted to and from a UAS and/or controller and the type of communications involved. The Pen/Trap Statute criminalises the 'use' or 'installation' of a 'device' or 'process' that 'records,' 'decodes,' or 'captures' non-content dialing, routing, addressing or signalling (DRAS) information.

In the FAA Reauthorisation Act of 2018, Congress codified the term 'unmanned aircraft' as an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft. Additionally, the use of spoofing interdiction may carry further penalties due to its interference with GPS signals.

There are currently limited international standards governing proper design and use of C-UASs. Given the nascent stage and rapid growth of the industry, there has been limited opportunity for international standards to emerge.

GlobalData's Counter-Drone Technologies September 2022 report authored by Harry Boneham, reveals that Raytheon Technologies, Northrop Grumman, Leidos, Leonardo and Lockheed Martin are some of the leaders in drone security space, while Droneshield, Kratos, Accipter, and STANLEY Security are some of the up-and-coming challengers. Leaders in this space are leveraging their existing experience and expertise to carve out a sizeable position in the C-UAS market. However, mirroring the proliferation and expansion of the UAS industry, several startups and smaller existing firms are starting to enter into the C-UAS market.

With the use of drones expected to increase in the coming years and with new technologies such as AI and drone swarms maturing, the counter drone technologies market is expected to proliferate ●

Pinky Hiranandani, Principal Analyst at GlobalData, has over 10 years of experience in telecom, media, and technology industry, with specific areas of expertise including drones, artificial intelligence, wearable tech, fintech, cloud computing, RPA and IoT.

Israel has worked in association with the US to make progress in the C-UAS sector

Picture credit: Israel Aerospace Industries

MGT europe

DroneTERMINATOR

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

THE APP SCANS VARIABLE HOLOGRAMS
WITH HOLOGRAPHIC VARIABLE ENCRYPTED INFORMATION

AUTHENTICITY GUARANTEED

Dr Paul Dunn, *reflects on how holograms provide a digital and optical vision for industries in transition*

Protecting and authenticating security and ID documents presents challenges for holograms but the technology's capacity to evolve and integrate in the optical and digital space reflects its continued potency in security applications. New optical and digital developments are reshaping the role and nature of holograms in document and ID security. They are also driving innovative and sophisticated design solutions for often non-descript security documents, simultaneously enhancing the security of an identity document, as governments and issuing agencies around the world, as well as other global entities, wrestle with losing billions of dollars a year in revenue through incessant counterfeiting of documents and insidious ID fraud.

Meanwhile the cost of paying for anti-counterfeiting measures to bring criminals to justice can add up to hundreds of millions of dollars. The problem has also been exacerbated in the last two years by the impact of Covid, which has accelerated digital transformation in almost every industry, accompanied by drastic opportunities for increased fraud.

The use of optical and physical technologies to protect valuable documents against existing and emerging threats is paramount

Providing innovative and sophisticated solutions for security documents requires not only a design that will make a document attractive; it also means enhancing the intrinsic security of that document. Secure document conception can be achieved for ID cards and passports, for example, by integrating security features with exclusive designs that highlight attack attempts and facilitate controls such as checking that an ID document matches the bearer.

Today, propelled by advances in materials and applications, holograms designed to protect and authenticate, are integral elements of optical variable elements (OVE) on ID documents, helping to verify identities both in person and remotely.

Ground breaking technologies such as Idemia's Lasink Helios are to the fore in these applications: its technology is linked to a DOVID (Diffractive Optical Variable Image Device) and combined with holographic technology displays striking optical effects, such as colour variations of the portrait including a full polychromatic view with true colours, which vary depending on the angle of view. Easy to inspect, resistant to multiple types of fraud and durable, the use validates both secondary and main portrait images on documents, thus confirming the identity of the document holder – both images are interlinked to make forgery virtually impossible, deterring any attempted fraud.

The IHMA estimates that there are as many as three billion identity documents issued worldwide, the evolving challenges posed by fraud see governments, issuing authorities and law enforcement turning to innovation to stay ahead of criminals and fraudsters. Here, the use of direct laser interference patterning (DLIP) applied by the Fraunhofer Institute for Material and Beam Technology in Germany can be seen as a versatile tool for producing holographic motifs and diffraction-based elements on most materials; the optical security elements can be written directly on the surface as well as in the volume of a transparent material for improved authentication and greater individualisation of security documents.

Conventionally, a DOVID protects the most important information of a document, ie the primary image of the document holder. It can additionally cover the holder's data and a secondary image. So conventionally all this information is printed or laser engraved by the manufacturer and protected by DOVIDs. However, rather than simply protecting the information, security solutions provider OVD Kinegram's novel technology allows for the creation of a secondary image and/or data directly. The laser personalized KINEGRAM is highly secure and protects against ID fraud and document falsification. This three-layer system is laser processed to radically alter their appearance from a black to mirror like effect, or transparent or even eye-catching optical effects.

Besides offering intrinsic protection, the use of two metal layers/effects provides further benefits and protection – both appearances are in perfect registration and thus cannot be copied by unauthorised printing processes. Moreover, the ability to integrate the embedded KINEGRAM elements over a larger area in perfect optical harmony with other features (such as the security print) leads to a document design that is intuitive and self-explanatory, and hence readily available for human inspection. The design tells a story that even the untrained eye can immediately understand, while the solution protects the personalised data and the photograph of the passport's data page for ID3 format passport data pages and ID1 format identity cards or driving licences.

SMARTPHONE TECH IS BEING USED WITH HOLOGRAM PROGRAMMES FOR AUTHENTICATION

Today, the use of optical and physical technologies to protect valuable documents against existing and emerging threats is paramount – for instance, the role of optical and digital technologies in securing health status passports is gaining increasing traction – while great strides are being made in the areas of micro and nano-optical structures and other new approaches to document security. Indeed, the future evolution of optical and digital document security is set to play an important role in the transition to digital documentation for some time to come.

New digital NanoCast technology from NanoGrafix enables the online production of variable holograms or any other optical structures on any printing press with the special NanoCast module. Each hologram can be different and have different holographic encrypted information that can be used for authentication and track and trace purposes. This can be installed on any existing machinery to 'print' these holograms or optical structures onto banknotes, security documents such as Tax Stamps, ID documents, etc. With this module security printers no longer need to outsource holograms or any other optical structure. The holograms are instantly produced and can be different from one another. Each banknote or secure document will then have for the first time a unique holographic identifier. No more outsourcing of security features or extra handling and storage of printed materials. In this way, the chances of documents being compromised are reduced while ensuring a readily available supply of 'instant' holograms to support global authentication and anti-counterfeiting programmes.

Smartphones are also increasingly being used in combination with hologram programmes to facilitate authentication. In this fast-evolving landscape, security features such as holographic foil-stripes that cannot be replicated are being created. This type of technology allows law enforcement and other specialists to 'read' a document using a smartphone or LED lighting, in

▶

the process providing a robust way to authenticate and thwart counterfeiting and forgery.

The continued use of holography in optical and digital document security points to the technology's underlying versatility, cost effectiveness and graphical flexibility. Indeed, it will continue to flourish in those markets where a highly effective security feature is required as governments and other issuers of ID cards, passports and driving licences have to implement security technologies to protect an increasing array of documents from counterfeiting attacks.

> **THE IHMA ESTIMATES THAT THERE ARE THREE BILLION IDENTITY DOCUMENTS ISSUED WORLDWIDE**

Equally, financial and secure documents are protected against counterfeiting with holograms incorporating complex origination and production processes unavailable to criminals. De La Rue's holograms feature hot stamping holographic foil technology that can be applied to a multitude of substrates and make it impossible to remove the device without damaging the foil and the substrate beneath. Smartphone technology is increasingly being used in combination with hologram programmes for authentication purposes, and we continue to see new developments such as Koenig & Bauer Banknote Solutions' ValiCash making inroads.

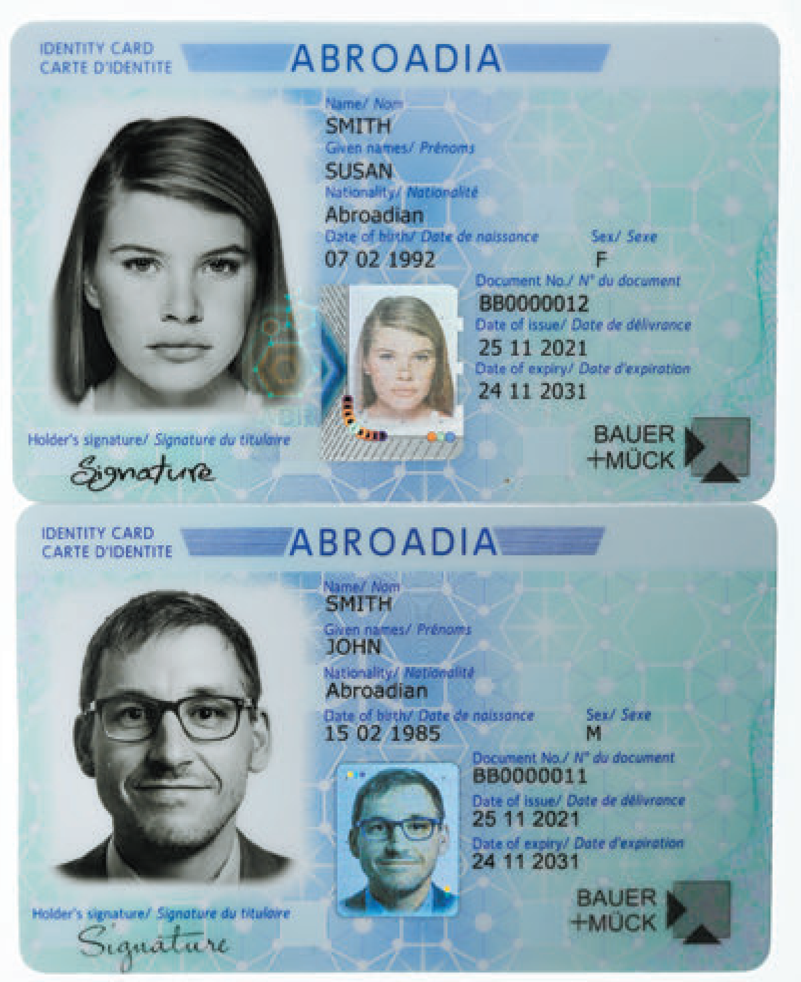
This is an app that not only identifies high-security documents, but also authenticates them, flagging either a 'pass' or 'fail response almost instantaneously. Since the system is based on the intrinsic intaglio print properties of the document, it does not rely on specific inks or hidden features. It can also be adopted and used for other applications including birth certificates and other high security printed documents, so long as they contain intaglio print.

STEP FORWARD

The optical and digital space heralds exciting development opportunities for holograms, which can deliver an exceptional representation of the 3D world and pose a significant step forward in the search for better imaging. The opportunity for further integration by innovative, forward-thinking companies is huge, as digital holographic technology, increasingly operating via smartphones and devices, provide a visceral and ardent interpretation of the world, allowing people to see and sense images in a way that is comfortable and natural.

Moreover, the use of well-designed and properly deployed authentication solutions, as advocated by the ISO 12931 standard, enables those with ID protection responsibilities to verify the authenticity of a legitimate product, differentiating it from counterfeits. Even those that carry a fake authentication feature can be distinguished from the genuine item if the latter carries a carefully thought-out authentication solution. The advantages holography offers will continue even as digital and mobile ID technologies gain increasing levels of traction ●

Dr Paul Dunn is chair of the International Hologram Manufacturers Association (IHMA). The IHMA is made up of more than 80 of the world's leading hologram companies. Members include the leading producers and converters of holograms for banknote security, ID cards and passports, other secure documents, brand protection, packaging, graphics and other commercial applications around the world, and actively cooperate to maintain the highest professional, security standards.



IDENTITY CARD
CARTE D'IDENTITE
ABROADIA

Name/ Nom
SMITH
Given names/ Prénoms
SUSAN
Nationality/ Nationalité
Abroadian
Date of birth/ Date de naissance
07 02 1992
Sex/ Sexe
F
Document No./ N° du document
BB0000012
Date of issue/ Date de délivrance
25 11 2021
Date of expiry/ Date d'expiration
24 11 2031
Holder's signature/ Signature du titulaire
Signature
BAUER +MÜCK

IDENTITY CARD
CARTE D'IDENTITE
ABROADIA

Name/ Nom
SMITH
Given names/ Prénoms
JOHN
Nationality/ Nationalité
Abroadian
Date of birth/ Date de naissance
15 02 1985
Sex/ Sexe
M
Document No./ N° du document
BB0000011
Date of issue/ Date de délivrance
25 11 2021
Date of expiry/ Date d'expiration
24 11 2031
Holder's signature/ Signature du titulaire
Signature
BAUER +MÜCK

The use of properly deployed authentication enables those with ID protection responsibilities to verify the authenticity of a legitimate product

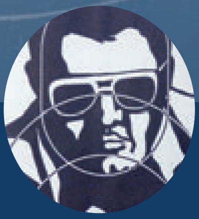
Variable holographic images with variable holographic encrypted information.

MCQUEEN TARGETS

LIVE FIREARMS TRAINING TARGETRY

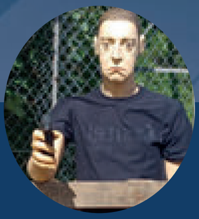
CIVILAIN TARGETS

MILITARY TARGETS



POLICE TARGETS

THREAT ASSESSMENT



3-D FOAM TARGETS

3-D FOAM ACCESSORIES

Hit the mark every time with

MCQUEEN TARGETS

GALASHIELS, SCOTLAND

targets.ukgal@sykes.com

+44 (0)1896 664269

mcqueentargets.com

INCIDENT BRIEF

Europe

16 September, London – UK
A police officer was stabbed repeatedly in the neck and another constable stabbed through the arm after a man with a knife was challenged in central London.

16 September, London – UK
A man was arrested by Metropolitan police in Westminster Hall, where the Queen was lying in state, after reports of someone running up the steps to the catafalque and touching the coffin.

19 September, Leicester – UK
Fifteen people were arrested after weeks of disturbances between Hindu and Muslim people since an Asia Cup cricket match between India and Pakistan on 28 August.

22 September, Reykjavík – Iceland
A foiled terrorist plot led to the arrest of four men as several semi-automatic weapons and thousands of rounds of ammunition were seized at nine locations.

25 September, Hounslow – UK
A man was arrested while attempting to flee the country after four men were hit by a car in west London, leaving two critically injured.

26 September, Kortrijk – Belgium
Police in the Netherlands arrested four suspects over what Belgium's justice minister described as a plan to kidnap him. Vincent Van Quickenborne, who is also the mayor of the city in western Flanders, blamed a drug mafia in a video message run by state broadcaster RTBF.

Americas

14 September, Washington –USA
Three Iranians were charged for trying to hack and extort hundreds of thousands of dollars from organisations in the United States, Europe, Iran and Israel.

15 September – USA
Uber was forced to take several of its internal communications and engineering systems offline after its computer network was breached. The hacker revealed themselves to be aged just 18.

16 September Montana – USA
American Airlines filed a data breach notification letter with the State Attorney General's Office, disclosing that Hackers gained access to sensitive personal information following a phishing campaign.

9 October, Long Island – USA
Two teenage boys were hit by gunfire from a moving car outside of the home of New York congressman and Republican candidate Lee Zeldin.

10 October, across the country – USA
Websites for more than a dozen US airports were temporarily brought offline by cyberattacks, with Russian-speaking hackers claiming responsibility for the disruption.

13 October, North Carolina – USA
Five people, including a police officer, were killed in a shooting in a residential area in Hedingham. The suspect was "contained" by police following an extensive manhunt.

Asia

13 September, Swat – Pakistan

Five people, including an influential anti-Pakistani Taliban tribal leader, were killed when they drove over an improvised explosive device in the north-western city.

16 September, Tabayin – Myanmar

Government helicopters struck a school in north-central Myanmar, killing at least 13 people, including seven children.

30 September, Kabul – Afghanistan

A suicide blast at an education institute in the Dashti Barchi neighbourhood killed 19 people and wounded 27. There was no claim of responsibility for the attack.

2 October, Malang regency – Indonesia

At least 125 people were killed and around 320 injured at a football match in one of the world's worst ever sports stadium disasters.

6 October, Nong Bua Lamphu province – Thailand

Thirty-seven people, most of them young children, were killed in a gun and knife attack by a former police officer at a preschool.

8 October, Shuafat – Israel

Armed individuals opened fire at a military checkpoint in east Jerusalem, killing an Israeli soldier and injuring two others.

8 October, Iran

The country's main news channel was briefly hacked and interrupted with images and messages in support of the continuing protests over the death of 22-year-old Kurdish woman Mahsa Amini.

12 October, Jerusalem – Israel

Israeli forces used live fire during confrontations with Palestinian protesters throwing stones and firebombs, sparked by the search for a suspected Palestinian gunman.

19 October, Yangon – Myanmar

Three prison staff and five visitors, including a 10-year-old girl, died after bombs hit a crowd queueing to drop off parcels for inmates at the country's main prison for political detainees.

Africa

9 September, Borno State – Nigeria

Over 200 terrorists were killed by Nigerian military in a joint land and air coordinated attack where three abducted Chibok girls were rescued.

12 September, Abyan province – Yemen

An explosion caused by an improvised device killed four Yemeni separatist fighters during an anti-jihadist sweep in the south of the country.

16 September, Borno State – Nigeria

29 Boko Haram insurgents were killed in an ISWAP ambush and the ensuing fighting that was said to "go on for hours".

21 September, Bam province – Burkina Faso

14 people were killed by armed insurgents while repairing a bridge between the villages of Bayen Foulgo and Komsilga.

24 September, Borno State –Nigeria

A major highway between Maiduguri and Damboa was closed as troops of the Nigerian Army were ambushed by Boko Haram militants.

24 September, Maiduguri – Nigeria

A soldier was killed when Boko Haram insurgents attacked a convoy of troops in an ambush on the Maiduguri-Damboa road. The troops engaged the insurgents in a shootout that lasted for hours.

1 October, Ouagadougou – Burkina Faso

Angry protesters attacked the French embassy in the capital after supporters of the new coup leader accused France of harbouring the ousted interim president.

8 October, Lake Chad – Nigeria

Eight Boko Haram insurgents were killed when fighters clashed with members of ISWAP.

18 October, Mzimba – Malawi

Authorities discovered a mass grave in the north of the country containing the remains of 25 people suspected to be migrants from Ethiopia.

NEWS

Europe

UK businesses still losing mission-critical company data

Provider of backup, recovery and storage solutions, Arcserve, has announced key findings from its annual independent global research study that highlight how the loss of critical data continues to disrupt businesses and remain an issue for organisations. In the research study of experiences and attitudes of UK IT decision makers, 83 percent of respondents reported a severe loss of critical data in their organisation. Of that number, 36 percent had permanent data loss. The research study also found that many UK organisations could not maintain business continuity on time once data was lost or compromised. As many as 91 percent of respondents said that 12 hours or less is an acceptable level of downtime for critical systems before there is a measurable negative business impact. Still, only 59 percent could recover from a severe data loss in 12 hours or less. Meanwhile 18 percent of the businesses surveyed couldn't recover data for one day or more. The results also suggest that a new approach to disaster recovery is needed, with organisations continuously updating, testing and documenting their disaster recovery plan to build data resilience. It concluded that protecting and recovering data should be elevated to all company levels with specific goals.

UK defence spending to double to £100-billion by 2030

Ben Wallace, the UK defence secretary, has claimed that military spending will double from its current level to hit £100-billion in 2030 as a result of Liz Truss' commitment to increase the armed forces' budget to 3 percent of GDP. In an interview with the *Sunday Telegraph*, the minister said the military is: "actually going to grow" for the first time since the end of the cold war – although he did not specifically commit to reversing a planned cut in the size of the army. Truss had promised during her leadership campaign to lift defence spending from 2.1 percent of GDP to 3 percent by 2030, well above a commitment made by Boris Johnson in June to increase it to 2.5 percent by the end of the decade. Wallace explained Truss' promise would be worth billions more to the military, claiming: "On current forecast, that's roughly a defence budget of £100-billion in 2029-30. We're currently on £48-billion. So that's the difference. In eight years, that's a huge amount." Despite the extra sums on offer, Wallace said he could not yet speculate on which parts of the military would benefit.

CPNI launches training course for security control room operators

The Centre for Protection of National Infrastructure (CPNI) has launched a new course for security control room operators. The course and associated guidance produced by CPNI enables businesses and organisations to plan, prepare and respond to terrorist incidents, increasing the capabilities of security control room operators and other security personnel. Uniquely based around research undertaken since 2017, the course offers world-first immersive exercises that simulate multiple terrorist incident scenarios, enabling delegates to practice decision making in real-time, as if they were in a real control room. The course is informed by the recently updated guidance, developed through detailed analysis of previous terrorist incidents – extensive research that has included live simulations of attacks and surveys of existing Command and Control capabilities.

Norway's police select Sepura TETRA radios

The Norwegian Police Service has signed an agreement with Northcom for the purchase of Sepura TETRA radios for use on the Nødnett emergency services network. The Police IT Unit has approved the deal that provides front line police users throughout the country with the choice of Sepura's SC20 and SC21 handheld radios for field officers, while fleet vehicles and control rooms will be equipped with Sepura's SCG22 mobile radio. The agreement also includes the purchase of audio and power accessories, service agreements, product training and support with programming and maintenance over an initial four year period. The agreement can be extended for two years if requested. Norwegian Police have been long term users of Sepura TETRA radios since purchasing their first devices in 2013.

Ministers warn of scammers with fake energy bill support

A scam alert was issued by ministers encouraging people not to fall foul of fraudulent messages asking them to provide bank details as the energy price guarantee came into force in early October. The government fears scammers could target people by wrongly telling them they need to claim for the support announced due to rising energy bills and the cost of living crisis. There is no need to apply for the schemes, with most customers receiving the support automatically through their energy bill, while households in Northern Ireland will get the same help from November. The business secretary, Jacob Rees-Mogg, said he wanted to: "urge people today to stay alert to scams" because the support would: "reach people automatically" and he underlined that there was no need to apply. He added that the financial help being offered was unprecedented and would protect households and businesses "across the country from what was going to be an 80 percent increase in energy bills this winter". Consumers are being urged to report any suspected scams and the government has once again underlined that no household should be asked for bank details at any point.

NEWS

Americas

Colombia dissidents agree to ceasefire

At least 10 armed groups in Colombia, including the Gulf Clan crime gang and members of the Farc rebels who rejected a peace deal have agreed to participate in unilateral ceasefires, according to the government. President Gustavo Petro took office in August and has promised to seek "total peace" with armed groups, fully implementing a 2016 peace accord with the Revolutionary Armed Forces of Colombia (Farc) and meeting with dissidents and gangs. Among the groups are two Farc dissident groups – the Central General Staff and Second Marquetalia – as well as the Clan del Golfo, the Sierra Nevada de Santa Marta Self-Defence and others Rueda did not name. Leftist rebels and crime gangs are understood to participate in extortion, murder, drug trafficking and illegal gold mining. Petro – himself a former member of the M-19 urban guerrillas – has said his government could offer reduced sentences to gang members who hand over ill-gotten assets and give information about drug trafficking. Petro also wants to restart Havana-based peace talks with largest active rebel group the National Liberation Army (ELN), which were called off by his predecessor. The ELN favours a bilateral ceasefire to pave the way for renewed talks, its top negotiator told Reuters.

CIA websites discovered with flawed security

Research conducted by security experts at the Citizen Lab, University of Toronto, have revealed that the CIA used hundreds of websites for covert communications that were severely flawed and could have been identified by an "amateur sleuth". The flaws reportedly led to the death of more than two dozen US sources in China in 2011 and 2012 and reportedly led Iran to execute or imprison other CIA assets. The university started investigating the matter after it received a tip from a reporter at Reuters. The group has revealed that it will not be publishing its findings in an effort to avoid putting CIA assets or employees at risk. But its findings raise serious doubts about the intelligence agency's handling of safety measures. Using just a single website and publicly available material, Citizen Lab said it identified a network of 885 websites that it attributed: "with high confidence" as having been used by the CIA. It found that the websites purported to be concerned with news, weather, healthcare and other legitimate websites and had been active between 2004 and 2013 and most probably have not been used by the CIA recently.

Guns bought with credit cards in the US will now be trackable

Credit card purchases of firearms in the US can now be tracked and any purchases that are deemed suspicious can additionally be shared with law enforcement, following new measures set up by the International Organisation for Standardisation. The ISO voted in favour of creating a merchant code (a four-digit code that categorises retailers across all industries) for firearms stores. Numerous credit card companies such as PayPal, Stripe and Square don't allow gun purchases. For the credit companies that do, the total cost can be extra high due to interest. As a result, many gun buyers often use cash for their purchases; potential buyers are often seen asking in online forums whether it's better to buy guns with cash or credit, with many voting for the latter.

US and Mexico to break gangs' Haiti stranglehold

The US and Mexico have proposed a multinational force in Haiti to help break the stranglehold of gangs over the distribution of fuel, water and other basic goods. Presenting a resolution at a special session of the UN security council in mid-October, US envoy to the UN Linda Thomas-Greenfield called for: "a limited carefully scoped non-UN mission led by a partner country with the deep, necessary experience". The main port in the country and fuel terminal has been blockaded by gangs, leading to widespread famine and a cholera outbreak. As the session convened there were demonstrations across Haiti, calling for the resignation of the prime minister, Ariel Henry. Negotiations with opposition groups aimed at resolving the crisis have reached an impasse.

Elbit to supply night vision systems for US army

Elbit Systems of America LLC, has been awarded an order valued at approximately $107-million for the supply of Enhanced Night Vision Goggle – Binocular (ENVG-B) systems, spare parts, logistics support and test equipment to the US army. The order will be executed in Roanoke, Virginia and will be supplied during the years 2023 and 2024. The order is part of an Other Transaction Authority (OTA) contract received in 2020, with a potential value that could reach a maximum of $442-million. The ENVG-B integrates powerful night vision capabilities and head-up situational awareness that allow soldiers to navigate and perform at their best in the modern, complex battlefield. ENVG-Bs are equipped with high-performance white phosphor image intensifier tubes for better scene contrast providing soldiers better situational awareness in the dark, but also when there is fog, dust or smoke. The ENVG-B system includes a wireless connection to soldiers' rifle-mounted thermal weapon site and augmented reality overlay, enabling rapid target acquisition and improved situational awareness in various battlefield conditions. Bezhalel (Butzi) Machlis, Elbit Systems President & CEO, said: "This order attests to the quality of Elbit Systems of America's technologies and their unique operational contribution".

NEWS

Asia

Elbit Systems to Supply Hermes 900 UAS to the Royal Thai Navy

Elbit Systems has been awarded a contract valued at $120 million to supply Hermes 900 Maritime Unmanned Aircraft Systems (UAS) and training capabilities to the Royal Thai Navy. The contract will be performed over a three-year period. Under the contract, the company will provide the Thai Navy with Hermes 900 Maritime UAS featuring maritime radar, Electro Optic payload, Satellite Communication, dropable inflated life rafts and other capabilities. The Hermes 900 Maritime UAS is intended to enable the Navy to perform both blue water and littoral missions, dominate vast swathes of sea and long coastlines, communicate with operational vessels and carry out civilian missions such as maritime Search and Rescue and identification of suspicious activities and potential hazards. UAS of the Hermes family have been selected to date by more than 20 customers including Israel, UK, Switzerland, Canada, the United Nations, European Union, Brazil, Chile and Mexico.

Hacker apologises for data breach and drops ransom threat

A hacker seeking a ransom payment from Australian company Optus in exchange for millions of customer records, published 10,000 records online at the end of September before going on to retract the threat and deleting all of their demands. The attacker initially uploaded a text file of 10,000 records to a data breach website before promising to follow it up with 10,000 more records each day for the next four days unless Optus paid $1-million in cryptocurrency. The text leak contained names, dates of birth, email addresses, driver's licence numbers, passport numbers, Medicare numbers, phone numbers and address information. It also included more than a dozen state and federal government email addresses, including four from the defence department and one from the Australian Department of Prime Minister and Cabinet. However, the next morning, the attacker apparently had a change of heart, deleting their posts and claiming they had also deleted the only copy of the Optus data.

IAI announces a new subsidiary located in New Delhi, India

Israel Aerospace Industries has opened a new subsidiary in New Delhi, India. The company's investment in Aerospace Services India is widely regarded as a strong demonstration of IAI's support for the Indian government's 'Atmanirbhar Bharat' (Make in India) vision. It is also believed to demonstrate the commitment to the strong partnership between IAI and DRDO in developing and supporting advanced systems for the Indian armed forces. Boaz Levy, IAI's President and CEO commented: "Aerospace Services India is leveraging top technology, innovation and talent to deliver customer satisfaction so that they can focus on their mission. IAI has a well-established operation in India, working with various partners and customers in the Indian market. Through the years, IAI has pursued a flexible and adaptive business policy to comply and respond to PM Modi's 'Self-Reliance' vision." ASI is establishing state-of-the-art facilities to provide product life cycle support services for the air-defence systems in the country.

Singapore ransomware task force to protect businesses

The Singapore Government has set up an inter-agency counter-ransomware task force to pool representatives from different sectors in an effort to better tackle what has become a growing worry among businesses in the country. The task force, set up earlier this year, will develop and make recommendations on potential policies, operational plans and capabilities to improve Singapore's counter-ransomware efforts. The Cyber Security Agency of Singapore comprises senior government representatives from the technology, cybersecurity, financial regulation and law enforcement domains. Ransomware cases in the country have gone up by 54 percent between 2020 and 2021.

Kaspersky cyberattack warning

Nearly 10 years since Kaspersky unmasked an active cyber-espionage campaign primarily targeting South Korean think-tanks, the state-sponsored group known as Kimsuky continues to show prolific updating of tools and tactics. Kaspersky's senior expert revealed the possibility of this Advanced Persistent Threat (APT) threat actor expanding its operations with its abundant capabilities. Kimsuky, also known as Thallium, Black Banshee and Velvet Chollima, is known to update its tools very quickly to hide its infrastructure and make it harder for security researchers and auto-analysis systems to acquire payloads. Seongsu Park, Lead Security Researcher for Global Research and Analysis Team (GReAT) at Kaspersky, found that the notorious group has continuously configured multi-stage command and control servers (C2) with various commercial hosting services located around the world. A command and control server helps a threat actor control their malware and send malicious commands to its members, regulate spyware and send payload. Park explained: "From less than 100 C2 servers in 2019, Kimsuky now has 603 malicious command centres as of July this year which clearly suggests that the threat actor is posed to launch more attacks, possibly beyond the Korean peninsula. Its history suggests that government agencies, diplomatic entities, media, and even cryptocurrency businesses in APAC should be on high alert against this stealthy threat." In early 2022, Kaspersky observed a wave of attacks targeting journalists and diplomatic and academic entities in South Korea.

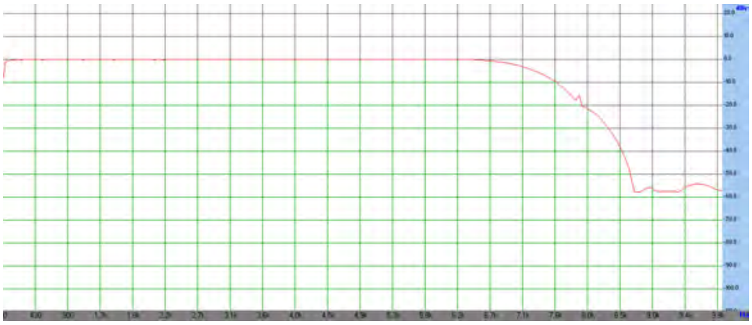
MGT SST-33

DATA SHEET

STEREOPHONIC DIGITAL RECORDABLE STETHOSCOPE - WITH PERSPEX DUST COVER

OVERVIEW

MGT-SST-33 is the best choice when you need to hear through the walls. It processes the audio signal using the greatest stereo digital audio technologies, which have been adapted to this market as a high-reliability DSP system.



To improve the characteristics of all audio paths, high-quality DAC and ADC sample the audio signal at a very high frequency (over-sampling approach).

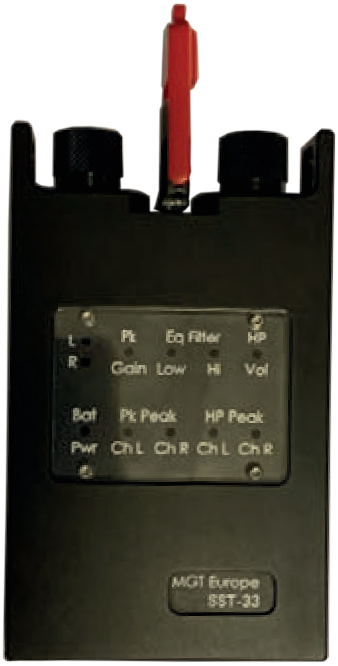
An incredible five-band equalisation technology gives you a crystal-clear audio experience.

All you need to set up the device is the two knobs and the frontal led.

The Host Full-Speed USB Port allows you to plug in a memory stick and record all audio in an uncompressed format.

The MGT-SST-33 has a perspex dust cover and high-quality connectors for the best connections.

TECHNICAL SPECIFICATIONS



Input	2 balanced channels
Bandwitdh	50Hz - 8KHz
Sample Frequency	16KHz
Microphone Gain	59.5db
Microphone AGC	Yes
Line Out Gain	0 ~ 40db
Headphone Gain	0 ~ 40db
Equalizer Bands	5
Gain Each Bands	+/-12 db
Audio Output	Stereo Headphones
Stereo Separation	-70db
DAC	16 bit DAC ADC input sensitivity 0.707 vrms
USB File System	FAT 16 or 32
Compression	None
Power Voltage	3.0V~5.0 V DC
Power Consumption	280mW (70mA at 4V)
Battery	3.7v 1100 ma Li-Ion battery
Size	75mm x 125mm x 20mm

NEWS

Africa

President Buhari: Boko Haram are "fraudulent people"

President Muhammadu Buhari has described Boko Haram as "fraudulent people" who have been overwhelmed by his administration since 2015. Speaking in Owerri in mid-September, the President blamed the elite for not thinking hard about Nigeria, adding that though his government has done: "extremely well," those who are supposed to commend his administration for his achievements have refused to speak out. He also said despite earning so much from crude oil, his predecessors failed to develop the country's infrastructure. "When we came, unfortunately, the militants were unleashed, production went down to half a million bpd. Again, unfortunately, the cost of petroleum went down from $28 to $37." The President additionally claimed that before he came into office in May 2015, Boko Haram terrorists controlled local governments in Borno State, before noting that has become a thing of the past: "Go and ask the hardworking governor of Borno State. Federal Government is in charge now".

Cybercrime against insurance companies rise in South Africa

Cybercrime in South Africa is growing at an overwhelming rate according to a recent survey carried out by Armenian-founded cyber defence firm EasyDMARC. The report suggests that nearly half of South Africa's insurance companies cannot cope with rising cases of email phishing, while banks are similarly struggling to combat spoofing attacks. "Out of 35 South African insurance companies, only 18 have a DMARC policy deployed for email authentication. This means only 51.42 percent of insurance companies are prepared against phishing, spoofing and spamming attacks attempted in their name," the report said. DMARC is a technical cybersecurity standard designed to protect email senders and recipients from cyberattacks. The report also shows that only 18 of the 38 banks using DMARC have set email defence mechanisms that ward off 100 percent of phishing attempts. According to a 2021 Interpol report, South Africa leads Africa in cyber threats and ranks third globally, with 230-million threats detected last year. Most of these (219-million) came through emails.

Uganda unveils tougher penalties for cyber criminals

The Parliament of Uganda passed the Computer Misuse (Amendment) Bill, 2022 in early September to impose tough new penalties on cyber-crimes. The bill is designed to amend the previous act of 2011 to enhance the provisions on unauthorised access to information or data; prohibit the sharing of any information relating to a child without authorisation from a parent or guardian; and to prohibit the sending or sharing of information that promotes hate speech. With deletion of clauses that sought to bar convicts under the law from holding public office or running for elections in 10 years, the rest of the clauses unanimously sailed through uncontested, with MP Gorreth Namugga (NUP, Mawogola County South) dissenting. A new clause to the bill, proposed by ICT committee chairperson, Hon. Moses Magogo, created penalties for computer users who take refuge in pseudo accounts.

Borno PC: 389 policemen killed fighting Boko Haram

The Police Commissioner in Borno, Abdu Umar, has said that 389 policemen have been killed and 450 others injured in the fight against Boko Haram insurgency since 2011. Umar revealed that over 24 police barracks and 30 stations have been destroyed. Speaking at the inauguration of a newly constructed police station and barracks, Umar lauded the state government for its support to the police, adding that the government reconstructed some of the vandalised police stations across the state before commending donors and development organisations for helping rebuild destroyed police structures and facilities.

Nearly half of global terror victims are African

The threat of terrorism and organised crime is becoming increasingly entrenched across Africa according to the head of the UN Office on Drugs and Crime. UNODC chief Ghada Waly warned the Security Council in early October that illegal trafficking is depriving millions of a decent livelihood. Waly explained that there were around 3,500 victims of terrorist acts in sub-Saharan Africa last year – nearly half of those recorded worldwide. The vast Sahel region in particular has become home to some of the most active and deadly terrorist groups, and it is essential to gain more understanding of the links between organised crime and terrorism, through rigorous data collection, Waly added. The evidence is that the illegal exploitation of precious metals and minerals are fuelling the extremists with significant sources of income and benefitting the groups that control extraction, and trafficking routes. She said based on UNODC research: "We have established that illegally mined gold and other precious metals are being fed into the legitimate market, providing huge profits for traffickers". Wildlife trafficking has also been reported as a possible source of funding for militias with the illegal trade in ivory alone generating $400-million in illicit income each year. "We support member countries to put in place the policies, legislation, and operational responses required to better address terrorist threats… In 2021 alone, we implemented 25 counter-terrorism projects in Sub-Saharan Africa, with over 160 activities delivered, and trained 2,500 people," the UNODC chief stated.

DIARY DATES

2022-3 Conference and Exhibition planner

15-17 November ISC East 2022

Manhattan, New York
Organiser: Reed Expos
Tel: +1 203 840 5602
Email: inquiry@isc.reedexpo.com
www.isceast.com

18 December International Conference on Big Data, IoT, Cyber Security and Information Technology 2022

Pune, India
Organiser: Institute of Research and Journals
Tel: +91-8280047516
Email: papers.iraj@gmail.com
www.iraj.in/Conference/10078/ICBDICSIT/

17-19 January Intersec 2023

Dubai, UAE
Organiser: Messe Frankfurt Middle East
Tel: +971 4 389 4500
Email: intersec@uae.messefrankfurt.com
www.intersec.ae.messefrankfurt.com

28 February - 1 March Cyber Intelligence Europe 2023

Bern, Switzerland
Organiser: Intelligence-Sec Limited
Tel: +44 (0) 158 234 6706
Email: events@intelligence-sec.com
intelligence-sec.com

15-17 March DSEI Japan 2023

Makuhari Messe Tokyo, Japan
Organiser: Clarion Events
Tel: +44 (0) 207 384 8246
Email: japan@dsei-japan.com
www.intelligence-sec.com

28-31 March ISC West 2023

Las Vegas, Nevada
Organiser: Reed Expos
Tel: +1 203 840 5602
Email: inquiry@isc.reedexpo.com
www.iscwest.com

25-27 April The Security Event 2023

NEC, Birmingham
Organiser: Nineteen Group
Tel: +44 (0)20 8947 9177
Email: info@thesecurityevent.co.uk
www.thesecurityevent.co.uk

16-18 May IFSEC 2023

ExCeL London
Organiser: Informa PLC.
Tel: +44 (0) 20 8052 0660
www.ifsecglobal.com

14-17 November Milipol Paris 2023

Paris, France
Organiser: Comexposium
Email: visit@milipol.com
https://en.milipol.com/

YOUR MOBILITY SPECIALIST FOR ARMOURED VEHICLES

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

TSS International official distributor for:

RODGARD HUTCHINSON®

TSS HEAVY DUTY WHEELS SEMA WORLD ANTI-TERRORISM SAFETY FEATURES Téléflow

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

GA-ASI's Gray Eagle UAV variant

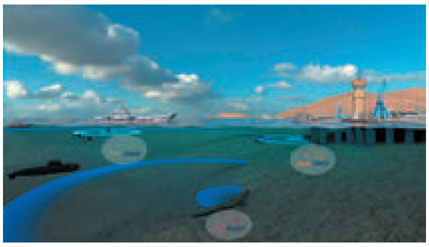
General Atomics Aeronautical Systems, Inc. (GA-ASI) has launched its latest variant of the Gray Eagle line of Unmanned Aircraft Systems: Gray Eagle 25M. The GE-25M brings a Modular Open Systems Approach to the Multi-Domain Operations-capable system to ensure incremental enhancements can be made at the speed of emerging threats. The "M" stands for Modernised and incorporates open architecture aircraft and ground systems, advanced datalinks and an upgraded propulsion system, significantly enhancing the ability to add new capabilities, provide resilience to electronic threats, and deliver expeditionary employment to austere locations. "GE-25M incorporates MOSA across the aircraft and ground system architectures, which enables rapid integration of advanced payloads and communication equipment, along with Artificial Intelligence and Machine Learning capabilities," said GA-ASI Vice President of Army Programs Don Cattell. "This will reduce the sensor-to-shooter timelines, while simultaneously reducing the datalink bandwidth requirements in a contested environment, thus increasing range and resiliency." The onboard 'edge processing' capability will maximise the utility of the Medium-Altitude, Long-Endurance aircraft providing, in near real time, threat Detection, Identification, Location and Reporting (DILR) to the US Army and Joint Force.

Sonar-based solution for underwater defence

DSIT Solutions Ltd. showcased its multilayered defence solution for securing strategic assets against various types of underwater threats in diverse ranges and sea depths. These include hostile military, terror and illegal activities, intrusion, sabotage and smuggling by divers, Semi-Submersible Vehicles, Autonomous Underwater Vehicles, Unmanned Underwater Vehicles, Remotely Operated Vehicles and all submarine types. DSIT presented the Shield Sonar Family – at Euronaval 2022, demonstrating hermetic protection and defence solutions from underwater threats for ports, harbours, shore and offshore sites as well as other strategic assets including underwater pipelines and cables, at sea and on land. DSIT's advanced solutions secure all layers from the immediate, to short and long ranges as well as from shallow to deep-water threats, providing relevant and applicable protection and security solutions for militaries, HLS and Law Enforcement agencies. The solution includes the Shield family of sonars that handle immediate, close-range threats, and are stationary sonar systems. A land-based mission control system manages these sonars, deployed in coastal and littoral waters – utilising advanced signal processing and displays, and machine learning techniques for automation algorithms – and reduces operator workload and required expertise.

Azena smart cam growth

Azena has announced upgrades to its open platform for smart cameras that offer new integration capabilities into existing video surveillance systems and tools for more efficient device management for systems integrators. The new capabilities make it simpler for the integrator to configure and deploy smart cameras using specialised analytics into a customer's existing video surveillance system. Metadata from these specialised analytics, such as weapons detection, tank level monitoring or flood detection, are automatically converted into events for some of the most popular video management software platforms from Milestone, Genetec and Network Optics. This supports integrators in creating vertical and customer-specific, end-to-end solutions that leverage video analytics data across systems and departments. With more than 100 unique apps available in the growing Azena Application Store, integrators can select one or more of those apps or develop and upload their own apps that can be visible and sold only to their customers. This enables highly specialised integrators to further protect their unique approaches to certain vertical markets or other specific customer needs while still leveraging the Azena platform as part of their tailored solution.



Videx strengthens flagship door entry systems

Videx has enhanced two of its door entry and access control systems, adding a new remote relay module to its 4G GSM offering and the VX2300 door entry video intercom. The new remote relays create a more robust and secure entry system enabling all door and gate control to be isolated away from the entrance panel in a secure location. Additionally, the relays can be used for extra services such as triggering additional doors or gates, activating security lighting or other functions requiring a relay for triggering purposes. The Art.2813 relay module is now available for the Videx GSM range of systems and the Art.2313 is available for the VX2300 2 wire video system. These new relays complement the remote relays already available for the VX2200 system (Art.2213) and the IPURE IP range (Art.2505). The Art.2813 comes in a wall mountable small ABS plastic enclosure, powered from 12Vdc and includes a 3A dry contact change over relay output and two additional auxiliary outputs to control up to three outputs per module.

ODSecurity's new contraband detection software

ODSecurity globally launched THEIA – the only full body scanner with automatic threat recognition software available on the market today – at International Corrections and Prisons Association, in Orlando, Florida in late October. THEIA uses complex Artificial Intelligence software, to automatically highlight and identify anomalies in scan images, which will direct staff to potential contraband, thereby stopping contraband from entering and improving the safety of prison estates. It is driven by machine learning algorithms and has been trained on large collections of 'negative' body scan images, ie images that are free of any contraband. These scans have taught THEIA what a negative scan should look like, and it has learnt to recognise anything that should not be part of a full body scan and highlight the anomaly to the operator. The symbiotic relationship between the operators and THEIA reduces operator error and improves overall safety within prisons and custodial estates.

GLIDE BOLLARDS

Flexible, ingenious and totally secure, Securiscape's Glide Bollard HVM system is ideal for protecting busy premises where access needs to be controlled – and yet it couldn't be simpler. The system uses industry-leading shallow fixings and moveable bollards that can be moved side-to-side to create an opening and pushed back into position to prevent unwanted vehicles gaining access.

- Crash-tested and capable of withstanding the impact with a 7.2 tonne lorry travelling at 40mph - without significant bending or buckling
- **Available as the Glide Bollard 30 and Glide Bollard 40, whose footings measure just 210mm and 240mm deep respectively**
- Manually operated and incorporating removable and lockable panels designed to blend into the street or road surface
- Manufactured in the heart of the UK from high quality materials and lowered in place as a complete cassette

All Securiscape Products have been tested to **PAS68** or **Iwa** and have **full certification**

Securiscape Limited **+44 (0) 1335 370979**
info@securiscape.co.uk www.securiscape.com

FOLLOW US ON:

securiSCAPE®
protecting people in public places®