www.intersec.co.uk

intersec

The Journal of International Security

November/December 2024

EYES IN THE SKIES

Why 'heterogeneous' connectivity is the only way ahead for drones

Locked up

Is prison rehabilitation compatible with security?

POLMIL®

ON-GROUND RELOCATABLE SECURITY FENCING

POLMIL® CPNI ASSESSED

POLMIL® PAS 68 RATED
(Test Reports on Request)

POLMIL® MOB ATTACK TESTED

POLMIL® TESTED AND PROVEN

POLMIL® HOT DIPPED GALVANISED FOR COASTAL ENVIRONMENTS

POLMIL® WITH WATER BALLAST

POLMIL® IS A DIVISION OF BLOK MESH UK LIMITED

THE QUEEN'S AWARDS FOR ENTERPRISE: 2016

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

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

Tel: UK +44 (0) 151 545 3050

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

Tel: FR +33 (0) 3.20.02.00.28

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

Tel: Qatar +974 6652 1197

www.polmilfence.com

intersec
Volume 34 Issue 10
November/December 2024

EDITORIAL COMMENT

As events continue to evolve on an almost daily basis as Israel continues to wage war with Hamas in Gaza and Hezbollah in Lebanon, it comes as something of a surprise that the rising threat of Islamic State and al-Qaeda in the UK is regarded as arguably a more signifcant concern for British security . In early October MI5 top bod Ken McCallum issued a stark warning that his agency has: "one hell of a job" on its hands to keep the UK safe as Iran and Russia are also doing their bit to undertake assassination and sabotage plots on these shores. Acknowledging that the revival of IS in Afghanistanhas played a significant part in: "a bit of an upswing" in Britons looking to travel abroad to learn new skills and techniques from the terror group, McCallum revealed that it is not the case that Israel's war has led directly to an increase in terrorist plotting in the UK. He did, however, acknowledge that there has been: "rising public order, hate crime and community safety challenges" that police had had to deal with.

Spy chiefs are understood to be particularly focused on the revival of IS' Afghan affiliate, Islamic State Khorasan Province (ISKP), which has grown in strength after the withdrawal of Western forces from Afghanistan. The group claimed responsibility for the deadly attack in Moscow in March where militants opened fire at a concert, killing 133 people and wounding a further 140 others. Terror threats, however, tend to develop over a long time with the "ripples from conflict in that region" not necessarily arriving on our shores in a: "straightforward fashion according to the MI5 Chief.

Though the current terror threat in the UK remains unchanged at "substantial", McCallum has drawn attention to the way Iran has been behind "plot after plot" here in the past couple of years with five new Iranian-backed attempts uncovered this year alone – taking the total since January 2022 to 20.

Then there's Russia whose GRU military intelligence agency has been engaged in a: "sustained mission to generate mayhem on British and European streets" with everything from arson to sabotage attacks being carried out.

Taken together, the number of MI5's state-based investigations, including the aforementioned Russian and Iranian threats – and not forgetting the small matter of China – has risen by as much as 48 percent in the past year.

Depressingly, McCallum has warned that the number of terror cases that involved MI5 investigating under 18-year-olds is continuing to grow, particularly extreme rightwing threats online. "Sadly, 13 percent of all those being investigated by MI5 for involvement in UK terrorism are under 18," he notes. "That's a threefold increase in the last three years. Extreme rightwing terrorism in particular skews heavily towards young people, driven by propaganda."

Clearly, that "one hell of a job" claim is no understatement and it's more important than ever that MI5 remains vigilant in these challenging times.

Jacob Charles, editor

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 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: November/December 2024

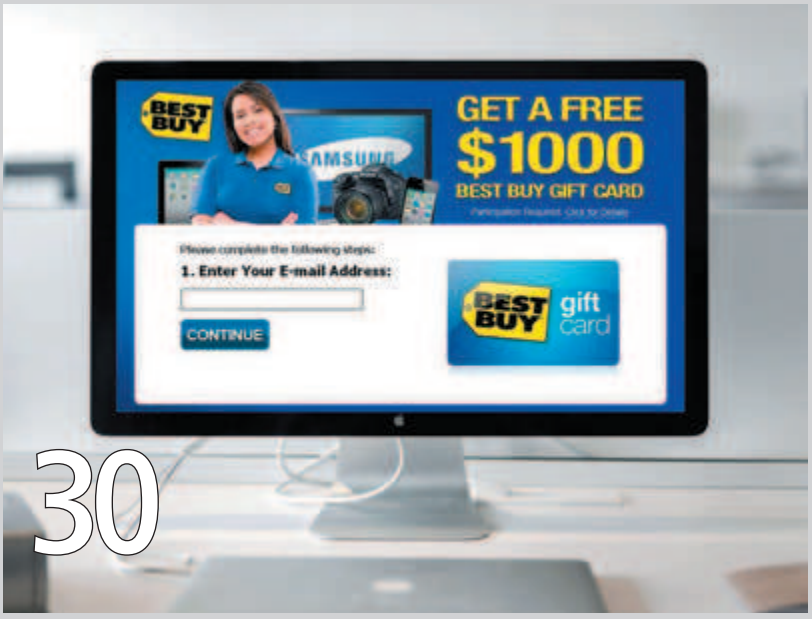
CONTENTS

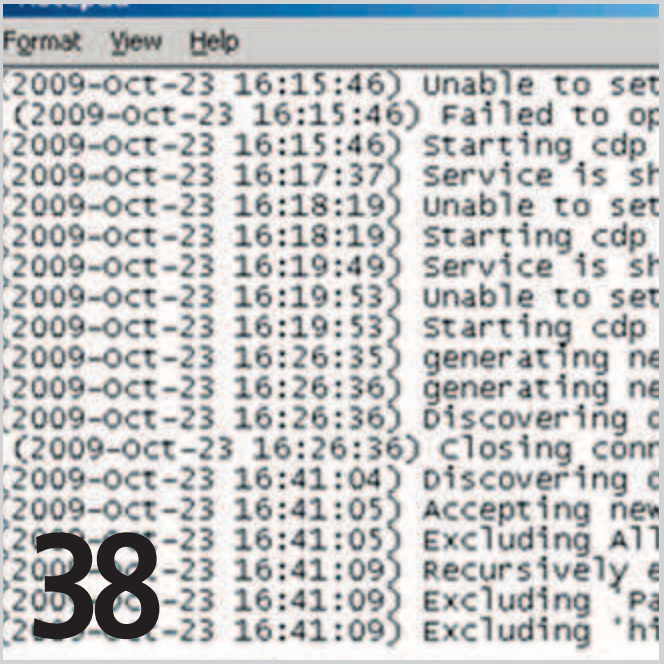
November/December 2024 www.intersec.co.uk

intersec

Features

Regulars

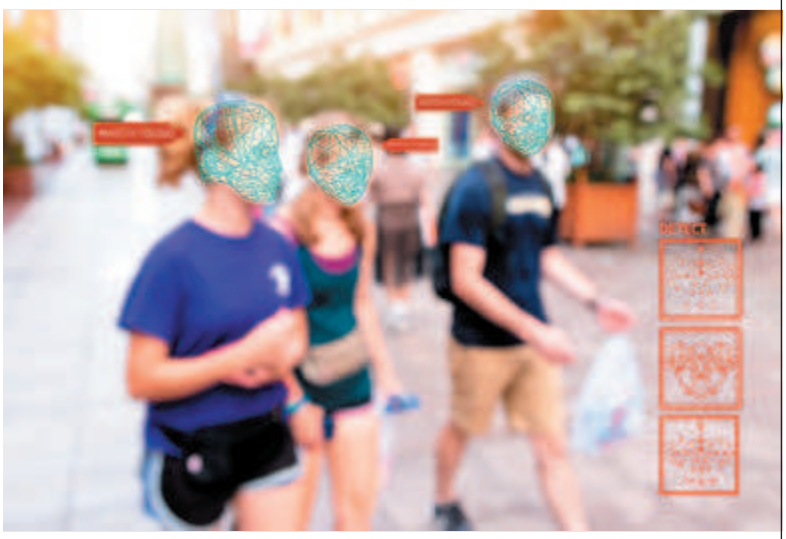




FACIAL RECOGNITION MYTHBUSTER

Tamara Morozova *examines some of the leading misconceptions about facial recognition*

Facial biometrics is not a novel technology, it is being used to elevate security and operational efficiency for more than a decade. Although the applications of facial recognition technology (FRT) still requires vast exploration, its footprint is constantly deepening. As its adoption expands over federal and private operations, questions about the technology's reliability and legality surface. The misinterpretation of advanced technologies is nothing new, it comes as a byline of lack of awareness and unfamiliarity. In this article, we'll be busting some common misconceptions around facial recognition technology.



FACIAL RECOGNITION CAN LEAD TO FALSE IMPEACHMENT OF INNOCENT PEOPLE

Contrary to the general belief, facial recognition systems (FRS) do not identify each and every individual under a camera. Instead, the system is trained to verify the presence of a known offender according to the pre-fed offenders list. It supports the traditional techniques of tracing the whereabouts of the person of interest, as the security officials no longer have to guess if an individual under the camera is the criminal or not. The system speeds up the process and identifies the person for faster and accurate security compliance. So, there are no risks of innocent people getting falsely condemned for a crime as facial recognition efficiently works to prevent it.

FACIAL RECOGNITION TECHNOLOGY PROPAGATES RACIAL BIAS

Facial recognition technology is becoming more and more reliable as the algorithms advance. The problems of false positives and mis-identification occur when an FRS is not tested on a diverse sample. Nonetheless, the frequency of such errors is estimated to be 0.2 percent or less, according to the studies by leading technology regulatory institutes. Especially in the context of bias on the ground of colour of skin, there is no sound evidence of differences in identification results. Growing adoption of facial recognition technology over the years has helped training the technology to work precisely under adverse conditions and across diverse data sets. Following this, facial biometric systems have come to achieve accuracy with chances of error falling down to near zero.

FACIAL RECOGNITION TECHNOLOGY POSES PRIVACY RISKS

This narrative is a very common misconception. Contrastingly, facial biometrics is one of the least instigators of privacy breaches. It can not be easily compromised like alphanumeric passwords, unique identification numbers or hyper-personal information. When a face image is scanned under a facial recognition engine, it is converted into numeric values to match the identification algorithms in the technical system. In other words, the mode of reception of a person's face biometrics is translated into the language a computer system can comprehend, making it almost impossible to misuse. Also, such technologies are subject to compliance with global privacy policies like GDPR, committed to data protection and authorised use.

PEOPLE'S FACE IMAGE DATA IS STORED IN FRS

Since the facial biometrics systems work on identification only, the area under surveillance is accessed to verify a person of interest. The system matches the individual's data points to the existing identification values to verify the presence of a blacklisted person. The faces of unidentified persons, on the other hand, are neither disclosed nor stored by the system.

BIOMETRICS CAN BE EASILY FOOLED

One of the prime capabilities of a facial recognition system is liveness detection, which differentiates an actual person from a synthetic identity. So, an accurate FRS can not be fooled by deep fakes, images of the authorised person, lifting the eyelids of a person or through synthetic identity proofs. In fact, it prevents identity cloning frauds, which can otherwise be troubling because of traditional password-based access control and slow security processes. AI-powered facial biometric systems rely on advanced algorithms updated time and again to counter the challenges of evolving security concerns. Experts have come to vouch for innovative technologies that lead the way to build a robust security infrastructure.

Being a complex technology, it's only natural that myths exist around the use and implementation of facial biometrics. In order to trust a technology, a deep understanding may not be required but awareness of its capabilities can open up the way to exceptional possibilities. Facial biometrics is meant to restore trust on security operations, while improving experience and efficiency.

Biometric facial recognition systems have come to achieve accuracy with chances of error falling down to near zero

Tamara Morozova is CEO at RecFaces.

Picture credit: AdobeStock

Picture credit: IDMCF

WAR ON ISRAEL

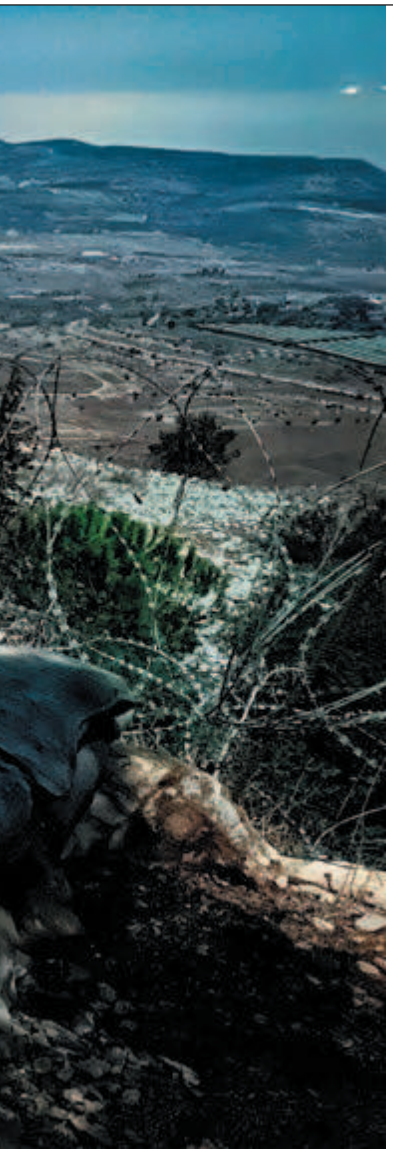
Jeanne McKinney *examines Hamas and Israel's race to secure the grail of power in the Middle East*

The following article is largely based on a series of one-on-one interviews with an unnamed member of the IDF community who remains anonymous due to security issues in an active war. A name has been assigned to protect this warfighter: IDF Community Member (IDFCM).

A little over a year from the heinous Hamas massacres on Israel's civilian communities and military posts on 7 October, Israel finds itself fighting in a war on seven fronts – Gaza, West Bank, Lebanon, Syria, Iraq, Iran and Yemen. On 14 October, Brigadier General Amir Avivi – founder and Chairman of Israel Defense and Security Forum (IDSF) – gave a briefing reviewing the progress of dismantling these terrorist groups' attack plans and operations. He begins lamenting when Israel's defence system failed to intercept and destroy two drones launched by Hezbollah that made it to training base Golani, (near the town of Binyamina) resulting in the deaths of four Israeli soldiers and injuries to others.

The Golani Brigade, a unit in the IDF 36th Division, is considered an elite Army unit. Two Golani battalions were there on 7 October and suffered grievous casualties, reported FDD. A battalion computer and communications officer explained how hi-tech plays a huge role in IDF's 'circle of fire' to identify and bring the fight to the enemy, minimising friendly fire. That day, as hard as it was fighting in multiple locations, Golani, like 300,000 other soldiers called up to respond to the 7 October attack, spent over ten days defending Israeli villages from a second Hamas wave – eliminating all invading terrorists.

To compare, at the height of the war in Afghanistan Obama had surged 100,000 US troops into the country.



The view of Israel from a former Lebanese army outpost that IDF forces took

Those forces worked with nearly 190,000 Afghan security forces to destroy the Taliban chokeholds and entrenchment throughout the land. Fifty other nations were part of the ISAF coalition engaged in the goal to defeat al-Qaeda and Taliban allies.

Israel has had no such help to fight terror. Yet, to date, the Israel War Database shows it has killed 101 Hamas leaders. Ground operations in the Gaza Strip as of 23 October, included an IDF airstrike on a Hamas command and control site in Gaza City, IDF 162nd Division clearing in Jabalia, and elements of IDF 143rd Division operating in Rafah. The IDF has announced multiple evacuation zones in the Gaza strip since December 2023.

Post 7 October, the game drastically changed and Israeli troops trained to enter Gaza, taking over strategic locations. At this point, there was no more border between Gaza and Israel proper. Gazans were not crossing over into Israel to work. Outsiders, including US officials, were crying foul to Israel for the human suffering in Gaza – demanding aid be let in. "Israel enables aid to get into Gaza, says IDFCM. Yet we are faced with terrorists taking over the food trucks, just like they did in Somalia. So, it is with Gaza." He adds, "That's true Islamic power. The terrorists take it by force and if you want anything, you get it from them. It is a microcosm of how the Middle East works – it is the one who carries the biggest stick."

Outsiders do not understand the Middle East cultures, believes IDFCM, and he is not the only one who thinks the US empowers the wrong people. Plenty of Americans agree speaking up on podcasts, talk shows and in the news. Right now, the US is empowering the terrorists they fought originally in Afghanistan by sending them billions in cash (something we'll cover in more detail in a future issue). Biden rewarded Tehran for seizing American hostages – empowering them with a $6-billion release of Iranian assets for the Mullahs. This was preceded by a $1.5-million ransom payout by Obama for kidnapped Americans in 2009 and in 2016 another $1.7-billion plus seven jailed Iranians in exchange for five American hostages.

Conversely the Trump administration secured the release of more hostages seized without ransom payments and used only a prisoner swap, outlines the Heritage Organization.

If we pay, Iran will continue to seize hostages. "The money will bolster Iran's embattled dictatorship, provide it with additional resources to violently repress its own people, and boost the threat posed by its missiles, drones, proxy groups and advance its threshold nuclear weapons program."

Global security is not solved by laying down to terrorists' demands. We must make the demands. The world must recognise in Gaza they have enjoyed full Palestinian autonomy, able to build what they want, do what they want and yet have allowed Hamas to blow their opportunities and set them up for failure and war. This, while Israel has supported them. With a population of four-five million in both Gaza and Judea Samaria (West Bank) "why don't they have their own power plants, waterworks, *etc.*, as they have a ridiculous amount of money?" questions IDFCM.

To give context: "Five million people have received ten times more than what the Marshall Plan put into the rebuilding of Europe." Congress appropriated $13.3-billion for post-World War II recovery. "That's how much foreign aid has gone to the Palestinians," IDFCM explains.

Yet Israel is the one starving the Palestinians, reports mainstream news. There is no official Palestinian 'state' and Hamas' invasion is for land indigenous to the Jews. Power speaks the loudest and Israel has demonstrated that to Hamas, Hezbollah and their parent Iran since day one of this war began on 7 October .

ISRAEL IS NOT WASTING ITS TIME OR GIVING SECOND CHANCES TO ISLAMIC TERRORISTS

Brigadier General Avivi has been transparent about Israel's actions and the goal: "to bring the Iranian regime to its knees, and really deprive them of any future nuclear capabilities. This is not a campaign that can be done in a week or two. It might be many months." As the major campaign evolves, Israel's eyes are on the US election and the new president. "We really hope it will be an administration that will be proactive because we want to deal militarily with Iran because there is no other way to change riots in the Middle East," confirms Avivi, adding, "If Israel needs to do it alone, we'll do it alone, but it's much better to have a coalition dealing with this."

Avivi acknowledges after speaking with one of Israel's air defence generals: "Israel has really focused a lot on building capabilities to deal with rockets and missiles, but a bit less focus on the drones. We need to do a further buildup of capabilities," yet assures, there is no technology gap or shortage of means: "The Army needs to buy more radars of different kinds, procure capabilities like they had in the past… and in the coming couple of months the laser will become operational, and this will help a lot."

Israel's Iron Beam laser air defense system operates against rockets, mortars, UAVs, cruise missiles, and low-flying targets. The Iron beam will equalise effectiveness with economy of air defence to shoot down missiles and drones that are cheaper for terrorists to deploy. The new laser weapon in concert with the Iron Dome missile batteries that can deal with large rocket barrages and are not impaired by weather, helps Israel further tighten its defence envelope. The IDF is operating with seven divisions, three in the South and four in the North, remaining proactive and fierce with its responses.

As the capabilities of Hamas and Hezbollah degraded rapidly, Israel started to look to the East. "Israel is shifting the centre of gravity of the buildup of the forces to Iran," said Avivi two weeks after Iran fired 180 missiles into Israel in what Iran claimed was a response to killing Hezbollah leader, Hassan Nasrallah. The Israeli military said most of the missiles were intercepted, although some landed on the ground. At that point, the world watched – sat back and did nothing to Iran and instead became worried that the war "would escalate". Israel is already fighting terror on seven fronts; is that not major escalation?

This map illustrates the fronts that Israeli forces are currently fighting

Picture credit: Instagram

A recap of Israel's strategic moves in a Middle Eastern world that only respects might. The *Wall Street Journal* reported, first Israel removed the Hamas de facto government out of the Gaza enclave, destroying strategic terrorist complexes in an expansive labyrinth of tunnels spanning 640km, leaving fewer places to hide. Then, it took out Hezbollah's leadership and started ground operations in border areas of Southern Lebanon. Prime Minister Benjamin Netanyahu put his sights on Iran in a tit-for-tat move for an Iranian ballistic missile attack on Israel on 1 October.

THE US IS EMPOWERING THE TERRORISTS THEY FOUGHT ORIGINALLY BACK IN AFGHANISTAN

Israel wasted no time to hunt its targets down. Yahya Sinwar, the architect of the 7 October massacres who lived in Gaza's subterranean city, was on the top of the list. On 16 October, Israel struck, killing Yahya Sinwar, by forcing him from the tunnels. Israel's internal security agency Shin Bet has been busy working with the military, ratting out the underground and securing communities above ground, to prevent these same people from ever attacking Israel again.

Sinwar had a chance to escape, according to the *Wall Street Journal*, in exchange for allowing Egypt to negotiate a release of the hostages still held by Hamas, but he refused. That may be hard to believe because Israel will never forget the horrors of 7 October, and most likely, once located, would have never let Sinwar continue his plan to remake the Middle East. Sinwar's shocking assent to war resulted in devastation for Gaza and widespread suffering throughout the region. People, homes and livelihoods were wiped out as he sought to cut off the hand that gave Gaza a chance.

What have we learned so far from Israel? It is not wasting time or giving second chances to Islamic terrorists. Its diplomatic relations with other Arab states have to date survived this war. It stays at the planning tables and develops defensive and offensive strategies by day. It responds with resilience and precision to the countless attacks it has endured this past year. It wants to bring the remaining hostages home and is leaving a legacy as a terrorist terminator in the bloody game that erupted on 7 October.

Israel is growing its defence industry, producing its own armaments. "You want to be as independent as possible," says Avivi, acknowledging Israel does depend on the US National Security Council decisions as allies. "We need to produce our own munitions and have an Army big enough and sophisticated enough to defend the people of Israel. We do not expect anybody to fight for us." That said: "When we talk about Iran and the threat to the globe, it is not just Israel's problem. It is a global issue and needs to be treated as such."

"America likes strong allies, not weak allies," believes Avivi. Israel is proving it every day. One small country has literally deconstructed leadership of two regional terror groups and is gearing up to face wild card Iran. Israel is determined, ready, and exacting ●

Part three of this series will examine Israel's first ever attack on Iran's military bases that was unprecedented, as well as the latest developments in the Hamas, Hezbollah, Iranian war on Israel.

JEANNE MCKINNEY IS AN award-winning military journalist, book author, and documentary filmmaker. She recently published the true historical account of *Triumph Over the Taliban: The Untold Story of US Marines' Courageous Fight to Save Camp Bastion* (now on Amazon). McKinney also wrote, directed, and is currently producing a limited documentary series called *Ronin 3: The Battle for Sangin* - that follows 3rd Battalion, 5th Marines through a labyrinth of murder holes and IEDs in a heavily entrenched Taliban stronghold in 2010, on mission to restore security to the local Afghan people.

A night shot from a former Lebanese army outpost that IDF forces took over. Israel is in the background.

Picture credit: IDMCF

DURABOOK
Prepared for the Unexpected

UNLOCK A NEW ERA OF AI PC EXPERIENCES

Dedicated NPU to run AI applications faster

14.0" Full HD DynaVue® sunlight readable display

Certified by MIL-STD 810H military-grade standards

Thunderbolt 4, Wi-Fi 7, Bluetooth 5.4, 4G/5G and GPS

INTRODUCING THE DURABOOK Z14I & S14I AI-POWERED RUGGED LAPTOPS

The next wave of rugged computing is here. Durabook Z14I and S14I laptops empowers organisations within the utilities, field services, manufacturing and security sectors to enhance field operations with on-device AI capabilities. Equipped with a dedicated Intel® Core™ Ultra NPU for AI acceleration, both laptops are well-suited for field operations, unmanned aerial vehicle (UAV) control, real-time analytics, and on-site project duties, ensuring seamless productivity and unparalleled experience.
Durabook Z14I and S14I AI-powered rugged laptops invite users to embrace a new era in AI computing.

Windows 11

intel CORE ULTRA 7

intel CORE ULTRA 5

www.durabook.com

BREAKING THE CYCLE

Sid Madge *outlines the future of prison rehabilitation programmes and asks if they can be compatible with security*

One of the most contentious issues in the discussion about rehabilitation is the early release of prisoners, a measure often used to ease overcrowding in prisons. Early release programmes, such as parole or home detention curfews, are designed to reward good behaviour and encourage participation in rehabilitation programmes. While they offer potential benefits in terms of reducing reoffending by reintegrating prisoners into society gradually, they also raise serious security concerns.

Victims of crime often feel betrayed by a system that releases offenders back into society before their full sentence is served. Their concerns are valid, early release sometimes results in offenders reoffending before they have fully addressed the root causes of their behaviour. This creates a feeling of insecurity and fear, especially for victims who feel that justice has not been fully served.

Another significant concern linked to the early release of prisoners is the rise in security issues within retail environments. Shoplifting and petty theft have become more frequent as individuals struggle to find employment after release. Without adequate support, ex-prisoners, many of whom face financial instability and homelessness, turn to crime out of desperation. Retailers are bearing the brunt of these increased security threats, with incidents of shoplifting and property damage on the rise in many areas.

In England and Wales the prison population has soared to over 83,000 people

This not only represents a failure to rehabilitate individuals before their release, but also poses a broader public safety issue. Retail workers and business owners feel increasingly vulnerable, as they witness a rise in theft and other low-level crimes that are sometimes carried out by recently released offenders. The costs associated with this increase in criminal behaviour are not only financial but emotional, as retail employees are often on the front lines of these security breaches.

Despite the security concerns, it is not necessarily true that rehabilitation is not the way forward or that rehabilitation is not compatible with security. In fact, ultimately, rehabilitation done right should be a great step forward in those terms.

It's important to consider the scale of the problem. In England and Wales, the prison population has soared from around 18,000 in the early 1900s to over 83,000 today. Similar trends are seen across Scotland and Northern Ireland. This sharp rise is a symptom of a system that places emphasis on incarceration over rehabilitation. As prisons swell, the financial and social burden grows too, costing the UK taxpayer around £5 billion a year to maintain the prison system, while the cost of reoffending adds a staggering £18 billion annually. This escalating financial strain underscores an undeniable truth: imprisonment alone is not an effective deterrent.

Yet behind these staggering numbers are human lives, individuals who have fallen into a vicious cycle of crime, punishment, and repeat offences. While prisons were designed to serve as correctional facilities, they are increasingly becoming revolving doors. Nearly half (48 percent) of released prisoners in the UK reoffend within a year. For some groups, such as those serving short sentences, this rate is even higher. A significant reason for this is that, in many cases, rehabilitation is overlooked or underfunded, leaving prisoners ill-prepared to reintegrate into society.

One fundamental shift that must occur is focusing on the people inside prisons, not the prisons themselves. Brick-and-mortar facilities don't reform individuals. Holistic, human-centred rehabilitation programmes do. Many prisoners enter the system having faced severe disadvantages: poverty, lack of education, trauma and addiction are prevalent. These individuals need more than just containment; they need tools to rebuild their lives.

Prisons should be places of transformation where individuals are not only punished, but also given opportunities to break the cycle of criminality. Programmes that provide education, vocational training and therapy are essential, yet often underutilised due to budget constraints or overcrowding.

Addressing the human element inside prisons is key to breaking the cycle of despair. Many prisoners lack a sense of purpose or hope and, when released, return to environments where their circumstances remain unchanged. Without hope, meaningful rehabilitation is nearly impossible. In these cases, we must focus on instilling self-worth and purpose in inmates. Support programmes tailored to their specific needs can provide this, whether it's through education, skill-building or even restorative justice practices that help them take responsibility for their actions and repair harm done to victims.

It's important to recognise that no two prisoners are alike. The criminal justice system often approaches rehabilitation with a 'one-size-fits-all' mindset, but this is fundamentally flawed. Each prisoner arrives with a unique set of experiences, challenges and traumas. Some may struggle with addiction, others mental health issues and still others a history of abuse. Addressing these underlying causes of criminality requires personalised interventions.

By customising rehabilitation programmes to the needs of individual prisoners, we can begin to see more meaningful outcomes. This can include offering specialised addiction services, therapy for trauma survivors or job training tailored to individual skills and interests. The focus should be on equipping each prisoner with the tools to avoid reoffending by addressing the root causes of their criminal behaviour.

Perhaps one of the most overlooked aspects of incarceration is its intergenerational impact. Studies show that children with incarcerated parents are up to three times more likely to enter the criminal justice system compared with their peers. This is largely due to the instability that incarceration brings to family dynamics, leading to poor educational outcomes, social isolation and a lack of positive role models.

PRISONERS SHOULD BE GIVEN MEANINGFUL OPPORTUNITIES BREAK THE CYCLE OF CRIMINALITY

To break this cycle, support for prisoners must extend beyond the walls of the prison. Family support programmes that provide care and resources to children of prisoners can make a profound difference. By addressing the needs of these children, we can help break the intergenerational cycle of incarceration.

The financial cost of reoffending, £18-billion annually in the UK, is a glaring indicator that radical change is needed. This isn't just about money; it's about lost potential and human suffering. Reoffending is driven by a complex mix of factors, including unemployment, mental health issues, addiction and homelessness. Many prisoners leave the system only to find themselves back in the same circumstances that led to their initial imprisonment.

Radical change must start by addressing these factors head-on. Instead of focusing on punishment, the criminal justice system should prioritise equipping individuals with the skills, resources and support necessary to reintegrate successfully. This includes access to stable housing, job opportunities, mental health services and addiction treatment.

Prison rehabilitation programmes that focus on vocational training and education have shown great promise. These initiatives provide prisoners with practical skills that can help them secure employment upon release, which is a key factor in reducing reoffending. Currently, only 17 percent of prisoners in the UK are employed upon release, a shocking statistic. If individuals can learn new trades or develop skills during their incarceration, they are far less likely to return to a life of crime.

Successful examples of these initiatives include construction training programmes, where inmates learn valuable skills such as bricklaying or carpentry,

or literacy and numeracy courses that prepare them for further education. By investing in these types of programmes, we not only reduce the burden on the prison system, but also provide individuals with the opportunity to lead meaningful, productive lives after release – making their communities more secure.

NEARLY HALF (48 PERCENT) OF RELEASED PRISONERS IN THE UK REOFFEND WITHIN A YEAR

One of the biggest barriers to reintegration is the stigma that former prisoners face. Society often views those with a criminal record as irredeemable, making it difficult for them to find employment, housing or community support. This stigma perpetuates the cycle of reoffending, as former prisoners are often left with few opportunities outside of crime.

Removing this stigma is essential if we are to reduce reoffending rates. Employers, landlords and society at large must be willing to give former prisoners a second chance. One way to encourage this is through restorative justice programmes.

Restorative justice offers a powerful alternative to traditional punishment. This approach encourages offenders to understand the impact of their actions, make amends with their victims and take responsibility for their behaviour. It also provides victims with a voice and a sense of closure, which can be empowering.

In combination with community support, restorative justice can be a transformative tool. Communities can play a key role in supporting former prisoners as they reintegrate into society. By offering mentorship, job opportunities and social support, communities can help reduce reoffending rates while creating a safer and more inclusive environment for all.

Rehabilitation programmes have already shown success in reducing reoffending rates. Examples such as Norway's prison system, which focuses on rehabilitation over punishment, have demonstrated that treating prisoners with dignity and equipping them with skills and support can lead to lower recidivism rates. In the UK, several pilot programmes focusing on education, mental health and restorative justice have shown promising results.

However, these programmes need to be scaled up and properly funded to make a real impact. A shift away from purely punitive measures toward a focus on rehabilitation, restoration and reintegration is essential to address the rising prison population and reduce the cost of reoffending.

The challenge for policymakers and prison officials is finding the right balance between rehabilitation and public safety. Early release schemes must be accompanied by stringent risk assessments and adequate supervision of offenders. Otherwise, the public, including victims, are put at risk. Furthermore, any reoffending during early release can damage public confidence in rehabilitation as a whole, potentially leading to harsher sentencing policies that prioritise punishment over rehabilitation.

Effective rehabilitation programmes must address these concerns by offering former prisoners the skills and opportunities they need to secure legal employment. Without viable alternatives, many fall back into criminal behaviour, exacerbating security concerns for both businesses and the wider community.

The future of prison rehabilitation programmes lies in a radical shift in how we view incarceration. Punishment alone is not enough; we must focus on rehabilitation, restoration and reintegration. By addressing the root causes of criminal behaviour, supporting individuals through personalised rehabilitation programmes and removing the stigma that surrounds former prisoners, we can create a system that works for everyone. The cost of inaction is too high, both financially and socially. It's time for a new approach, one that prioritises human dignity, hope and the chance for a better, more secure future ●

SID MADGE is the founder of Meee and the creator of the Counting on Confidence programme, designed to foster the belief that education and learning are vital for leading a more fulfilling and positive life.

Each prisoner arrives with a unique set of experiences, challenges and traumas

Picture credit: AdobeStock

Kestrel TSCM ® Professional Software

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

Signals Intelligence Support System ™

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

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

Kestrel TSCM ® Professional Software | Kestrel ® SIGINT Professional Software

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

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

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

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

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

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

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

Kestrel-net ™

Actionable **RF** Intelligence

www.kestreltscm.com

VILUTION

Your vision , Our solution

United Kingdom & European Union Master Distributor

Professional Development *TSCM* Group Inc.

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

AERIAL AUTOMATIC

Tristan Wood *explains why 'heterogeneous' connectivity is the only way ahead*

Some forecasts predict the drone economy exceeding $90-billion globally by the end of the decade as numerous industries realise the potential to transform their operations, from enterprise and logistics to first responders and defence.

The market materialised in the late noughties, originally out of a military requirement but was also quickly adopted in civilian life, initially for aerial photography and video. News, media and broadcasters followed not long after.

In the ensuing two decades the commercial and civil market has experienced exponential growth, attaining a worldwide value of $2.9-billion by 2018, more than doubling in size since then. According to Statista, excluding defence, its market value is forecast to reach $4.7-billion by 2028, with nearly 1-million drones expected to be in operation in the UK alone by 2030 (PwC, 2022).

Today, UAVs are making themselves indispensable in myriad other sectors, including disaster recovery, search & rescue, weather tracking, geotechnical mapping, precision crop monitoring, through to law enforcement and border control. As increasing investment pours into this still nascent industry annually, the development of hundreds of more applications are underway, including those more left of field, such as patient drug-delivery.

All UAS applications raise two principal safety concerns: aerial collisions and loss of control

As the market develops, so the world around it needs to adapt quickly, with more infrastructure required to maintain safe operations in the face of growing volumes of traffic, and with that, complexity and risk. This goes beyond just 'hard' infrastructure, such as take-off and landing sites and air traffic management control systems, but necessarily includes services such as cyber security, insurance and fleet financing.

While governments and regulators work hard to clear the way for the safe, ubiquitous application of UAS, a major focus for their attention will concern aircraft visibility and identification. However, nothing will take the place of the need for robust communication and safety, especially when it comes to BVLOS operations.

Policymakers around the world are fine-tuning their approach, balancing privacy, security and environmental concerns with the many benefits UAS clearly offer. A decade ago, the US Federal Aviation Administration began offering exemptions for drone companies to operate including for use cases in insurance, construction and agriculture. Today it's a global conversation, with many authorities, including those in China, India and the UK, exploring how to create a regulatory and licensing framework to support such a fast-growing but inherently risk-bearing industry.

All UAS applications raise two principal safety concerns: aerial collisions and loss of control. Mid-air collisions can occur if the pilot cannot see or avoid crewed aircraft in time, especially when flying sub-500 feet, and so this includes helicopters, aircraft taking off and landing, or agricultural aircraft maintaining crops at low altitude. In the US, reports of drone-sightings from pilots, police and the public have increased five-fold over the past year, and the same goes for the rest of the world including in China, Dubai and the UK where a number of near-miss incidents have occurred and been reported.

The second category, loss of control, can result from a system failure or if the drone flies beyond its signal range, or from frequency interferences and hackers. While onboard systems like RTH (Return To Home) and DAA (Detect And Avoid) reduce some of the risk in these situations, mission-critical tasks fail with potentially unacceptable consequences. However, there's an even bigger problem – no connectivity at all.

So, how do you guarantee connectivity when only 20 percent of the globe is covered by terrestrial networks? And if satellite is the answer, even with 'low cost' LEO arriving on the scene, Starlink among them, what's the cost penalty for always-on must-have connectivity?

Commercial drones that use conventional RF (Radio Frequency) datalinks generally employ 2.4GHz or 5.8GHz frequencies, both of these falling within the unlicensed industrial, medical and scientific (ISM) segments of the spectrum. It's tried and tested, scalable and generally safe this side of the horizon, but not for BVLOS, nor is it robust enough to allay hijacking and jamming.

UAVs that use licensed and regulated cellular communications will use either LTE/4G, which uses a range of frequencies below 6GHz, or 5G connectivity, which offers connection speeds that are hundreds of times faster still and ideally suited for resource-heavy operations such as real-time HD footage during autonomous deployment.

These can be single or multi-sim, including e-sim, and while these services have the potential to offer a good range, they are completely dependent on physical infrastructure and cell towers, which excludes remote territories and about 80 percent of the globe's surface! Finnish telecommunications business Nokia has recently partnered with Swiss mobile provider Swisscom to deploy a nationwide drones-as-a-service (DaaS) network across Switzerland. Public safety agencies such as police and fire services will be able to request a drone flight from Swisscom Broadcast, not dissimilar to a ride-sharing service, to access real-time data and provide live situational awareness reporting of incidents. In territories where cellular companies can collaborate like this, and importantly where there's already infrastructure in place, these are great solutions. Unfortunately, most of the globe's surface is nowhere near a terrestrial network and is unlikely to be any time soon.

NEARLY 1-MILLION DRONES ARE EXPECTED TO BE IN OPERATION IN THE UK ALONE BY 2030

Satellite technology, with high uptime and reliability, can offer global always-on communication and control. Historically, satellite technology has been expensive to integrate and generally been deployed on large, high-endurance and military UAVs flying over large distances and at high altitude. Few commercial deployments have been able to justify the capital and operational costs, the power budget and equipment weight associated with satellite connectivity, especially when they may be operating at low elevations where line of sight to satellite may be compromised.

Despite recent advances in telecommunications technology – from 5G and disruptive low-cost LEO satellite services – no single network service can address the exponential demand for seamless connectivity on the move. Nor is there any provider which can offer a single comprehensive solution that can address coverage, bandwidth, reliability and most importantly cost.

As we have seen, all technologies have their advantages, so what if one could blend all of these together, with none of their downsides? The answer is true hybrid – or more accurately, a heterogeneous connection to provide the most resilient solution to always-on, ubiquitous connectivity well beyond the horizon, independent of the coverage of terrestrial infrastructure and not solely reliant on satellite.

Designed to meet the challenges presented by speed and mobility as an asset moves through different areas of network coverage, smart networking enables a dynamic connection to various operators using a range of underlying communication technologies such as 3G, 4G, 5G, wi-fi and satellite.

True hybrid is not a failover or redundancy technology, neither being the same thing anyway. At their core, true hybrid networks become 'heterogenous' – turning a single bonded connection – fixed line, cellular, satellite, point to point radio, whatever the underlay or infrastructure – into one

seamless connection. The benefits of which, for the user, are off the grid. A heterogeneous connection also enables intelligent management of physical, virtual and financial resources to suit an almost limitless range of conditions.

Central to hybrid is SD-WAN – a technology that uses software-defined networking concepts to distribute network traffic across a Wide Area Network (WAN). This architecture creates a virtual overlay that bonds underlying private or public WAN connections, such as wi-fi, 3G, 4G/LTE, 5G, LEO, GEO & MEO satellite. As a result, hybrid SD-WAN networking can agnostically combine and transition between these networks.

BEING ABLE TO INTEGRATE EXISTING CONNECTIVITY WITH FUTURE SERVICES IS A POWERFUL PROPOSITION

In this way, multiple network technologies are able to work seamlessly together, actively sharing the load and resources, by combining and binding together a potentially unlimited variety of bearers into a single 'pipe'.

Delivering a faster and, crucially, more reliable service, a hybrid platform adapts to a range of variables associated with each bearer's performance and any other environmental conditions affecting it, in order to optimise performance and manage costs. Similar to how voice calls are routed for minimum cost, settings in a hybrid environment can be adjusted to use the most cost-effective option, like prioritising cellular over satellite if it is performing well enough. The same approach can be taken for QoS to ensure important applications perform well despite limited network capacity and changing bandwidth and latency. Being able to integrate existing with future connectivity services is also a powerful proposition enabled by the inherent agnostic characteristics of software defined network technology.

The concept of a UAV – fitted for example with a world-first solution like RazorLink, which Inmarsat has embedded within its newly launched maritime-focused NexusWave – agnostically making use of any carrier network, based on location, cost or quality of service, has too long been a guarded secret. But it shouldn't be. And in UAS and many other sectors, the market opportunities are seemingly unlimited for the adoption of true hybrid.

Many other industries spanning defence, space exploration, connected and autonomous vehicles, emergency services, telehealth, cloud-based HPC, as well as AI and machine learning, require more than just connectivity – they demand an 'intelligent connection'.

Few theatres in life push the boundaries of technological innovation more than defence, and in Ukraine we have watched and read daily news about the impact of drones in changing the course of combat, both in attack and defence.

As well as their destructive power, UAVs as airborne observation platforms significantly enhance situational awareness and the creation of a common operating picture. They can also be a crucial aid by acting as a relay point, connecting tactical units with the command post. With hybrid connectivity, drones or other assets can move seamlessly between networks, picking and choosing bearers of opportunity based on any range of preset criteria.

There are plenty of use cases where military drones will play a crucial role in the future, including swarms of drones or other distributed systems. However, their capabilities will only be fully realised with the robust connectivity that true hybrid alone can guarantee.

Now transpose this into the civil sector, where the power of heterogenous networks are fully harnessed and the possibilities are endless to transform the ability of UAV to comprehensively address tasks across all industries, and to do so safely and efficiently for the first time – and potentially moreover at less cost. ●

TRISTAN WOOD is CEO and founder of Livewire Digital.

The market opportunities are seemingly unlimited for the adoption of true hybrid UAS

MESA 2.0 Advanced WiFi Detection Just Got Better!

Detect, analyze and locate WiFi devices.

New Firmware Update Delivers New Capability.

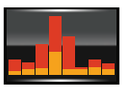
MESA® 2.0

Portable Spectrum Analyzer

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

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

Spectrum View



SmartBars™ (Patented)

Mobile Bands

WiFi

Bluetooth

MESA® 2.0 hand-held Spectrum Analyzer

FOR MORE INFORMATION CONTACT:

International Procurement Services (Overseas) Ltd

118 Piccadilly London W1J7NW

Phone: +44 (0)207 258 3771

Email: sales@intpro.co.uk

FRONTIER PITTS

PROTECTING YOUR WORLD

WWW.FRONTIERPITTS.COM +44 (0) 1293 422800

GATES » BARRIERS » BLOCKERS » BOLLARDS » PEDESTRIAN

HVM

«HOSTILE VEHICLE MITIGATION»

LPS1175 - FORCED ENTRY

Frontier Pitts, Crompton House, Crompton Way, Manor Royal, Crawley, RH10 9QZ

LOOK TO THE FUTURE

David Tuddenham *reveals how AI is being used for security tracking, resulting in a step change in capability*

We are moving ever closer to an era where all our movements are tracked by cameras that can analyse behaviours and predict potential threats. This isn't a dystopian plot, but a reality shaped by the advancements in artificial intelligence (AI) and its integration into tracking systems. And, while this technology is likely to enhance security, it also raises critical questions about the potential for misuse and the level of decision-making autonomy that can be introduced without adequate controls.

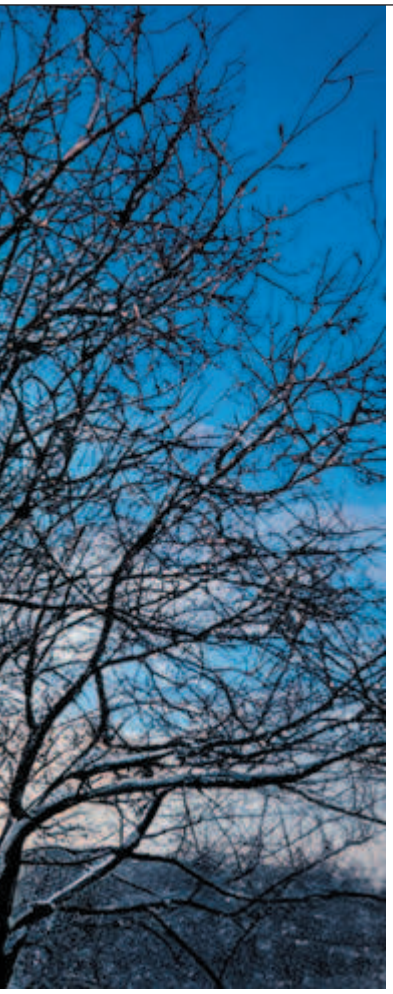
How do we ensure that these powerful tools are used in a way that delivers a step change in capability, while providing the level of real time controls required to prevent unintended consequences? In the defence sector, 'traditional' methods of targeting and tracking no longer meet the demands of evolving threats to global security. The emergence of agile, cost-effective and capable counter unmanned aerial vehicle (C-UAV) technology has accelerated changes in the defence industry and, when used by hostile actors in complex operational environments, state of the art applications can offer their operators a tactical advantage and pose a major security threat.

Overcoming this challenge requires advanced persistent surveillance that can maintain effective detection and identification with a low operator burden. This has been one of the drivers behind a rethink over how surveillance should be conducted – and this is where AI comes in.

AI can be programmed to sift through historical data as well current intelligence to predict enemy movements and strategies before they happen, allowing operators to anticipate future threats and start planning their countermeasures pre-emptively.

Advanced video tracking systems can follow targets over long periods, even in cluttered environments. This is crucial for tracking enemy movements, vehicles or drones.

Picture credit: Chess Dynamics



DEFT can track a variety of targets, from multi-rotor and fixed-wing drones to naval vessels and land vehicles

Further, AI systems can process sensor data to identify and classify targets more accurately than human operators. This reduces the risk of friendly fire and increases the precision of military operations.

AI video tracking enhances border security by monitoring and detecting unauthorised crossings. It can track individuals or groups and alert security personnel to potential breaches. And, in search and rescue operations, video tracking helps locate and follow individuals in distress, even in challenging conditions like dense forests or built-up urban areas.

AI video tracking is extensively used in intelligence, surveillance and reconnaissance (ISR) operations. It has the capability to monitor significant expanses of terrain, identify potential threats – whether on land, at sea or in the air – and provide real-time situational awareness to operators.

Drones and other unmanned systems use video tracking for navigation, target acquisition, and surveillance. AI also powers autonomous drones that can perform reconnaissance missions. These systems can navigate complex environments and make decisions based on real-time data.

AI-powered drones and satellites can monitor huge areas autonomously, identifying and tracking potential threats and provide footage in real-time. They can analyse their own video feeds to detect unusual activities or movements and can process vast amounts of data from various sensors and cameras to identify potential threats and monitor activities in real-time.

AI can also be used in autonomous ground vehicles for reconnaissance missions, reducing the risk to human soldiers. These vehicles can move through hostile terrains and gather intelligence without direct human control.

The ethics of AI security tracking are complex and multifaceted, but some key concerns are bias and fairness. For example, AI facial recognition has led to false arrests of civilians after misidentifying individuals; and surveillance systems have been found to exhibit biases, which can lead to disproportionate targeting and surveillance of minority communities.

Jeena Joseph, writing in the journal *AI & Society* in August 2024, says: "AI systems do not merely reflect the biases of their developers; they actively shape our behaviours and perceptions in nuanced and often deleterious ways. For instance, consider the application of AI in law enforcement, where predictive policing algorithms identify potential crime hotspots and optimise the allocation of officers. At first glance, this approach appears pragmatic and data driven. However, these systems frequently exacerbate existing biases, resulting in an increased police presence in already heavily monitored areas... The ramifications of biased AI extend well beyond mere data inaccuracies; they impact lives and societal structures, perpetuating systemic inequality and injustice."

To work towards more equitable and reliable AI tracking, strategies for operating systems include incorporating data from various ethnicities, genders, ages and other relevant categories; focusing on detecting behaviours rather than identifying individuals; and establishing robust governance frameworks to oversee the development and deployment of AI systems.

To achieve these goals, systems should be monitored continuously by human operators and updated to address any emerging biases. This involves regular testing and validation against fresh data to ensure ongoing fairness and accuracy. Having diverse teams involved in the design and development of AI systems can help identify and mitigate biases from different perspectives.

Deep learning is a subset of machine learning that uses artificial neural networks to simulate the decision-making processes of the human brain. Deep learning can address AI bias through several key strategies.

Techniques like data augmentation can help create a more balanced dataset by artificially generating new data points. This can help mitigate biases that arise from imbalanced datasets. Regularly monitoring AI system performance and updating it with new data can help maintain fairness and accuracy over time. This involves ongoing validation and testing to ensure the model adapts to new patterns without introducing bias.

One of the most common applications of deep learning for video analysis is object detection and tracking. This involves detecting and tracking specific objects in a video recognition sequence. Popular techniques include the use of a convolutional neural network (known as a ConvNet or CNN) to learn complex patterns from data.

THREATS CONSTANTLY EVOLVE AND SO MUST THE TECHNOLOGY TO COUNTER THEM

Such deep learning models are used in software for analysing video and detecting and tracking objects for trained classes, such as vehicles, ships, drones, or people, in real-time. More advanced video analytics software provides functionality for object counting and rule-based analysis, for example people-counting in areas with large crowds.

Another typical application of deep learning for video analysis is action recognition. This involves recognising specific actions in a video sequence or real-time video streams. Deep learning models can be trained to classify actions performed in different contexts or environments. More advanced methods apply video recognition or understanding, pose estimation, emotion analysis or face recognition to analyse and understand the context of video data.

Considering these innovations, video recognition and motion detection analysis are very popular for detecting activities in a scene by analysing a series of video frames.

Techniques for video motion detection or progress analysis include frame referencing or pixel matching to detect horizontal and vertical changes between a set of images or video frames.

Video tracking is now often preferred to alternatives such as infrared, due to its greater ability to classify its targets, but this has led to a greater expectation of video tracking to advance and meet the pressing demands of warfare and, considering the challenges discussed here regarding ethics and bias in AI, there is a need for a more 'hybrid' AI solution, which enhances the abilities of human operators and reduces the burden, without taking over from them completely.

In response, state of the art Deep Embedded Feature Tracking (DEFT) technology is already being developed and it is proving to be holding up effectively against new and evolving security threats.

Deep Embedded Feature Tracking (DEFT) is an AI-powered advanced real-time video tracking capability designed to provide accurate and robust tracking in complex situations. Chess Dynamics, for example, has installed DEFT on its newest CHARM Video Target Trackers, and the system uses its deep learning approach to optimise the identification and tracking of a moving target.

The technology has the potential to revolutionise surveillance, enabling reliable tracking of targets that are becoming increasingly difficult to follow. Threats can aggressively change appearance, helped by background clutter and other fast-moving and agile objects in the environment, but AI powered deep learning-based algorithms allow a comprehensive model to be made of the tracked target, enabling the system to accurately locate dynamic targets and reliably re-acquire them following periods of occlusion.

AI SYSTEMS CAN IDENTIFY AND CLASSIFY TARGETS MORE ACCURATELY THAN HUMAN OPERATORS

DEFT can track a variety of targets, from multi-rotor and fixed-wing drones to naval vessels and land vehicles and can do so with efficient autonomy. This means it can identify threats and enable automated acquisition and reacquisition of targets, while minimising false alerts. This reduces the burden on the operator to stare at a screen for long periods of time to detect and identify adversaries. The rapid and accurate identification of small, fast-moving threats is key to effective threat mitigation and protection of critical assets.

The technology creates comprehensive models of the target, allowing for continuous accurate tracking after occasional occlusion, for example. It provides for improved surveillance of difficult targets – an issue not unknown in C-UAS circles – in which traditional algorithms often struggle.

These models are continuously fine-tuned to enhance human user understanding of the target, resulting in precise long-term, robust tracking performance. The technology enhances the AI-driven target detection and tracking capability and integrates with neural network-based object detection and classification of targets.

As discussed, the increased proliferation of stealthy drones and more flexibly deployed forces has posed an unprecedented threat to security and privacy. These agile and hard-to-detect devices capitalise on cluttered environments to evade traditional surveillance methods, highlighting the urgent need for innovative technologies to counteract them. DEFT has been developed in response to this growing issue.

Threats constantly evolve and so must the technology to counter them, so our focus therefore must remain on continual enhancements that stay one step ahead of this changing threat profile.

Chess Dynamics is incorporating DEFT into smaller electro-optic systems and products while maintaining the high tracking performance of the technology. This will mean it can be integrated into autonomous platforms or installed within a camera to optimise performance of the automated video tracking and surveillance capabilities within a single device.

The multi target tracking ability of DEFT enables the system to measure the similarity between different detections and tracks to avoid confusion when there are multiple threats of the same kind in a small vicinity. Enabling effective multi target tracking on a device the size of a soda can is certainly a challenge, but such an enhancement is a key focus for defence leaders, and we are confident of further advancements in capability as we continue to invest in this product and technology.

There is huge potential for further innovation in artificial intelligence, and technology continues to develop exponentially to counter threats that seem to be adapting just as quickly.

Chess has already played a hugely significant role in this development and will continue to do so as we use AI to support and optimise operator and system performance ●

David Tuddenham is Group Managing Director of Chess Dynamics.

More advanced methods apply video recognition or understanding, pose estimation, emotion analysis or face recognition to analyse and understand the context of video data

Picture credit: Chess Dynamics

THE QUEEN'S AWARDS FOR ENTERPRISE: INNOVATION 2020

eskan™

OFFER!

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

Increasing security. Reducing risk.

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

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

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

ELECTRONIC COUNTERMEASURES

IPS EQUIPMENT & SWEEP TEAM SERVICES

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

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

Looking for a

VIDEO POLE CAMERA
2.0 INSPECTION TOOL

EDD-24T NON LINEAR
JUNCTION DETECTOR (HANDHELD)

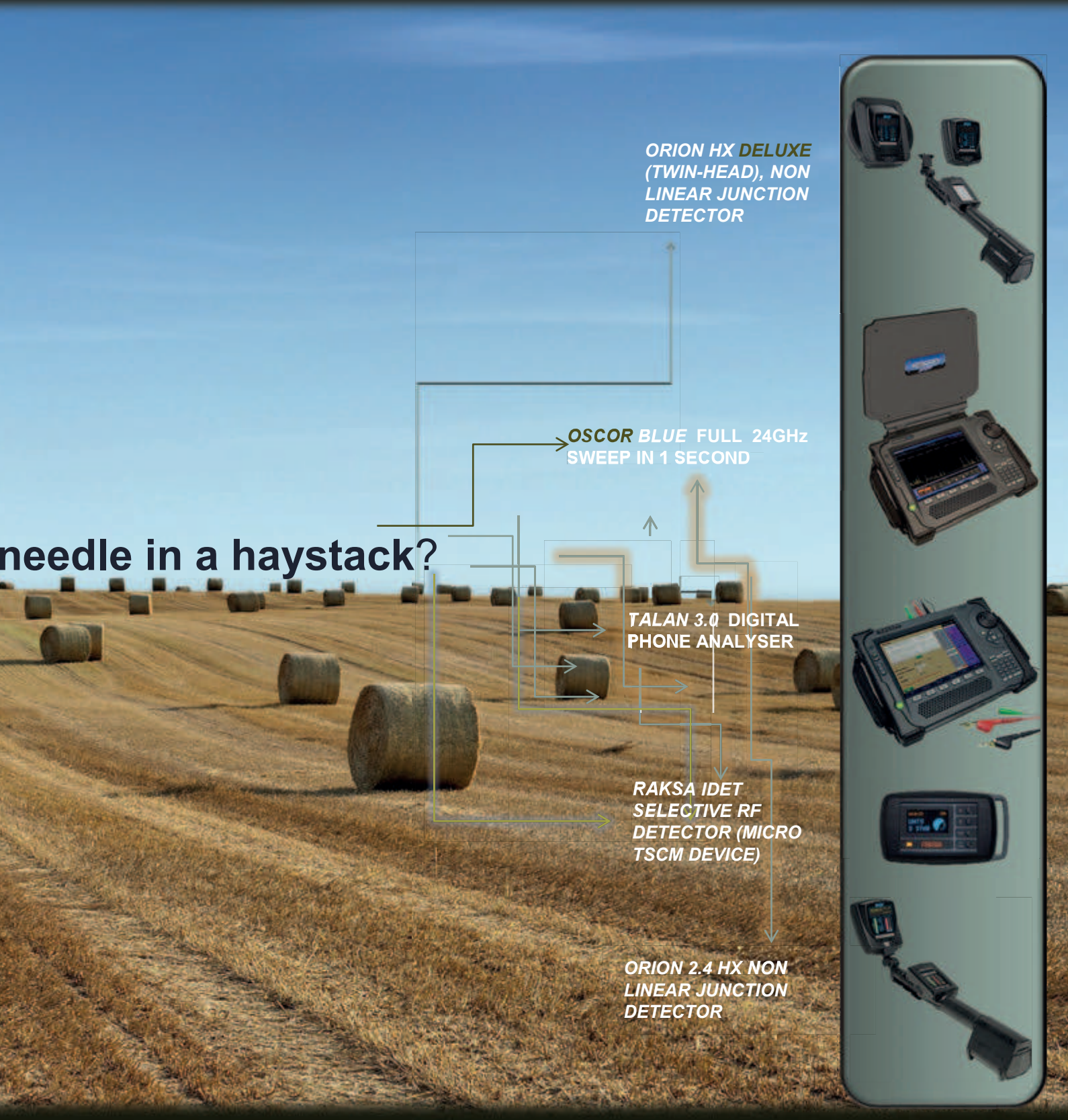
TSCM TRAINING
COURSES &
CERTIFICATION
UK/US/GLOBAL

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

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

Rapid Quote:

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



TSCM Equipment supply, training and de-bugging services

The preferred choice of Government & Law Enforcement Agencies worldwide.

Web: www.intpro.com

KNOWLEDGE IS POWER

Aaron Rosenmund *highlights the six most dangerous new threats security teams need to know about*

The rise of AI presents both extraordinary opportunities and intimidating challenges in cyber security. While AI can easily identify and exploit vulnerabilities, deploying it without robust security measures introduces significant risks.

As the technology evolves, many organisations prioritise AI innovation at the expense of security, leaving their systems vulnerable. This underscores the need for established security frameworks and ongoing education about the dynamic risks AI presents.

Organisations can effectively mitigate risks and safeguard operations by prioritising AI security and supporting cyber security professionals. Each year, experts at the RSA Conference discussed six of the largest new attacks and threats – and what actionable steps businesses can take to address them.

WEAKNESSES IN CODE

If you give GPT-4 a list of real-world vulnerabilities, it can exploit 87 percent of them autonomously. That means that hackers can use a publicly disclosed list to target companies. While this is the approach human hackers have historically taken – finding gaps in defences

Despite their best efforts, humans remain the weakest link in the security stack

Aaron Rosenmund
is Senior Director of Content Security and Curriculum at Pluralsight.

– the speed and ease at which an AI can do it changes the game. Applications become highly vulnerable if unpatched, with zero-day (publicly known, unpatched vulnerabilities) and one-day attacks (patched, but not applied) posing significant threats.

To effectively prevent AI-driven attacks, security teams must adopt a proactive approach by leveraging AI for defence – fighting fire with fire. Since human teams can't patch vulnerabilities as fast as malicious AI can detect them, ensuring businesses are fully equipped with AI capabilities is crucial. This requires security teams to be well versed in AI, while automating purple testing (where the role of both the attacker and defender are simulated) can create a continuous feedback loop of simulated attacks and responsive remediation strategies.

GENAI EXPLOITED AND WEAPONISED

"We need to have GenAI in our company" is a common phrase heard in businesses since the explosion of the technology. While innovations are moving quickly into products as businesses look to capitalise on new tech, they also open a significant entry point for attackers to exploit and weaponise against the business.

A survey by IBM found that 70 percent of C-suite respondents believe that, when it comes to AI, innovation takes precedence over security. And while 82 percent said: "secure and trustworthy AI is essential to the success of their business," only 24 percent of them said they're actually securing their GenAI products.

The risks of an insecure large language model (LLM) are significant and far-reaching. For example, attackers can exploit prompt injection to manipulate AI into revealing sensitive data or performing unauthorised actions, while training data poisoning can corrupt AI during its learning phase, leading to harmful outcomes like backdoor attacks. Looking ahead, there are concerns that attackers may co-opt AI systems to launch coordinated attacks, making it crucial to ensure newly branded AI is not moonlighting as a criminal.

To protect LLMs, start by adopting established frameworks like Google's Secure AI framework (SAIF) and Nist's AI Risk Management Framework. Conduct comprehensive modelling and data validation while enforcing the principle of least privilege.

SOPHISTICATED SPEAR PHISHING

In an era where a voice can be cloned from just a three-second sample of someone talking and verifying their identity, things will get very tough, very fast. We can't rely on companies to AI-generate protective content, as even subtle telltale signs can be easily erased.

This poses a significant challenge for remote identity verification, particularly in distributed workforces. To combat this, focus on strategies to establish and reestablish identities for customers and employees. Leverage AI to detect unusual behaviour, but remember that despite their efforts, humans remain the weakest link in the security stack.

SEXTORTION OF EMPLOYEES

Sextortion is an uncomfortable yet crucial topic to address in the age of GenAI. While the concept isn't new – like those emails threatening to expose what's on someone's hard drive – AI advancements have made it a growing threat, and anyone can be a target. Unfortunately, it usually doesn't end when payment is made. We're seeing attackers using an 'alternate' form of payment, such as giving access to a network, installing malware or any way that compromises a system.

Executives are most at risk, so implementing an executive protection program is vital. Educate the entire company on what sextortion is and what an attack might look like. It's uncomfortable, but these attacks thrive in an environment of ignorance.

THE SPEED AND EASE AT WHICH AN AI CAN FIND GAPS IN DEFENCES CHANGES THE GAME

MFA INTERCEPTION

Push notifications from Multi-Factor Authenticfication are becoming a nuisance, leading many users to click through them without giving them much thought. This makes them vulnerable to "attacker-in-the-middle" attacks, where attackers trick users into logging into a fake site. Once logged in, attackers capture the user's credentials and MFA code to access the real account.

While MFA is still better than nothing, it's not a silver bullet. To enhance security, users are required to enter a code from the login screen, as attackers won't have access to it. Add context to push notifications, such as sign-in location and tighten authentication measures for unusual login times.

LACK OF TRAINED CYBER PROFESSIONALS

The shortage of cyber security professionals is a well-known issue, with 71 percent of organisations having unfilled cyber security positions. This shortage leaves security teams understaffed and burned out, a problem exacerbated by the rise of AI.

Cyber security professionals must be more alert than ever, given the AI tools threat actors now have. However, only 12 percent have significant experience working with AI.

Focussing on upskilling your cyber security team in AI-based defence strategies and leveraging AI to reduce the burden of their job can be beneficial. Tasks like inbound message filtering, summarising incident reports, process automation and filtering bug bounty challenges can all be automated. Supporting employees with resources to stay informed on the way threat actors use AI and upskill on knowledge gaps will make for a more engaged and better-equipped team ready to defend against criminals.

In the face of significant cyber security threats, taking proactive and tangible steps to safeguard employees and the organisation is crucial. Addressing issues like the shortage of cyber security professionals, AI-driven attacks and sextortion requires a deliberate approach – from upskilling your team in AI defence to creating a supportive work environment. By staying vigilant and proactive, businesses can effectively minimise risks and enhance their overall security posture ●

YOU'VE BEEN 'AD

Grant Simmons *advises best practices for ad fraud protection*

Ad fraudsters operate by deceiving digital advertising networks for financial gain. This usually involves manipulating performance metrics through deceptive tactics such as fake impressions, clicks and conversions. Not only does this hamper the effectiveness of campaigns, it also drains ad budgets by diverting money towards fraudulent activities instead of reaching intended audiences.

Research indicates that 22 percent of all digital advertising spend in 2023 was attributed to fraud, amounting to $84-billion. This figure is anticipated to rise to $172-billion by 2028. The shifty and intricate nature of ad fraud makes it difficult to detect and can allow deceptive behaviour to go unnoticed for long periods of time, causing significant financial ruins. A high-profile example of this is multinational tech company Uber, which fell victim to ad fraud and was forced to process over 58-billion records to uncover false marketing campaign results. The organisation then had to find a way to recover millions in damages. To address these risks and prevent similar incidents, businesses should consider the importance of adopting proactive and comprehensive strategies among advertisers.

FRAUD BLOCKLISTING CAN BE USED TO PROTECT CAMPAIGNS ACROSS DIFFERENT APPS

First and foremost, companies need to understand the various forms that ad fraud can take. Domain spoofing, for instance, entails disguising poor-quality or fake websites as premium ones to trick advertisers into bidding on their inventory. Ad injection takes place when unsolicited or unauthorised ads are incorporated into genuine websites using browser extensions, ransomware and network proxies. Click fraud happens when false clicks are produced on an ad with the help of bots or malware, while impression fraud involves inflating the number of times an ad is displayed through bots, illegitimate sites and hidden pixels.

Dealing with each type of ad fraud requires a certain degree of finesse. Advertisers need to harness state-of-the-art detection technologies that can quickly spot and inhibit fraudulent conduct. For example, fraud blocklisting can be used to protect campaigns across different apps. This strategy involves creating and maintaining a comprehensive list of known fraudulent entities, such as suspicious IP addresses, domains or app IDs. Any traffic that goes against the installed blocklist is regularly flagged and excluded from being counted as a valid conversion. This helps advertisers to swiftly react to new fraud patterns and ensure that only genuine interactions are considered, which keeps the accuracy of campaign performance data intact.

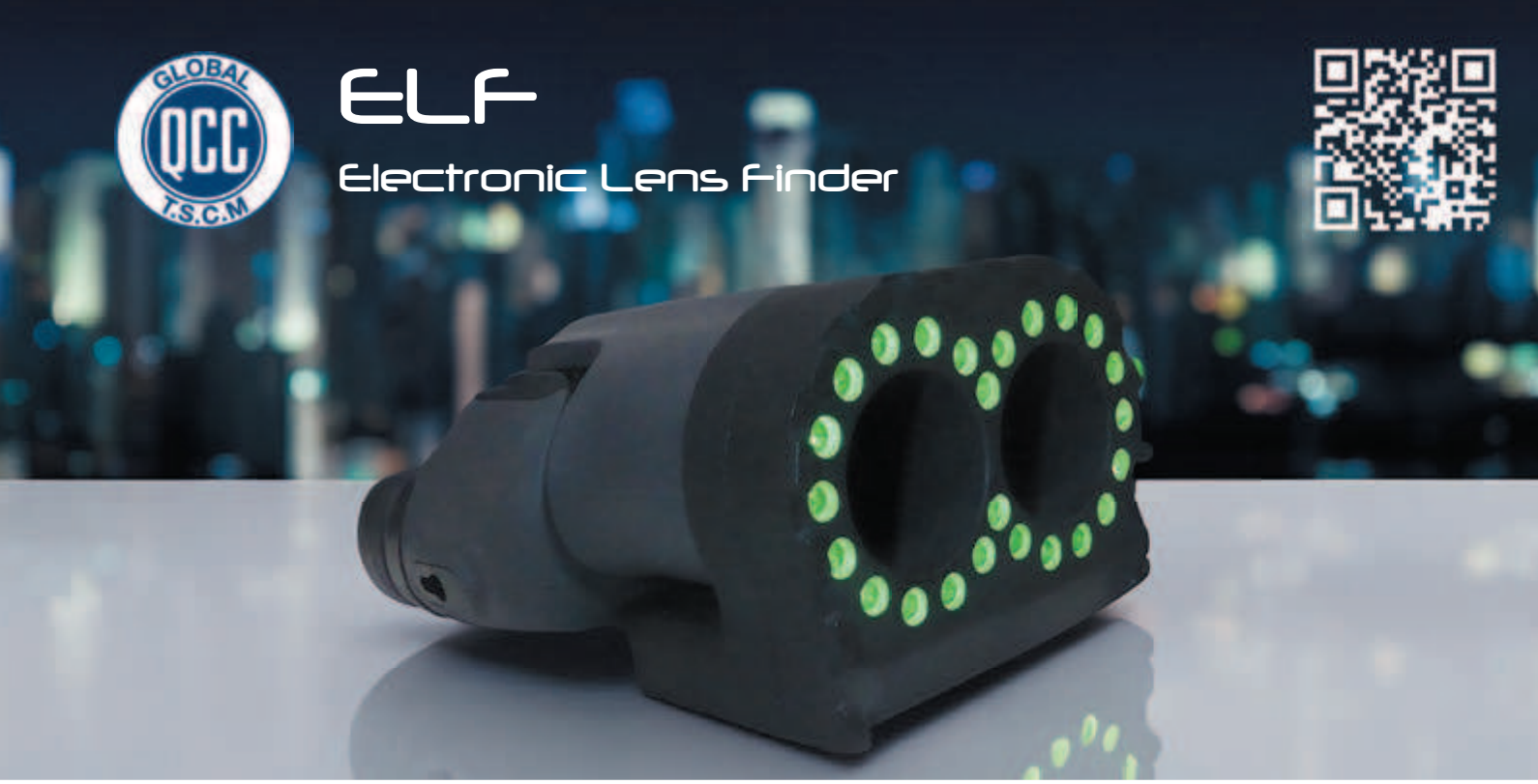
Setting guidelines for campaign traffic also plays an important role in safeguarding the integrity of advertising initiatives. Marketers can define criteria based on factors such as device type, location and campaign dates to ensure that traffic aligns with their standards. This helps to prevent any discrepancies or irregularities from being overlooked.

Tackling risks such as SDK spoofing, where false data is transmitted to mimic user interaction, is another highly recommended strategy. Detecting and preventing deceptive data in this context allows advertisers to avoid making payments for conversions, thereby guaranteeing that their marketing budget is allocated towards authentic user engagement.

Advertising fraud is a surprisingly complex issue that calls for equally complex solutions, while the cost of mobile ad fraud is rising exponentially each year and fraudsters aren't showing any signs of letting up in their attempts to steal from ad budgets. The growing sophistication of ad fraud schemes means relying solely on basic detection methods is no longer sufficient to combat increasing threats. In order to shield campaign successes and reserve budgets, advertisers must employ a comprehensive strategy that combines technology, transparency and continuous oversight. When following practices such as blocklisting, configuring advanced traffic rules and accurately detecting spoofed data, advertisers can considerably reduce the risk of ad fraud and get the most out of their marketing efforts ●

Research indicates that 22 percent of all digital advertising spend last year was attributed to fraud

Grant Simmons is VP at Kochava Foundry.



ELF

Electronic Lens Finder

Electronic Lens Finder & Delivery Set

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

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

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

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

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

Picture credit: AdobeStock

INSIDER THREATS

Miguel Clarke *underlines the potential damage that can be caused to your organisation's cyber security by a 'wild card'*

As cyber attacks escalate globally, organisations face growing challenges not just from external threats, but also from insider risks. With insider threat incidents surging by 44 percent in the past two years and the financial toll reaching a staggering $15.38-million per breach, the need for proactive security measures is greater than ever. This article discusses the critical role of leadership, employee morale and cross-departmental collaboration in combating these unpredictable, yet damaging, internal risks.

With the number of cyber attacks at an all-time high, causing billions of dollars in financial losses globally, organisations are facing unprecedented risks. From small businesses to large multinational corporations, the rise in sophisticated cyber threats has made it clear that no organisation is immune to the threat of data breaches, consequential reputational damage and not to mention costly legal ramifications.

However, it is not just external actors that need to be defended against. One of the most unpredictable and damaging cyber security risks organisations face today is insider threats. Originating from individuals who already have access to an entity's systems and data, insider threats can be inherently more challenging to detect and mitigate. These threats may stem from current or former employees, contractors or business partners who have, or have had, authorised access to the organisation's systems, networks and sensitive data.

Poor cyber security hygiene significantly amplifies the potential for destruction to an organisation

Recently published data provides real insight into the scale of the problem faced. In the last two years alone, there has been a 44 percent surge in insider threat incidents, with the average cost of each incident reaching an eye-watering $15.38-million. More alarmingly, between 2019 and 2024, the number of organisations reporting insider incidents has grown from 66 percent to 76 percent – that's nearly three-quarters of all organisations grappling with this issue. Insider threats generally fall into three distinct categories.

The first is malicious insiders who intentionally misuse their access for personal gain or to inflict harm on the organisation. These are often disgruntled employees or individuals who may be seeking financial gain, revenge or are working in collusion with external actors.

The second is negligent insiders, those who inadvertently compromise security through carelessness or lack of awareness. External actors, such as hackers, can exploit weak security practices or vulnerabilities to turn outsiders into insiders. Poor cyber security hygiene significantly amplifies the potential for destruction, with organisations that maintain strong security practices experiencing 35 times fewer destructive ransomware events.

The final type of insider threat is compromised insiders: individuals who have been coerced or manipulated by external actors into actions that jeopardise the organisation that employs them. This can occur through methods such as phishing, blackmail or social engineering – where attackers take advantage of vulnerable individuals to carry out malicious activities on their behalf.

It is important to remember that when it comes to insider threats and cyber security in general, there is no stereotypical perpetrator. As such, detecting insider threats is a real challenge, but there are several factors that organisations should consider and monitor closely.

The first is the length of employment. Notably, 38 percent of employees involved in dishonest behaviour have been with their organisation for less than a year, suggesting a higher risk-taking propensity early in employment. Taking this one step further, 75 percent of those recorded for unlawful data acquisition or disclosure have been employed for under five years.

That's not to say that longer-term employees are not exempt from risk. A striking 80 percent of those involved in bribery cases have been with their organisation for over ten years. This could be triggered by personal grievances, a sudden change in financial or personal circumstances or simply disillusionment with the company direction.

Vigilance is key when it comes to insider threats, and there are many 'red flags' that may give an indication of malicious intent. The first is unauthorised or suspicious data access and handling; this includes accessing sensitive information or systems without a legitimate need to know. Downloading, copying or transferring large amounts of data, attempting to bypass security controls or access restrictions and the unauthorised use of removable media or external storage devices should also be considered unusual and a potential security risk.

The next category is information technology misuse, such as installing unauthorised software, exhibiting unusual network activity, excessively using personal email or cloud storage for work, or experiencing frequent password resets or account lockouts.

Other categories include disgruntled or disruptive behaviour from staff, suspicious communications – perhaps with foreign entities or competitors, the use of encrypted or anonymous communication channels or even attempts to circumvent communication monitoring or surveillance systems.

Personal or financial issues are also something to look out for. Sudden or significant changes in lifestyle or spending habits, involvement in illegal activities or substance abuse, and financial difficulties such as debt or gambling problems can all increase an individual's risk profile.

SOMETHING THAT MUSTN'T BE OVERLOOKED IN THREAT PREVENTION IS EMPLOYEE MORALE

So, in addition to remaining vigilant, how can organisations successfully protect themselves against insider threats? In every insider threat case, there is a combination of network activity and employee behaviour. In other words, the malicious activity crosses both physical and electronic modalities.

Successful insider threat programmes require a multi-disciplinary team (MDT) approach involving individuals from across the organisation, responsible for physical security, cyber security, operational technology, information technology, HR and legal.

Monthly meetings of the MDT play a pivotal role in protecting organisations from insider threats, developing a strategy to support early threat detection, enable effective mitigation and ensure an appropriate response to anomalous behaviour.

Collaboration between HR and IT is particularly critical here because it combines the strengths of both departments to create a comprehensive approach to security. By combining their expertise and resources, HR and IT can create a powerful synergy that significantly reduces insider risk. The HR department has deep insights into employee behaviour, motivations and potential vulnerabilities. This knowledge can help IT security teams identify early warning signs of potential insider threats and tailor security measures accordingly. In addition, HR policies and practices can significantly influence the likelihood of insider threats. By working together, HR and IT can develop policies and procedures that foster a culture of security, promote ethical behaviour and discourage risky actions.

The employee lifecycle – starting from hiring practices to the working environment, training programmes and leadership quality – can significantly influence the likelihood of insider threats. Organisations should ask themselves: are we hiring the right employees? Are we providing adequate training? Does the organisation's culture encourage ethical behaviour or does it create an environment where malicious actions thrive?

Cultivating a culture of security and instilling a sense of responsibility and awareness among employees is crucial in the fight against insider

threats. This should be complemented by a strong governance and risk management programme that establishes clear guidelines and procedures about expected behaviours, both online and in the workplace. A comprehensive employee manual coupled with robust employee onboarding and offboarding processes will also help to shape an informed and vigilant workforce.

THE RISE IN CYBER THREATS SHOWS THAT NO ORGANISATION IS IMMUNE FROM BREACHES

Something that mustn't be overlooked when it comes to threat prevention is employee morale and effective leadership. Insider threats are largely 'people problems'. That is, most companies do not hire 'bad actors', but over time relationships can sour due to unresolved conflicts, poor communication, or a lack of support, which can cause disengagement, resentment or even malicious intent.

Having interviewed many insiders during my time in the FBI, a common complaint was always about a leader's behaviour or how they were treated. While this does not justify unlawful behaviour, it is a reminder that good leadership always matters. Transformational leadership, which inspires and motivates employees while fostering a positive and supportive work environment, is probably the most powerful tool one can employ to safeguard the organisation and its data. Employee well-being programmes contribute not only to the overall welfare of the workforce, but also to the prevention of potential insider threats by addressing underlying issues proactively.

Employee training and education are also key factors in preventing insider threats, and organisations should implement regular, engaging cyber security training sessions for staff to stay abreast of the evolving technological landscape. Organisations must align security training with company culture, set clear expectations for both leaders and employees, and conduct regular training sessions to reinforce the importance of cyber security. Encouraging preferred employee behaviours and setting a positive tone from the top can go a long way in preventing insider threats.

The implementation of User Activity Monitoring systems (UAM), which continuously assess behaviours, is also hugely beneficial, enabling the early detection of employees with heightened risk factors. Similarly, Entity Behaviour Analytics (UEBA) provides insight into anomalous activities and helps in understanding data movement, which is another key step. By gaining insight into how data moves within an organisation, who accesses it, and for what purpose, potential risk areas can be identified. Identity Access Management (IAM) integration is also important, linking data flow analysis with identity and access management strategies to ensure appropriate access control and minimise the risk of data exposure.

Ultimately, the purpose of every information security programme is to maintain the confidentiality, integrity, and availability of said information. Insider threats are a formidable challenge to this and for organisations to mitigate, but with the right strategies in place and by adopting a proactive, multifaceted approach, the risk and impact of these 'wild card' threats can be reduced substantially ●

Miguel Clarke is GRC and Cyber Security Evangelist at Armour.

Disgruntled employees can misuse their access for personal gain or to inflict harm on the organisation

Milipol
QATAR

Milipol Qatar 2024

وزارة الداخليـــــــة
Ministry of Interior
State of Qatar • دولـــة قطـــر

@milipolqatar
www.milipolqatar.com

BUILT TO LAST?

Rob Mather *outlines how renewed defence demand is stretching manufacturers and offers four key operational trigger points to achieve high-performance manufacturing*

Defence manufacturers are now facing a rebound in orders, with a reversal in downscaling and defence budgets increasing. But for increased demand to be met, there are four key focus points where digital tools can help defence manufacturers accelerate production – from AI-enabled anomaly detection, to unifying data platforms to bolster production and automating workflows, to keeping on the right side of regulations.

Surge in demand is straining defence manufacturers, but digital transformation can be a game-changer. Deloitte industry analysis underscores the urgent need for digital transformation within the defence ecosystem to address the challenges posed by escalating demand. The report highlighted the potential of modernising and integrating processes to enhance production efficiency, reduce cycle times and elevate product quality.

To achieve this, defence organisations must adopt a holistic approach to software and information management, breaking down silos and creating a unified system that connects the shop floor, right up to the executive suite. By integrating data from various sources, including Manufacturing Execution Systems (MES), Enterprise Asset Management (EAM), Customer Relationship Management (CRM) and Enterprise Resource Planning (ERP) systems, companies can establish a single source of truth to inform decision-making and streamline operations. Here are the top four areas of development where digital approaches are laying the foundations for high-performance defence manufacturing.

ARTIFICIAL INTELLIGENCE

To help deal with surges in demand, defence manufacturers have reversed inventory strategies from lean and just-in-time principles to over-stocking parts to ensure inventory buffer. Despite reducing production risks, financial risks have been increased due to cost of purchase, storage and tracking of materials and parts.

Key decision makers state they're facing a lack of skilled manufacturers and mechanics, such as those required for this MOD submarine factory

Rob Mather is Vice President, Aerospace and Defence Industries, at IFS.

To better balance risk, defence manufacturers can look to integrate operations and take advantage of demand-driven material requirements planning (DDMRP). This will ensure inventory levels match demand levels and supply chain variability. By looking at actual usage data, DDMRP can determine if the stock level for a part is sufficient to cover demand, making defence manufacturers more sensitive to supply chain disruptions, variations in demand and production downtime.

The use of AI within defence forces and manufacturers is on the rise. With the US Department of Defence budgeting $1.8-billion for AI applications and stating that AI applications will be used to help defence forces and organisations recognise patterns, learn from experience, make predictions and generate recommendations.

AI can help further de-risk production and financial issues. Manufacturers should look to combine anomaly detection and pattern recognition with real-time data correlation. The combination of AI anomaly detection and DDMRP can radically increase the speed and accuracy of problem detection throughout all aspects of the organisation and action potential chokepoints before they escalate into complex and costly problems.

INTEGRATING PLANNING AND PRODUCTION DATA

Defence manufacturing projects by their very nature are complex, with multiple production lines working to intricate assembly requirements. Project management, already a major challenge for defence manufacturers, is further exacerbated by this current ERP management software causing a disconnect throughout operations, alongside a lack of a skilled workforce readily available to defence manufacturers. Recent reports from Guidant Global highlight the workforce issues facing the UK defence sector, with key decision makers stating they're already facing a lack of skilled manufacturers and mechanics.

Implementing integrated project management software will allow defence manufacturers to align their planning through their operations to optimise their production and increase efficiency. The use of IoT technologies such as integrated project management software allows for data to flow in real time so people, systems, and capabilities can be leveraged in every aspect of their operations.

The increased visibility brought by integrated project management software can allow for manufacturing teams to react quickly to new priorities. Ensuring workers and machinery are coordinated to maximise efficiency and capacity and avoid time, money and resources being wasted.

NEW STANDARDS FOR WORKFLOW AUTOMATION

One of the biggest challenges defence manufacturers are struggling to overcome due to rising demand levels is reducing lead times. In August 2023 the delivery time for production materials reached 87 days. Despite being reduced by 13 days compared with 2022, the average lead time has yet to recover to pre-pandemic levels. Integrated workflows can help defence manufacturers reduce this with its ability to provide all relevant parties with data so that people, machines and assets' time and skills are all optimised. A key part of digital transformation within the defence manufacturing industry is to move away from siloed data to real-time data that flows from the shop floor to the top floor of defence manufacturers. Powerful Manufacturing Execution Systems (MES) with integrated workflow engines will allow for data to flow from end-to-end, so every worker has operational visibility of what's happening and what needs prioritising.

Utilising powerful MES with integrated workflow engines brings far more benefits to defence manufacturers compared with typical ERP systems with data aggregators or business intelligence reports. Integrated workflow systems are accessible for all relevant parties – providing vital insights into ongoing work everywhere.

ONE OF THE BIGGEST CHALLENGES DEFENCE MANUFACTURERS FACE IS REDUCING LEAD TIMES

BEWARE REGULATIONS

Defence manufacturers operate in an industry defined by regulatory requirements whether it's supply chain, cyber security, sustainability or employment – they all have their own regulations to comply with. This requires defence manufacturers to have fully traceable operations and processes which generate information that is readily available for regulatory reporting.

As regulations get stricter, current disjointed systems make it hard for defence manufacturers to meet requirements, with slow data compilation and increased risk of information being inaccurate or out-of-date. A real-time, single source of the truth is really needed.

This means manufacturing management platforms should include integrated and automated templates for mandatory government reports that are ready to use when called upon. Combining MES and ERP in one place will also help them comply with the ISA-95 standard from the International Society of Automation (ISA). This ensures they are using these standardised data models and communications to enable consistent and accurate data exchanges throughout all business systems.

To capitalise on the current surge in spending, manufacturers must view their transition to digitised operations as a strategic imperative – including the readily available tools at their disposal. Partnering with specialised technology providers can accelerate this journey by providing tailored solutions and deep industry expertise. By consolidating disparate data systems into a unified, intelligent platform, defence manufacturers can de-risk supply and demand, optimise operations, enhance decision-making, and ensure regulatory compliance. Ultimately, a robust digital foundation is essential for achieving high-performance manufacturing, mitigating risks, and sustaining long-term growth in this dynamic and, once again, growing market ●

LOG FILE PROTECTION

Simon Bain *provides an explainer on log files: what are they, why do they matter and how do we protect them?*

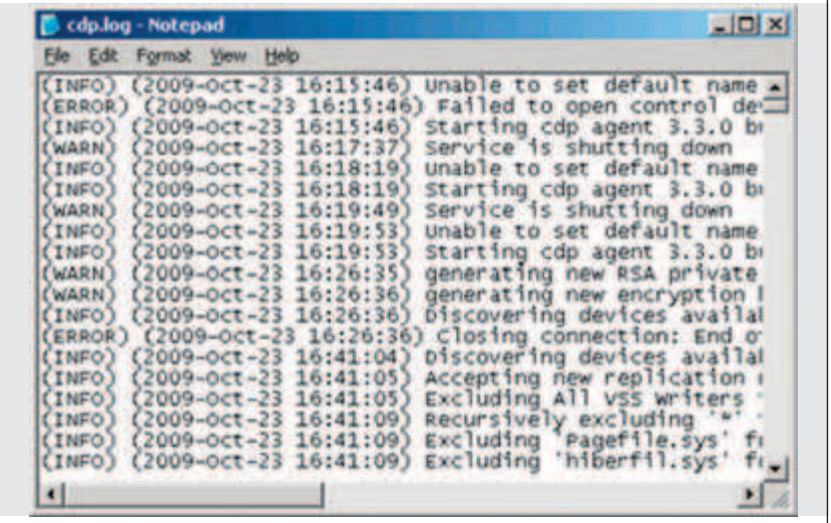
Log files come with many challenges. Firstly, they exist as enormous volumes of data. Almost everything that a user does is recorded, meaning that they quickly pile up, and not all of them are useful. Secondly, they aren't all uniform as they come in various shapes and sizes, serving various purposes. Event logs, system logs, access logs and server logs are just some of the various types that are collected and stored. This large volume of data means that processing and analysing logs for use can be both extremely time-consuming and complex.

And thirdly, you often need access to them, but you always need to protect them at the same time. According to advice from the NCSC, good logging practices provide the ability to understand, trace and react to system and security events. Cyber criminals will seek to get their hands on a company's log files in order to identify vulnerabilities, force changes, steal data and hold users to ransom. Adequately protecting them is therefore paramount. But what is a log file?

A log file is a record of actions taken on or by an application within a computer system. They are the primary data source for network observability. They usually contain information about usage patterns, activities and operations within an operating system, application, server or another device. They can also contain IP address, emails and law-protected information. Crucially, they record what is happening without knowing why it is happening. In other words, logs are not intelligent. Instead, they are simple read/write text files full of valuable information with often very little in place to protect them.

Log file monitoring and analysis increases the observability of the network, creating transparency and allowing visibility into the cloud computing environment. It can show what is happening within the system, including design malfunctions and malicious activity. This threat intelligence allows IT teams to identify where particular system improvements might be needed, can support security efforts and be used to capture the behaviours of end users. They're also useful for meeting compliance requirements and can be leveraged for audits.

The biggest risk that comes with log files is often complacency. Senior leaders often don't take the threat of attack seriously enough and protect them adequately. In reality, if hackers get access to log files, their content can be invaluable. Specifically, criminals can inject false entries, delete specific logs to erase traces or modify details like timestamps and IP addresses. They can even disable logging services to stop any activity from being recorded in order to hide that an attack has happened.



Logs can also be relatively easily exfiltrated and stolen as they're often in plaintext with no encryption to protect them. This means your data can be stolen and shared or used to exploit you. Either way, once it falls into the wrong hands it can become very costly to get it back or recover.

The first step is recognising that although log files may not look useful on the surface to the untrained eye, they almost always contain a map and keys to the inner workings of your business and should be treated as such. On the market currently, there exists specialist security software that watches for anomalous activity that might indicate an attack commencing or indicate that one is already in progress. If not acted upon fast enough, logs can also be used to clean up after the attack. It is possible to cause such a mess in the logs that visibility is lost for weeks.

Technology such as OmniIndex's LoggerBC can enable log files to remain encrypted at all times while allowing actionable AI threat intelligence from these fully encrypted log files. LoggerBC works on a native and private AI: Boudica. Boudica analyses encrypted log files to identify patterns, threats and vulnerabilities in a system and alert users to any potential threats in real-time with easy integration into Google Looker.

Powerful fully homomorphic encryption technology ensures that log files are encrypted at all times and never left vulnerable to attack. Log files are also stored in a private and secure blockchain to ensure they can't be accessed by criminals and are protected from the threat of ransomware. Protecting log files is no easy task, but can be achieved with the latest technologies. Without it, businesses remain at risk to attack, breach and exploitation ●

Almost everything a user does on a computer is recorded as a log file

Simon Bain is CEO at OmniIndex.

MCQUEEN TARGETS

LIVE FIREARMS TRAINING TARGETRY

AIM FOR THE BEST.

CIVILAIN TARGETS

MILITARY TARGETS

POLICE TARGETS

THREAT ASSESSMENT

3-D FOAM TARGETS

3-D FOAM ACCESSORIES

Hit the mark every time with

MCQUEEN TARGETS

GALASHIELS, SCOTLAND

info@mcqueentargets.com

+44 (0)1896 664269

mcqueentargets.com

INCIDENT BRIEF

Europe

1 October, Copenhagen – Denmark
Three Swedish men were arrested after hand grenades were thrown near the Israeli embassy in the capital. No one was harmed.

1 October, London – UK
A 14-year-old girl was left with potentially life-changing injuries, while a 16-year-old boy is in hospital, after a substance – believed to be acidic – was thrown at them by a male who approached them outside their school.

2 October, Stockholm – Sweden
Police confirmed the Israeli embassy was hit by bullets and launched an investigation into serious weapons offences.

16 October, Birmingham – UK
Counter-terrorism police are investigating whether Russian spies planted an incendiary device on a plane to the UK that later caught fire at a DHL warehouse.

22 October, London – UK
A man was charged with the murder of a 16-year-old boy after he was found stabbed to death in Islington.

23 October, Ankara – Turkey
Five people were killed and 22 others wounded in an explosion at the headquarters of the national aerospace company, Tusas. Gunfire was also heard.

25 October, London – UK
A man has been arrested on suspicion of attempted murder after a woman and two children were stabbed in Dagenham.

Americas

1 October, Florida – USA
Two concealed devices made with fireworks were found at the Seminole Hard Rock Tampa, forcing the Seminole police and the FBI to evacuate the casino to twice.

14 October, Lazaro Cardenas – Mexico
The Mexican navy arrested 23 people in its largest-ever drugs bust, seizing over eight tonnes of illicit cargo.

14 October, New York – USA
Police arrested numerous pro-Gaza protesters outside the Stock Exchange after a demonstration.

15 October, Iqaluit – Canada
An Air India plane bound for Chicago had to make an abrupt landing after a false bomb threat. The emergency stop came less than a day after Canada and India expelled senior diplomats in a widening feud between the two countries.

16 October, Phoenix– USA
Police faced widespread criticism following as body camera footage showed two white officers violently using a stun gun on and punching a deaf Black man with cerebral palsy.

19 October, Lexington – USA
Three people were killed and eight others wounded in central Mississippi when at least two people fired guns at a group of several hundred people who were celebrating a high school football team's homecoming win.

19 October, Georgia – USA
A mass shooting during homecoming weekend at Albany State University left one person dead and five others wounded.

Asia

1 October, Churachandpur district – Manipur
Unidentified gunmen shot dead a commander of the Kuki National Army insurgent group in the Kuki-dominated village of Leisang.

1 October, Jaffa – Israel
Six people were killed and 10 wounded in a shooting and knife attack in the Israeli seaside city that occurred minutes before Iran launched a huge missile attack on the country.

2 October, Riyadh – Saudi Arabia
A fitness instructor and influencer was stabbed in the face in prison with a pen after being jailed in January for promoting women's rights on social media.

3 October, Paju – South Korea
A North Korean defector living in the South Korea was detained after ramming a stolen bus into a barricade near the heavily militarised border, in an attempt to return to his homeland.

6 October, Karachi – Pakistan
An explosion near the international airport of the southern Pakistani city killed two Chinese nationals and injured several others. No one claimed responsibility.

12 October, Mumbai – India
Politician Baba Ziauddin was shot near his car while he was leaving his son's office. He died later in hospital. No one has yet claimed responsibility.

15 October, Singapore
Singapore's air force mobilised two fighter jets in response to a bomb threat on an Air India Express flight bound for the city-state.

19 October, Caesarea – Israel
Benjamin Netanyahu's house was targeted by three drones, two of which were intercepted. No one was home at the time.

22 October, Enga – Papua New Guinea
At least seven people were killed and more than a dozen were missing after gunmen ambushed a public bus and shot passengers in Lagaip district.

Africa

1 October, Borno State – Nigeria
Boko Haram terrorists abducted 15 farmers in the Ngoshe community of Gwoza Local Government Area. Five of the abducted individuals were killed, along with a member of the Civilian Joint Task Force.

1 October, Borno State – Nigeria
Multinational Joint Task Force troops intercepted a group of Boko Haram terrorists transporting 40 hostages during clearance operations in Mongunu. The militants fled and the hostages were freed.

4 October, off the coast of Djibouti
As many as 48 people were confirmed dead and more than 100 others still missing after smugglers forced migrants to leave their boats and swim in the Red Sea.

5 October, Port Harcourt – Nigeria
Police are investigating after two explosions in the early hours of the day. One occurred at the Rivers State secretariat of the All Progressives Congress (APC) while the other was at the headquarters of the Obio/Akpor council. No one was hurt.

6 October, El Dheer – Somalia
Authorities reported the killing of 47 militants from the al-Qaeda-linked al-Shabaab group during a military operation which included the destruction of their base and a car bomb.

14 October, Borno State – Nigeria
A soldier was killed by Boko Haram terrorists who attacked troops in the Mafa Local Government Area.

19 October, Maputo – Mozambique
Attackers killed a Mozambique opposition lawyer and a party official after firing rounds at a car in which they were travelling.

24 October, Borno State – Nigeria
Four abducted people were beheaded by extremists believed to be from Boko Haram – who released a video of the murders.

29 October, Morocco
A hacker leaked the personal data of 180,000 Esport North Africa users just hours before the tournament. No financial details were believed to have been exposed.

NEWS

Europe

Hate crimes in Scotland up since law introduced in April

Recorded hate crimes in Scotland have risen by 63 percent since new legislation came into force, with officers saying the increase reflects greater public confidence that offences will be investigated. Data reveals a significant rise in hate crime against disabled people and elderly people. Police Scotland says concerns about the impact on freedom of speech have not been borne out. The Hate Crime and Public Order (Scotland) Act came into force on 1 April and consolidated the existing law on crimes that are "aggravated by prejudice", adding age to other protected categories, and created an offence of behaviour that is "threatening or abusive" and "intends to stir up hatred". The deputy chief constable, Alan Speirs, said: "When there is increased public trust and confidence, people will speak out. I don't think this rise suggests any community is less safe now than they were six months ago, but it does show more people are highlighting their concerns. Figures reveal 5,437 hate crimes were recorded between 1 April and 1 October.

Ireland is "playground" for Russian intelligence

Ireland is a "playground" for Russian intelligence, a former deputy chief of an Irish army unit has said following claims that a member of parliament was recruited by the Kremlin to undermine Anglo-Irish relations during Brexit talks. Cathal Berry, now a member of the Irish parliament, said he had not been surprised by a report in early October that the unnamed politician had been recruited as: "an agent of influence" in a honeytrap operation. "If you are looking to affect a western country with extensive assets and a poor security culture then Ireland is ground zero," Berry told the *Irish Times*. "Here the Russians get maximum impact for minimum effort. It is a playground for them." According to the report in the Irish Sunday Times, the aim of the operation was to build contact with loyalist paramilitaries at a time of sensitive discussions with the UK about whether there would be checks on the Irish border or not. The reported mission ties in with wider hybrid warfare efforts identified by the EU which it says can involve anything from disinformation to suspected arson and antisemitic attacks.

Thinktanks urge 'Trump-proofing' European security

Europe, the UK and Ukraine urgently need to "Trump-proof" their collective security by setting up a "Nato bank" to aid defence spending, a report released in early October suggests. Europeans have to face the reality that if Donald Trump wins the presidential election, he may quickly slash US defence spending in Europe, seek to impose a peace deal on Ukraine that leaves tracts of its territory in Russian hands and even withdraw from Nato altogether, the report by UK and German thinktanks claims. Such steps would have huge consequences for intelligence sharing and the viability of article 5, Nato's crucial collective self-defence clause, the report noted. To mitigate the impact of a second Trump presidency, Nato countries should support the creation of an allied multilateral lending institution, in practice a Nato bank, it said. This could "save nations millions on essential equipment purchases, offer low interest rates on loans to alliance members and introduce a new line of financing with longer repayment timeframes. The bank would be funded with initial subscriptions from Nato members in return for authorised capital stock".

Teenagers as young as 13 investigated for far-right terror

Teenagers as young as 13 are coming under suspicion of engaging in terrorism after being exposed to a toxic cocktail of easily accessible far-right extremism online, experts have warned. Insiders describe a: "horrible hateful soup" of social media content where children can "pick and mix" terrorist narratives, including the Terrorgram network – recently banned in the UK – of white supremacist channels on Telegram. Experts have tracked 49 children convicted of terror offences since 2016 – all but one of which are boys – with MI5 Chief Ken McCallum adding that: "13 percent of all those being investigated by MI5 for involvement in UK terrorism are under 18", a threefold increase in three years. The increasing proportion of children under scrutiny also poses problems, with questions arising over whether teenagers should be criminalised – with MI5 and experts acknowledging cases often raise issues of mental health or grooming.

NSSLGlobal provides satcom for Federal Office of Civil Protection

NSSLGlobalhas announced that it is set to provide satellite communications services and technology to Germany's Federal Office for Civil Protection and Disaster Assistance (BBK) for their management and delivery of critical crisis communications. NSSLGlobal will provide the 24/7 connectivity, hardware and technical support that teams need when operating in extreme conditions to protect the country. Portable satcom is the key to secure, rapid communications and the command and control of dispersed, small units, avoiding the delays and interruptions to terrestrial infrastructure that often accompany emergencies. Providing voice and data communications, NSSLGlobal will enable operators to pass vital information to decision-makers and those at the operational face at critical times. In addition, the BBK will use NSSLGlobal's INSIGHT business management portal to provide users real time information on all interactions, for comprehensive monitoring, control and alerting along with provision of data records.

NEWS

Americas

Online posts show IS interest in attacks on US ahead of election

After the FBI arrested an Afghan man in Oklahoma planning an election day shooting on behalf of the Islamic State in early October, warnings about IS-sponsored or inspired attacks in the west have intensified. The US attorney general, Merrick Garland, remarked there was a continuing need to: "combat the ongoing threat that [IS] and its supporters pose to America's national security". The online conversations are being led by IS-Khorasan (IS-K), the branch based in Afghanistan behind the Moscow attack that killed 145 people in March. IS-K has quickly become the most active international force of the terror group, having already carried out the deadly plot in Russia and another in Iran months before it. In a propaganda poster it released in September, IS-K put American targets top of its hitlist. While IS-K has seized on the tumult in Afghanistan since the Taliban took over in the summer of 2021 and established a base of operations there, its broader movement has also been heavily recruiting since the 7 October attacks and Israeli military operations that followed.

Jamaica welcomes US move to clamp down on gun trafficking

Jamaica's deputy prime minister has welcomed a campaign by the New York attorney general, Letitia James, to push through new measures and legislation to tackle gun trafficking from the US to the Caribbean. Horace Chang, who is also Jamaica's minister of security, praised a coalition of 14 US attorneys general, led by James, that is backing the passing of the Caribbean Arms Trafficking Causes Harm Act. Introduced in both houses of the US Congress earlier this year, the act aims to help curb illicit arms trafficking from the US to the Caribbean. In a letter to Congress, the attorneys general outlined actions that need to be taken, including improving resources for US port inspectors and increasing funding for the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF). The letter highlights Jamaica's alarming homicide rate of 53.3 per 100,000, pointing out that it is "currently the highest rate of countries with reliable statistics". It also flags that, according to Jamaican government estimates, at least 200 guns are trafficked into the country from the US every month, adding that these guns are fuelling violent crime and enabling drug smuggling networks that traffic drugs to the US. Chang said that he hoped the campaign would support Jamaica's efforts to combat gun crime, which he said include improving border control and creating new legislation.

Two men plead guilty to contract killing of Sikh man in Canada

Two men have pleaded guilty to the contract killing of a Sikh man who was acquitted in the 1985 bombing of an Air India flight from Montreal to Mumbai. According to an agreed statement of facts released by a British Columbia court, Tanner Fox and Jose Lopez confessed to shooting Ripudaman Singh Malik in 2022. But they remained silent over who hired and paid them for the murder. Malik was a prime suspect in the attack on Air India flight 182, which exploded off the coast of Ireland, killing 329 people. But he and another man, Ajaib Singh Bagri, were acquitted after a judge determined that two key prosecution witnesses were unreliable. The case came days after Canadian officials revealed a wide-ranging and violent campaign of intimidation of Sikhs across Canada orchestrated by India's government. Both men are due back in court on 31 October for sentencing. Two hundred and eighty Canadians died in the Air India attack, which remains the worst act of mass murder in the country's history. The victims included 86 children. A second bomb targeting another plane killed two baggage handlers after it detonated at Tokyo's Narita airport.

Illegal US-Mexico border crossing arrests fall to new low

Arrests for illegally crossing the US border from Mexico fell 7 percent in September to a more than four-year low, authorities said in early October. The border patrol made 53,858 arrests, down from 58,009 in August and the lowest tally since August 2020, when arrests totalled 47,283, according to US Customs and Border Protection. Mexicans accounted for nearly half of the arrests, becoming a greater part of the mix. In December, when arrests reached an all-time high of 250,000, Mexicans made up fewer than one in four. Arrests for other major nationalities seen at the border, including Guatemalans, Hondurans, Colombians and Ecuadoreans, have also plunged this year. San Diego was again the busiest corridor for illegal crossings in September, followed by El Paso, Texas and Tucson, Arizona. For the government's fiscal year ending 30 September, the border patrol made 1.53-million arrests after topping 2-million in each of the previous two years for the first time.

Trump and Vance's phones targeted by Chinese hackers

Chinese government-linked hackers are believed to have targeted phones used by Donald Trump and his running mate, JD Vance, as part of a larger breach of US telecommunications networks, according to a *New York Times* report. The Trump campaign was informed in late October that the phone numbers of the Republican presidential and vice-presidential nominee were among those targeted during a breach of the Verizon network, the paper said. Investigators are working to determine what data was accessed. The FBI and the Cybersecurity and Infrastructure Security Agency confirmed an investigation was under way into the "unauthorised access to commercial telecommunications infrastructure by actors affiliated with the People's Republic of China".

NEWS

Asia

China introduces cyber security rules for generative AI

China has announced plans to implement a string of new cyber security rules next year, placing an emphasis on national security and requiring companies providing generative artificial intelligence services to add extra data protection. The new network data security management regulations contain 64 clauses based on China's cyber security and data security laws. They will go into force from 1 January. Under the new rules, companies that provide services related to generative AI must enhance their training in data processing and other areas. They are also required to take steps to prepare for data breach risks. Non-Chinese operators must establish data processing centres within China if they handle personal data originating from the country. Under the general provisions, data processors that are deemed to have undermined China's national security, the public interest or legally protected interests will be held legally responsible. This applies regardless of whether the data is processed within China or abroad.

Cyber security threats on the rise in Hong Kong

Online threats have surged in Hong Kong this year, with scams, phishing and malware among the most common attacks, a survey found, as a lack of cyber security awareness plagues the city. As many as 49 percent of Hong Kong respondents have experienced online threats over the past 12 months, compared with 40 percent in the previous period, according to a report by antivirus software vendor Norton. Scams were the most common threat, affecting 34 percent of respondents with nearly two-thirds of the victims losing money or time as a result. The next most prevalent threats, phishing and malware, each affected 28 percent of the respondents. Hong Kong police said in July that financial losses resulting from online scams jumped 37 percent year on year in the first five months of 2024, even though the number of incidents rose less than 1 percent. Cyber security experts have described the city's businesses as an "easy target" for attacks because few companies know how to monitor for cyber threats.

Detection Technology expands its global footprint into India

Detection Technology, producer of X-ray detector solutions, has expanded its service and production facility in the greater Delhi, India. The move is designed to enhance customer experience by offering local service, quicker response and delivery times, and cost-effective solutions, all while maintaining the company's high standards of quality. "India is about to make significant investments in infrastructure, namely in the healthcare, traffic and manufacturing industries, and we want to be there to promote these projects." says Hannu Martola, President and CEO at Detection Technology. Located in a leading industrial hub at Cyberwalk Tech Park, IMT Manesar, Gurgaon, in the Delhi NCR area, the new service and production site benefits from excellent connectivity across India and internationally. Detection Technology's wholly-owned subsidiary in India is registered as DT Detection Technology India Private Ltd.

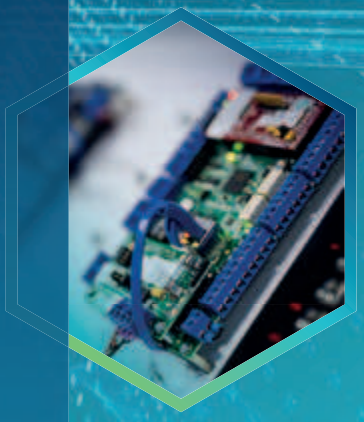
Milipol Qatar 2024 concludes with historic milestones

Milipol Qatar 2024, the 15th edition of the Global Event for Homeland Security and Safety, successfully achieved record visitor turnout of over 14,500 and a total of QAR 842-million in declared sales. The show was inaugurated by the Minister of Interior and Commander of the Internal Security Forces, Sheikh Khalifa bin Hamad bin Khalifa Al-Thani, who was accompanied by a number of Their Excellencies the Ministers and senior officials from the country, as well as guests including Their Excellencies the Ministers, police chiefs from various sisterly and friendly countries, ambassadors, experts, specialists from around the world and leading international companies specialising in internal security, and representatives of exhibiting companies. The show also attracted 360 official delegates who toured the exhibition. Major General Nasser bin Fahad Al Thani, Chairman of the Milipol Qatar Committee stated during the closing ceremony that the delegations' programme had a key influence in attracting 255 exhibitors from 26 nations across Europe, Middle East, Asia and North America of which 70 companies were from Qatar. International participation accounted for 70 percent of the exhibitor profile, with six International Pavilions from France, North America, Germany, Italy, Czech Republic and China. This edition also marked another significant milestone with seven new countries participating: Greece, Jordan, Latvia, Lithuania, Portugal, Saudi Arabia and Sweden. The event covered a wide spectrum of homeland security, featuring cutting-edge technologies in cyber security, anti-drone solutions and more. 20 percent of exhibitors were involved in authentication, access control, surveillance, transmission, communication and positioning, while 18 percent specialised in information technology and cyber security. Some 15 percent focused on fire and protection, major risk prevention, crisis management and civil emergencies response. "Milipol Qatar is also a huge opportunity for high-level exchanges between states when it relates to homeland security issues." explained Prefet Yann Jounot, CEO of Civipol and president of the Milipol International Network. Plans for the next show are already underway and some exhibitors have booked their stand. The next edition of Milipol Qatar is scheduled for 20-22 October, 2026, promising to bring even more security innovation for visitors.

THE SECURITY EVENT

8-10 APRIL 2025 NEC BIRMINGHAM

EUROPE'S LEADING COMMERCIAL, ENTERPRISE & DOMESTIC SECURITY EVENT



GET INVOLVED

WWW.THESECURITYEVENT.CO.UK

ORGANISED BY

Nineteen™

NEWS

Africa

Timbu: We are winning war against Boko Haram fighters

President Bola Ahmed Tinubu has said that his administration is winning the war against terrorism. In a nationwide broadcast, the President said before taking over 16 months ago, the country was bugged down by economic and security challenges. The President claimed that his administration has eliminated Boko Haram and bandit commanders faster than ever, adding that as of the last count over 300 commanders have been eliminated by troops in the North-East and North-West of the country. The President explained: "On the security front, I am happy to announce to you, my compatriots, that our administration is winning the war on terror and banditry. Our target is to eliminate all the threats of Boko Haram, banditry, kidnapping for ransom, and the scourge of all forms of violent extremism.

Blinken commends Africa Focus Group's fight against terrorism

US Secretary of State Antony Blinken underlined in early October the importance of the Africa Focus Group of the Global Coalition to Defeat Daesh – co-chaired by Morocco, the US, Italy and Saudi Arabia – in the fight against terrorism on the African continent. Speaking at the opening of the 11th ministerial meeting of the coalition, the US diplomat noted that the terrorist group is increasing its efforts to expand its operations outside the Middle East, particularly in sub-Saharan Africa, noting that the efforts made by the Africa Focus Group had: "helped African partners better align and coordinate to support civilian-led counterterrorism operations" in Sub-saharan Africa. These efforts are particularly relevant at a time when "in sub-Saharan Africa, ISIS affiliates have gained ground, compounding the threat already present from existing militant groups," said Blinken. Three years after its creation, the Africa Focus Group has become an essential component of the Global Coalition to defeat Daesh in Africa, while current needs and emerging trends require the reinforcement of this dynamic. .

Cyber security specialist Arctic Wolf expands to South Africa

Arctic Wolf, a leader in security operations, has announced plans to establish a team in South Africa and is recruiting local partners to drive adoption of its cyber security solutions. As from early October, a team of Arctic Wolf employees will help customers on the African continent to benefit from the company's security monitoring to detect and respond to cyber threats. It monitors computers, networks and cloud-based information assets from malicious activity such as cyber crime, ransomware. "We have had considerable interest in the advanced cyber security which we offer customers from businesses throughout South Africa and the wider continent, so it was a logical step to formally start operations there," Clare Loveridge, Vice President & General Manager EMEA, Arctic Wolf explained. "As a channel driven business, we believe it is critical for us to be able to recruit partners in South Africa with the vision and skills necessary to highlight to their customers the enormous benefits that Arctic Wolf can bring with its unparalleled protection. We have been delighted in only a few days, how much interest the South African channel has shown in what we do and in how we can work together to protect businesses large and small from cyber attack."

Breakdown in global order stalling progress in Africa

The global rise of populism and "strongmen" has led to an increase in authoritarianism in Africa that is holding back progress in governance, the businessman and philanthropist Mo Ibrahim has said. According to the latest edition of the Ibrahim index of African governance, 78 percent of Africa's citizens live in a country where security and democracy deteriorated between 2014 and 2023. The study, which is published every two years, measures the performance of African governments in the fields of security and law; participation, rights and inclusion; economic opportunity; and human development, which includes health and education. While the worst deterioration in the measures studied was in security and safety, democracy, including participation, rights and transparency, also deteriorated. In the sub-category of security and safety, more than half the continent's population saw violence increase over the last five years. The lack of security was slowing progress for economic opportunity as well as in health, education, social protections and sustainability.

Ghana launches national cyber security awareness month

In a pressing address during the official opening of the National Cyber Security Awareness Month in Ghana, concerns were raised regarding the alarming rise of misinformation proliferated through digital media platforms in the region. Highlighting recent trends, attention was drawn to the growing use of YouTube channels, encrypted messaging services like Telegram and deep fakes that specifically target electoral processes and political figures. The speaker emphasised the urgent need for enhanced public and media education as vital tools in the fight against disinformation. "Misinformation can undermine the integrity of our democratic processes, particularly during election periods," they stated. In response, the Ministry of Communications and Digitalisation, in partnership with the Cybersecurity Authority, is collaborating with digital platform owners, including Meta, to implement rapid response mechanisms for misinformation reports, especially during election seasons.

DIARY DATES

2024/5 Conference and Exhibition planner

9-12 December
Black Hat Europe 2024
London, UK
Organiser: Informa Tech
Tel: +1 866 203 8081
Email: blackhatregistration@informa.com
www.blackhat.com

14-16 January
Perimeter Protection 2025
Nuremberg, Germany
Organiser: NürnbergMesse GmbH
Tel: +49 9 11 86 06 88 89
Email: perimeter-protection@nuernbergmesse.de
www.discoverisc.com/east/en-us.html

5-6 February Cyber Security & Cloud Expo 2025
London, UK
Organiser: TechEx Media
Tel: +44 (0)117 973 2353
Email: events@saemediagroup.com
www.cybersecuritycloudexpo.com

11-13 March Security & Policing Home Office Event 2025
Farnborough, UK
Organiser: ADS Group
Tel: +44 (0) 207 091 7835
Email: registration@securityandpolicing.co.uk
www.securityandpolicing.co.uk

8-10 April
The Security Event 2025
Birmingham, UK
Organiser: Nineteen Group
Tel: +44 (0)20 8947 9177
Email: info@thesecurityevent.co.uk
www.thesecurityevent.co.uk

6-8 May
CyberUK 2025
Manchester, UK
Organiser: National Cyber Security Centre
Tel: +44 (0) 117 906 4554
Email: cyberuk-events@brayleinoevents.com
www.cyberuk.uk

3-5 June
Infosecurity Europe 2025
London, UK
Organiser: RX Events
Tel: +44 20 8271 2134
Email: rxinfo@reedexpo.co.uk
www.infosecurityeurope.com

4-5 June Cyber Security & Cloud Congress 2025
California, USA
Organiser: TechEx Media
Tel: +44 (0)117 973 2353
Email: events@saemediagroup.com
www.cybersecuritycloudexpo.com

9-12 September
DSEI 2025
London, UK
Organiser: Clarion Events
Tel: + 44 (0)330 912 1213
Email: customersolutions@dsei.co.uk
www.dsei.co.uk

HZL®

Specialist Solutions

HZL are delivering QNUK Level 4 Award in Physical Penetration Testing Operations(RQF)

The Standards You Walk Past® Are The Standards You Accept

Tel: 0333 200 1676 **Email:** info@hzlgroup.com
Website: www.hzlgroup.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

Audiebant solar-powered communication system

Audiebant has announced the release of Audiebant Outdoor, the world's first solar-powered, portable, app-driven mass communication system designed specifically for outdoor events. Formulated to provide swift and area-specific instructions to manage crowds, it helps to ensure public safety in emergencies including potential terrorist incidents. The system allows both live text-to-speech and pre-recorded messages to be broadcast instantly to multiple zoned areas, allowing organisers to direct specific groups of attendees to specific exits or safe zones during critical incidents. Powered by solar energy in low-light conditions and a battery backup for 10 days of continuous operation, the solution is moveable, adaptable, resilient and cost-effective for any event location. AI-driven communications ensure calm, clear and concise messaging to reduce fear and confusion, and messages can be initiated by an unlimited number of authorised users from any location using a mobile device or computer. Alongside emergency applications, the system can be pre-programmed to play health and safety information, event updates, promotional messages or background music.

Hanwha Vision Bi-spectrum Radiometric Thermal AI cameras

Hanwha Vision has unveiled its new high-performance nbi-spectrum radiometric thermal AI cameras, which are claimed to be ideal for use for perimeter protection, traffic monitoring, manufacturing, industrial facilities, data centres, solar farms and more. The TNM-C3620TDR/C3622TDR cameras serve as compact indoor models and feature QVGA resolution on the thermal lens and 2MP on the visible sensor, while the TNM-C4940TDR/C4942TDR outdoor models combine advanced VGA thermal and 4K video. The range is designed to deliver clear images in all lighting scenarios, with AI-powered analytics for accurate object detection and temperature monitoring between -20°C and 130°C. With the outdoor models supporting AI on thermal and visible sensors, they can not only detect objects in difficult lighting conditions, such as complete darkness, fog or rain, but also alert operators to potential intrusion, loitering or other suspicious behaviour. Meanwhile, the compact indoor models feature AI on the visible channel. By ensuring a high degree of accuracy across the range, false alarms triggered by irrelevant motion, for example wildlife or shadows, are significantly reduced, improving operational efficiency and meaning operators focus only on genuine events. Intelligent video analytics.

Veridos and Credence ID All-in-One Verification Device

E-Seek by Veridos and Credence ID have introduced the VeriCHECK M500+, the world's first all-in-one verification device designed to authenticate both digital and physical ID documents. This solution addresses the growing need for seamless ID verification as mobile credentials gain popularity alongside traditional physical IDs and integrates E-Seek's physical credential reader, already used by the US Transportation Security Administration at over 220 US airports, with Credence ID's Tap2iD digital verification platform. This combination enables secure authentication of digital IDs such as mobile driver's licences, using NFC and QR code technologies, and complies with the latest ISO standards. With compatibility across popular digital wallets, including Apple and Google, it offers flexibility for both government and commercial applications and operates in both online and offline modes to ensure uninterrupted service.

HID FARGO HDP5000e ID printer

HID has unveiled the next-generation of its FARGO HDP5000e designed to deliver vibrant, high definition cards and IDs. Engineered for universities, medium-to-large businesses, healthcare facilities and government agencies who need retransfer printing technology to effectively personalise contactless cards, the FARGO HDP5000e delivers an increased card throughput and greater Ethernet speed than its predecessors. The HDP5000e's SmartScreen interface is high-definition, while graphical OLED provides easy-to-understand notifications and walk-through prompts for setup, maintenance and troubleshooting. The printer's Workbench diagnostic utility with its Colour Assist spot-colour matching tool is built into the driver so users have immediate access to everything they need via a single driver download. The printer's unique resin scramble data protection feature effectively scrambles and subsequently conceals information printed with a resin panel. Used ribbon panels are thus rendered indecipherable, safeguarding cardholder data from fraudulent use. Moreover, the HDP5000e includes built-in AES-256 data encryption, support for UV printing and offers optional locks.

Supacat's new defence vehicles

Supacat launched two defence vehicles in mid-September. The first is a multi-role tactical light mobility vehicle (LMV) for light role and Very High Readiness forces. The second is a new addition to the High Mobility Transporter (HMT) family, with a 4-person armoured closed cab platform, giving it the flexibility to fulfil a wide range of roles in contested environments. The Supacat LMV combines highly proven ubiquitous Toyota automotive components with a bespoke chassis and battle-tested 'combat cell' and is manufactured in both 4x4 and 6x6 configurations to suit different roles – offering a payload of up to 3,200kg. The Supacat HMT is designed to support the UK MOD's Land Mobility Programme's fleet reduction to 15 core platform chassis types or less by 2030. Its 4-person closed cab provides integral blast and ballistic protection and the vehicle is compliant with Generic Vehicle Architecture requirements, supporting the electrical and electronic integration of a range of complex Mission Systems. It has a payload capacity of circa 4,000kg with integrated blast and ballistic armour, with the chassis load bed designed to allow easy physical integration of Mission Systems.

ATG ACCESS
PROTECTING WHAT MATTERS

BEAUTIFULLY SECURE

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

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

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

3DX-RAY

INSIGHT WHERE IT MATTERS

ThreatScan®-AS1

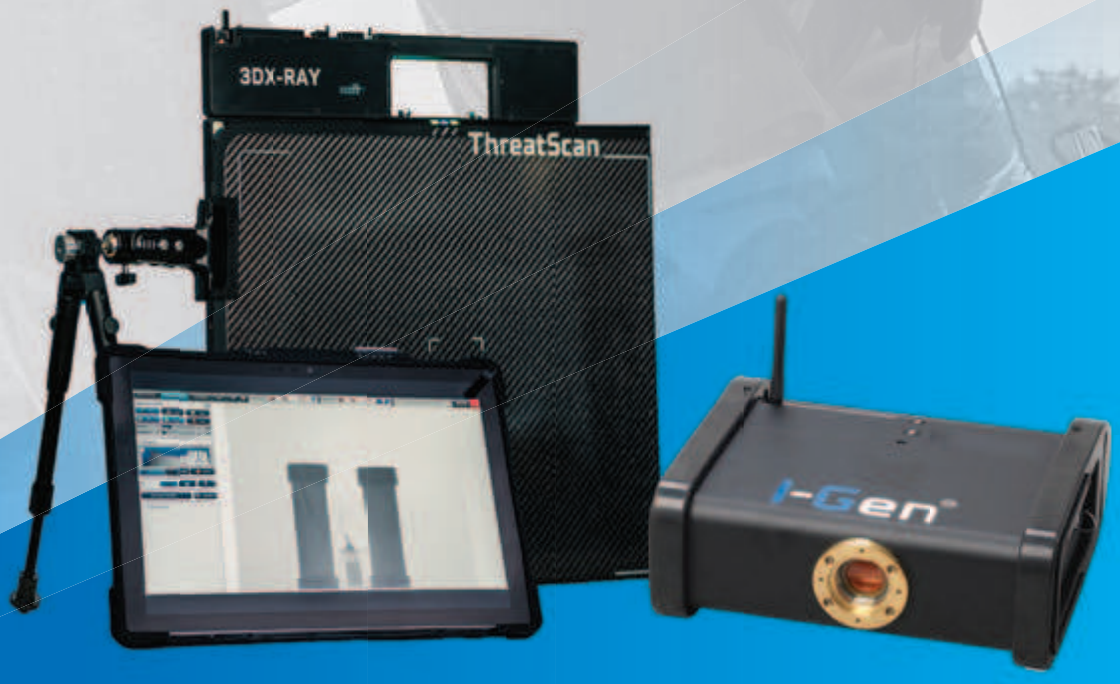
AMORPHOUS SILICON PORTABLE X-RAY SYSTEM

Amorphous silicon system c/w 120kV or 150kV generator

Portable, real-time x-ray scanning

High penetration with sub-millimetre resolution

Intuitive, user-friendly ThreatSpect software



www.3dx-ray.com

An **IMAGE SCAN** company