www.intersec.co.uk

intersec

The Journal of International Security

March 2022

REMOTE CONTROL

Benefits of autonomous ground vehicles

The new 'Protect Duty'

A proactive approach for businesses

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 32 Issue 3
March 2022

Cover photograph: ABD Solutions

Editor
Jacob Charles

Principal Consultant Editor
Maj. Gen.
Julian Thompson CB OBE

Design & Production
jellymediauk.com

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

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

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

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

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

EDITORIAL COMMENT

As bombs continue to rain down on Ukraine and fighting with Russian troops intensifies, the war has inevitably moved into cyberspace as fake news, deepfakes and cyber attacks become another key battleground for both sides. For its part, Ukraine's cyber-offensive has scored some major success with distributed denial of services (DDoS) attacks targeting Russian government websites including the Kremlin, the Duma and the Russia Today news service. Hackers have been coming together and organising their response using the Telegram app under the IT Army of Ukraine banner with – at the time of writing – 300,000 people joining up. Meanwhile the Anonymous hacking collective has also claimed credit for a number of attacks.

However, Western officials have: "strongly discouraged" joining the former group and initiating hacking activity against Russia in any way amid fears that activists could be making matters worse by breaking the law or launching attacks that could spiral out of control. It has been suggested that taking part in cyber attacks from either the UK or US could break domestic laws in those respective countries. Professor of cybersecurity at Surrey university Alan Woodward told *The Guardian* newspaper: "While I totally understand the sentiment behind the actions of many in this IT army, two wrongs do not make a right. Not only might it be illegal, but it runs the risk of playing into Putin's hands by enabling him to talk about attacks from the west."

No newcomer to fighting in the digital realm itself, Russia has scored a number of successes of its own, targeting Ukraine with a series of DDoS sorties and several 'wiper' attacks, which have destroyed computers. On the whole, however, Ukraine has put up a fairly stern resistance, limiting the impact of such attacks assisted by western governments. "Behind the scenes [there has been] a massive international government effort to support our Ukrainian allies in this space," said one official. Before cryptically continuing: "We are not seeing a heightened threat to the UK or generally to allies. It's fair to say that the level of cyber-activity we see is not significantly up or down".

Arguably the most significant win in this respect for Russia involving a western target has been the US telecoms company Viasat after a group of unidentified (but almost certainly Russian-backed) hackers disabled tens of thousands of modems used for communicating with the company's KA-SAT satellite, which supplies internet to customers in Europe, including Ukraine.

Meanwhile Russia has been carrying out infowar across social media, with perhaps the most high-profile example including a deepfake video of President Zelensky calling on soldiers to lay down their arms and return to their families. Despite efforts of social media platforms to limit the video's impact, it is understood to have reached as many as 5-million viewers. With Facebook and Instagram blocked in Russia, Twitter severely restricted and western content on TikTok non-existent, there remains concern about the quashing of dissident voices in Russia and the way that Putin still effectively controls the narrative.

Jacob Charles, editor

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

Subscriptions
Annual Subscription Rates: UK £180,
Europe £200,
USA post paid US$350
Other Countries air-speeded £250. Subscription Enquiries: subs@intersec.co.uk
Average net circulation per issue: 10,510
Intersec (USPS No: 006-633) is published monthly except Jul/Aug and Nov/Dec combined issues, by Albany Media Ltd

Subscription records are maintained at Albany Media Ltd, Warren House, Earlsdown, Dallington, Heathfield, TN21 9LY

Issue Date: March 2022

CONTENTS

intersec

Features

Regulars

SCANNA

High Performance, DR and CR X-ray systems from a name you can trust..
with x-ray generators you know and trust.

SCANSILC EOD - DR X-RAY

- Lightweight intelligent x-ray panels in 10 x 12" and 14 x 17" formats.
- Impact and drop tested to over 1m. Dirt and water resistant to IP67
- No extra interface box or splitter required - unlike competitive systems
- Solid state, no moving parts and load resistant to 170 kgs

SCANX SCOUT - CR X-RAY

A must in every bomb truck!

- Multi- size x-ray electronic free x-ray plates
- Wire free and flexible for tight access applications.
- Ground level imaging - no dead zone
- X-ray Multiple image plates in a single exposure. XTK software stitches your x-ray images together.
- Digital processor scans plates up to 130 cm long

All operating with the new Golden XR range of pulsed x-ray generators.

- Now with new higher performance Li-Ion battery power, custom pulses and custom delays!
- Simple to setup - no need to set kv or exposure time!
- Low radiation due to short nano-second bursts of x-ray!

XR150

XR200

XRS-3

Demonstrating in your area soon.
Email demo@scanna-msc.com

www.scanna-msc.com
info@scanna-msc.com

What next for Putin?

Major General Julian Thompson CB OBE Principal Consultant Editor

There has been much speculation in the media about the performance of the Russian army in Ukraine. A statement by the Secretary of State for Defence, Ben Wallace includes the opinion that: "his [Putin's] army is done" in Ukraine. I hope he is right. But we need to bear in mind that the politicians, and notably the party to which Mr Wallace belongs, have done much harm to the British defence capability (not that any other political party would have done any better; probably even worse). So, are they fit to make a judgement on military matters? Until the mid-Nineties the British army could field four well-equipped armoured divisions in Germany, and in addition had several well-equipped brigades in the UK ready to go anywhere. These included the elite 3rd Commando Brigade and 16 Parachute Brigade, along with the necessary shipping and aircraft to lift them. Now the British army might be able to scrape together two armoured brigades with around 160 tanks, along with a reduced number of high-readiness brigades. The air force and navy have similarly been trimmed. We can take comfort from the fact that we still maintain the nuclear deterrent. Although we have let our guard slip to the extent that the Russians have been spotted planting sonar buoys in the approaches to the Firth of Clyde. These warn the Russians of the departure of our nuclear submarines, both hunter-killers and missile armed 'bombers' from their base at Faslane.

The question to ask is: what if the Russians are not done? Some expert Russia watchers have assessed that other than some air-assault forces, the Russians have not put their best trained and equipped formations into Ukraine. Most military observers agree that with logistic units the much-quoted figure of 190,000 Russian troops in Ukraine is about correct – not by a long way the whole of their army.

The Russians still follow the Soviet tactical doctrine, including a system of echelons for offensive operations. When the first echelon loses momentum, or grinds to a halt, possibly through suffering heavy casualties in men and materiel, a second echelon passes through and continues the fight. What we are seeing in Ukraine is the first echelon at work. The second consists of the First and Twentieth Armies, which are composed of the best of Russia's army and the most modern equipment. Behind the second echelon is the strategic echelon, to be switched to where it can best achieve the strategic objective. This might involve opening a new front; perhaps by swinging the main effort from Kiev to the south, accompanied by a deception, Maskirovka, to give it its Russian name. The aim being to keep our eyes focussed on the area of Kiev, and especially on the much-publicised stationary convoy 40 miles long; the object of much scorn from media and 'armchair generals' alike. While we are all distracted perhaps airborne formations will envelop Odessa, in co-operation with the Black Sea Fleet marines. This could be followed by moving through Moldova east of the Dniester River to carry out a strategic envelopment of Kiev before moving into western Ukraine from the south.

Picture credit: Crown Copyright

Ben Wallace (at a recent Extraordinary meeting of NATO Ministers of Defence) believes Putin's army is "done"

We should remember that the Russians use information as a propaganda tool, manipulating facts and truth like weapons. They regard it as perfectly normal operational procedure to fix military and media attention on Kiev, while attacking with full force elsewhere. Russian success in Ukraine would be seen by Putin as payback time for 30 years of what Russians regard as provocations and insults by the West. For example, many former Warsaw Pact countries (effectively Russian satellites) including the Baltic States, Romania, Bulgaria, Hungary, Slovakia and Poland joined the EU and NATO. The West's intervention in the Balkans was seen by Russia as being directed against fellow Slavs, the Serbs. Russian success in Ukraine would be a warning to others not to contemplate joining NATO or the EU. In this respect the talk at high levels in the EU and NATO about Ukraine joining these organisations was irresponsible and strategically illiterate and was probably one of the main reasons why Putin invaded.

There has been speculation in the media about Putin resorting to nuclear weapons. There are some well-informed military commentators who do not believe he will take that step. They point out that Russia is faced by a superiority in nuclear weapons of three to one. Hence the likelihood of massive retaliation will deter Putin. But he might resort to chemical and biological weapons. He has them in his arsenal, and has used them in Syria, and we lest we forget, even closer to home in Salisbury, England; not a comforting thought.

Picture credit: ABD Solutions

AUTOMATION AND DEFENCE

Matthew Price *explores the benefits of autonomy when it comes to ground-based vehicles and security*

The defence industry has been moving towards vehicle autonomy for some time. Most existing automation has been adopted in the air and sea domains as navigating in these environments has a lower level of complexity. Autonomous and semi-autonomous drones are now commonplace in any defence fleet and have revolutionised how operations are carried out. However, automating ground vehicles has been technically more challenging; not only is the environment they operate in more varied, but the decisions needed to be made by the vehicle's AI are more complex.

One key driver accelerating the move towards automated vehicles is safety. According to Michael Griffin, the former US Department of Defense Under Secretary of Defense for Research and Engineering, 52

Retrofittable autonomous driving systems provide remote control of the Wolfhound

percent of casualties in combat zones can be attributed to personnel delivering food, fuel and other logistics. In 2009, a US Army study found there was one casualty for every 39 fuel convoys in Iraq and one for every 24 fuel convoys in Afghanistan. Automating logistics provides the opportunity to significantly reduce casualties and injuries.

Another key driver is cost. It is estimated that the US defence uses in excess of 320,000 barrels of oil per day. Automated ground fleets operate much more efficiently, supporting better vehicle and personnel utilisation and simplified operations. If a one percent fuel efficiency saving can be made through automation, it would save upwards of $100-million per year for the US Army.

Cost, as well as being a key driver, is also a key barrier to adoption. Fully autonomous vehicles require a significant amount of development, and this takes time and money. Another key financial element is the desire to maximise the ROI on the billions of dollars already invested in existing vehicle fleets.

However, the biggest reason why automated ground vehicles aren't commonplace is the technical challenge of achieving full autonomy. Controlling a vehicle is relatively simple, but perceiving the world ahead and then making decisions based on that information is incredibly complex. In theatre, vehicles will encounter a plethora of terrain, weather, lighting, obstructions and other vehicles. Also, any 'rules of the road' will often need to be ignored in certain scenarios adding a further layer of complexity.

By controlling elements of an operating environment and by focusing on specific operations, semi-autonomous capabilities can be achieved that provide most of the benefits that full autonomy has to offer.

By initially targeting specific user cases such as logistics or last-mile re-supply, increased focus can be placed on the unique operational requirements resulting in a tailored autonomy solution. In addition, to ensure effective adoption the impact on people and processes also needs to be considered. Applying new capability to existing ways of working will not deliver the full benefits that autonomy has to offer.

One solution that accelerates the adoption of autonomy and brings life and cost-saving benefits to the industry today is to retrofit autonomous capabilities to existing vehicle fleets. ABD Solutions recently demonstrated this approach when in partnership with NP Aerospace, developed the world's first fully automated Wolfhound Tactical Support Vehicle (TSV).

Retrofitting existing vehicles with autonomous capabilities requires a flexible solution that can be tailored to a specific vehicle, environment and operational scenario. A core modular, certified and secure software eco-system is used to build the various elements required for automation; including vehicle management, vehicle control actuation, communication, sense and detect, health and diagnostics and third-party integration.

This modular approach enables the autonomy solution to integrate with core and third-party technologies to ensure that specific requirements are met. The result is almost any vehicle can be retrofitted with autonomous capability and then fully integrated into any end user's existing operational/fleet management system.

For the defence industry, safety is arguably the key benefit of adopting vehicle autonomy. The technology enables personnel to be taken out of harm's way and to operate or manage fleets from a safe area. As well as removing personnel from direct harm, it can also reduce exposure to less obvious dangers.

Cybersecurity is also a key requirement when digitising vehicle operation and fleet management. As a result, it is critical that any system that is adopted is fully certified, conforming to industry-recognised cyber security standards.

There are several areas where vehicle autonomy provides cost savings to the defence industry. Firstly, automated vehicles can operate 24/7 without any downtime or need to switch shifts. This means that not only are fewer personnel required to carry out a particular task, but also fewer supporting resources (food, water, shelter *etc*). This can have a snowball effect on reducing the logistical cost of an operation.

52% OF CASUALTIES IN COMBAT IS ATTRIBUTED TO DELIVERING FOOD, FUEL AND OTHER LOGISTICS

A retrofittable autonomous solution will also significantly extend the lifecycle of the existing fleet. As there are billions of dollars invested in current vehicles, maximising return on investment on these assets is key to operators.

Across the globe, there is a desire to achieve more with fewer resources. As it costs more than £38,000 for a soldier to complete basic training in the UK, they should ideally be carrying out the most valuable tasks. Automating vehicles enables 'soldiers to be soldiers'. For example, this could mean reducing the number of drivers in a multi-vehicle convoy to just one, or in some situations none at all.

In a geo-fenced environment where logistical tasks are often repetitive, such as forward operating base resupply or fuel deliveries, all the vehicles involved can be synchronised. Mission planning software can ensure that all the vehicles take the most efficient route, reducing fuel consumption and the time to complete the operation. Vehicles that have the ability to detect obstructions can communicate them to the fleet management system to prevent others from encountering the same issue. Once the obstruction has been flagged the vehicle management system can generate an alternative route or a human can remote into the vehicle to immediately assess the situation.

One of the welcome side effects of autonomy is the digitisation of information from the vehicle. It creates new data streams that are invaluable to fleet operators. The vehicle's speed, location, fuel level, diagnostic status, distance to target *etc*. can all be relayed via the vehicle management toolset. Data analytics can process this information to assist with operational decisions, fleet maintenance scheduling and logistics planning.

HOW SOLUTIONS CAN BE USED

Convoys and logistics supply are examples of where personnel and equipment can be exposed to danger

on the battlefield. Vehicle autonomy solutions offer two main alternatives to a traditional convoy. A leading vehicle can be driven by a human with other vehicles in the platoon following the exact path of the lead vehicle. In low-danger scenarios, this is a very efficient way to transport multiple resources long distances. An alternative is to have the lead vehicle driven remotely by a human operator with other automated vehicles following the lead vehicle. This would be preferred in more hostile environments where reinforcements can remain relatively close.

AUTOMATING LOGISTICS CAN SIGNIFICANTLY REDUCE THE CHANCES OF CASUALTIES AND INJURIES

The most valuable advantage that vehicle autonomy solutions offer is removing personnel from dangerous situations. One of the biggest threats to soldiers is from Improvised Explosive Devices (IED). According to 'Honor the Fallen', a database created by the Military Times, nearly 50 percent of US soldiers killed in operation between 2010 and 2020 were caused by IEDs and similar statistics apply to British Army troops. Automated ground vehicles enable de-mining and route clearance to be carried out without the need for personnel to be in the blast proximity. The task can also be completed more thoroughly using accurate path following capabilities, improving the chances of success.

Automated vehicles can also be used to develop programmable targets for training exercises. The target vehicle can either be spontaneously remotely controlled by an operator or follow a specific path. Either can be accurately replicated and repeated all over the world, providing troops with more accurate live firing scenarios than the more traditional static targets or targets following 'rails' or winched along linear paths.

REMOTE CONTROL

The ability to control vehicles remotely creates strategic peacekeeping opportunities too. It helps to support an active peacekeeping presence in areas where it would not traditionally be possible to do so, or where resources are not available. It can also be used to generate physical mass in theatre through resilient swarms of low-cost automated systems rather than using large personnel deployments.

Fully autonomous vehicles will undoubtedly provide significant cost and safety benefits to the defence industry and the challenge now is how to integrate this technology in a timely and cost-effective way to maximise these benefits. Retrofittable autonomy driving solutions offer substantial operational safety and cost benefits and by utilising existing vehicle fleets and infrastructure they can be fitted today offering a stepping stone towards a fully autonomous future ●

Matthew Price is Managing Director of ABD Solutions, a specialist provider of retrofittable vehicle autonomy solutions.

Specially designed driving and pedal robots provide complete control of the vehicle

Picture credit: ABD Solutions

THE QUEEN'S AWARDS FOR ENTERPRISE: INNOVATION 2020

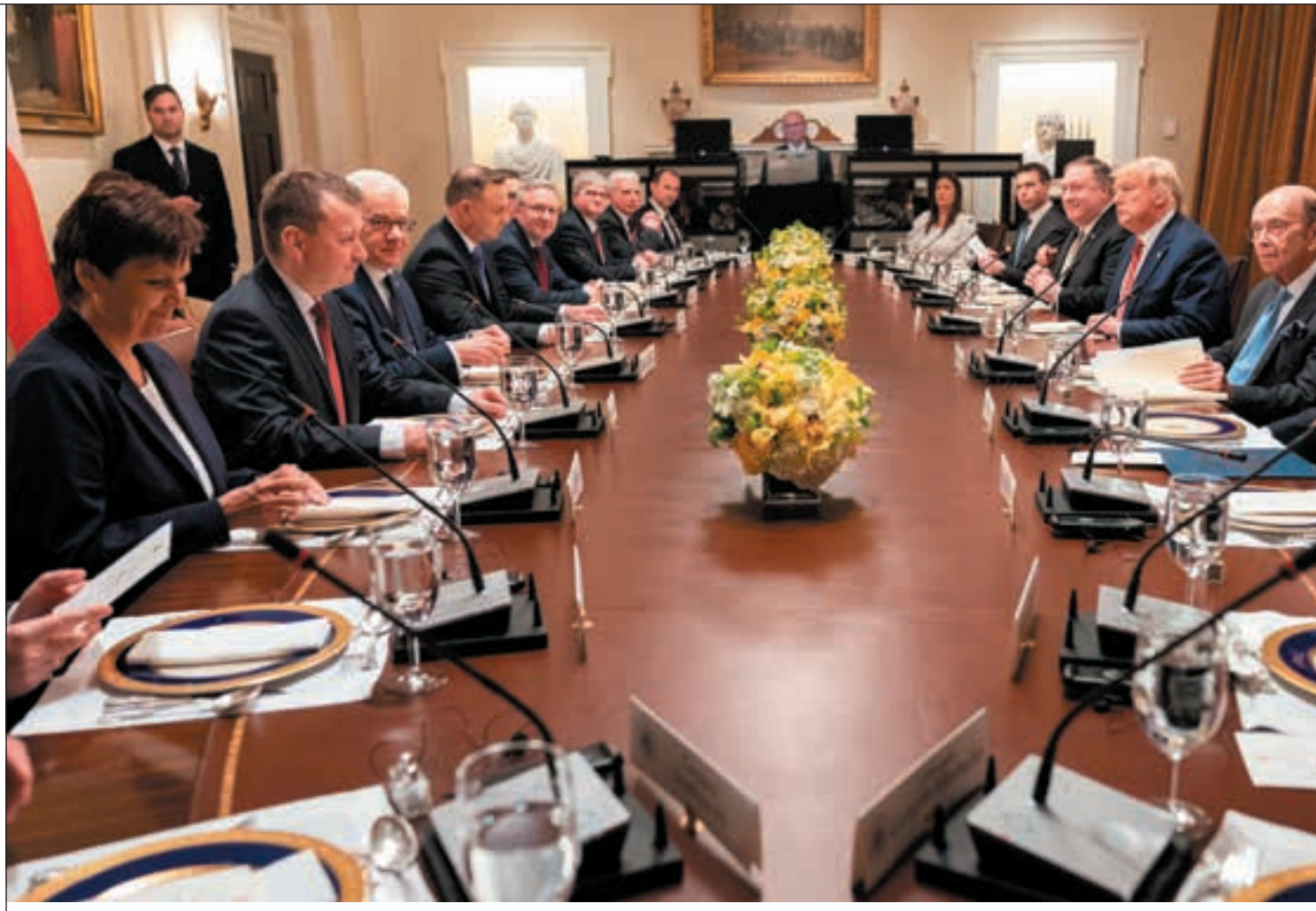
eskan™

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**



Picture credit: US Dept Defense

SEARCH AND DESTROY

Paul D Turner *explains the importance of Visible Light Communication when it comes TSCM*

Like all modern communication technologies, there are generally powerful security features and built-in safeguards that tend to provide a reasonable measure of technical security. However, threat actors have a nasty habit of finding and exploiting direct and indirect technology weaknesses, and finding inherent vulnerabilities that are often unrelated to the specific technology by exploiting other aspects of the overall system.

Optical threats are no exception and may include large window surfaces, gaps, openings and intercept technology. An array of human-factor issues relating to the improper deployment of the Visual Light Communication (VLC) technology; from an installation, setup and programming perspective, including physical security access vulnerabilities to critical infrastructure are problematic.

On another level, the compromise of input and/or output data streams and access to the underlaying driving technology is possible; bypassing an otherwise secure system. The vast majority of optical detection countermeasures devices are impactable to deploy effectively on more than one deployment perspective. Most optical detection devices fail to address the complexity and precision of the deployment detection methodology that is required to conduct a competent optical inspection within a TSCM role.

In a historical perspective and unfortunately, often by design, most optical countermeasure detectors fail to provide any measure of practical operator deployment-friendly features. As a result, any meaningful deployment strategy beyond the detection limitations suffers in practice. In this light, the remainder of this article will

It is vital that proper checks are carried out before any meeting likely to include sensitive information

focus on introducing a competent operator-centric detection strategy.

OPTICAL INSPECTION PROCESS

Initially, the technical operator should consider setting up an appropriate SDR radio near the centre of the Operator Defined Target Area (ODTA) at table or desk height (facing upward) for an occupied work space and on the floor in an unoccupied space. The radio needs to sweep down to at least 9kHz. The software must allow runtime and demodulation, including real-time intermediate broadband (IFB) operation.

The optical probe technology can be deployed stationary on a laptop computer or deployed as a walk-about resource on a mobile tablet computer. The physical size of the ODTA will need to be considered in order to determine the required or recommended number of stationary collection points, similar to the radio-frequency collection process utilised in a differential signal analysis role. Small work spaces of up to approximately 350 feet^2 can generally be treated as a single collection point, utilising the optical sensor probes directional capability, across a methodical and highly organised search pattern. The time-on-target required is dictated by the perceived or determined threat level assessment and the nature of the critical infrastructure under inspection.

Multiple passive optical sensor probes can be cascaded to expand directional variation coverage across the ODTA. Connecting the optical sensors to suitable SDR radio, using a low-noise RF coaxial cable provides the necessary signal-level detection capability. A slightly reduced optical sensor probe sensitivity may be realised with cable lengths beyond 3m if required, for specific infrastructure installation and deployment objectives.

The advances and usability of software-defined radio hardware and specialised TSCM software provides the needed conversion of optical signals to a baseband radio-frequency spectrum for capture, display and analytics. The process is to setup the software utilising pre-configured optical inspection profiles or to define a custom set of parameters unique to the assignment. Once the setup is accomplished, it is possible for the operator to enter a runtime collection environment at the software level by selecting the spectrum band tab, directly representing the optical spectrum profile.

RUNTIME DEPLOYMENT OPTIONS

There are several methods available to the technical operator that can be employed to undertake both a fast search and a comprehensive (recommended) optical inspection manually. The technical operator can utilise a differential signal analysis process to directly compare historical trace information with the current runtime capture to maintain a managed optical reference database capability. The technical operator can capture a series of reference traces within a single-location runtime environment. This method of deployment builds a dedicated series of reference traces that can be stored and recalled as powerful comparative peak optical references spectra data, representing each phase of the optical detection process.

A comprehensive, methodical search technique is required to identify somewhat illusive optical emanations. In particular, those that are threat actor periodic, on-demand focused or highly directional in nature.

Multiple optical sources "sum" make separation of friendly and potentially hostile signals extremely difficult. A standards-based and methodical approach is required, given the optically high-dispersion factor and therefore, low apparent power of typical digital LIFI and other potentially "summed" optical emissions that may be present. The operator's decision to deploy one detection process over another is firmly based on the available time-on-target, the assessed importance based on the threat level determined, operator preference, knowledge and experience relative to the OTDA.

A METHODICAL SEARCH TECHNIQUE IS REQUIRED TO IDENTIFY ILLUSIVE OPTICAL EMANATIONS

It is the hardware that provides significant deployment advantages for the operator, who can select the best radios for radio-frequency work and simultaneously handle uniquely and separate functions like power line and optical analytics during the same runtime environment across multiple radios or a single radio environment. Equipment resources that fail to provide this essential level of deployment integration are simply obsolete by today's standards-based, modern-moving target threat model.

MANUAL SEARCH OPERATION

It is essential that the technical operator provide sufficient time-on-target. Optical searches are time intensive and the operator should consider dedicated time-on-target apart from the normally required inspection protocol. The operator can establish a runtime session by selecting a pre-defined spectrum profile and methodically paint the room with the optical sensor probe, watching for spectrum changes across the sweeping profile or real-time Intermediate Frequency Broadband (IFB) option. It is recommended that the technical operator import a previously captured reference trace file into the software as a direct comparative for the specific room-level ODTA. This level of inspection is essential in identifying possible hostile Technical Surveillance Devices (TSD) that might be deployed to intercept room level audio or data sources, without the presence of the more easily detected radio-frequency signatures.

A search from the centre of the room (upward), is best practice for LIFI emissions, however, direct LOS emissions are best identified by selecting logical positions to intercept emissions that might be directed out of the room via windows or gaps, *etc*. Detecting passive laser attacks is best accomplished with the sensor probe facing the windows and away from the windows, looking for modulated laser reflections from room-level objects.

DIFFERENTIAL SIGNAL ANALYSIS

A standard and perhaps familiar location-based deployment strategy can be utilised to capture any number of in-depth comparative optical focus traces. Each additional capture location can reference the sensor probe direction. It is recommended that the operator capture a baseline reference trace by completely shielding (covering) the optical sensor probe. The operator can then setup and capture a second software

location, perhaps with the ambient room-level lighting off and another location with the lights on. This process, creates a baseline of any ambient optical interference or noise emissions. There will always be natural and artificial ambient optical noise to consider. The largest source of artificial optical noise results from the room-level lighting. Different lighting sources respond uniquely and must be taken into consideration by the operator in determining the presence of "summed" emissions from hostile optical threat technology.

THE TECHNICAL OPERATOR SHOULD SET UP AN SDR RADIO NEAR THE CENTRE OF THE ODTA

Separate location-based traces can be captured for upward, downward, north wall, east wall, south wall and west wall; above any dropped ceiling and below any sub-floor structure. The differential deployment method provides an extensive, well-documented process for high threat assignments; for evidentiary purposes and to facilitate analytical operator review.

CASCADING (RF + OPTICAL) DETECTION

The advantage of software-defined radio is a unique and innovative ability to provide cascaded deployment for optimal real-time Optical Spectrum Surveillance and Monitoring (OSSM). A single optical sensor probe can be deployed for small spaces and multiple optical sensor probes can be deployed for larger spaces. Multiple, passive optical sensor probes can be electronically combined, utilising a suitable power-splitter technology, to increase room-level sensitivity and detection exponentially and better facilitate simultaneous, multi-directional coverage.

Advanced support extends to simultaneously combining and capturing both radio-frequency and optical signals across any number of multiple spectrum bands, utilising software-defined radio, multiple-band capability across a single radio. A power-splitter can be utilised to simultaneously capture radio-frequency via spectrum band separation using any passive RF antenna and simultaneously process the received and combined optical signals from the optical sensor probe, and both the radio-frequency and optical spectra can be displayed on separately defined spectrum bands at the software level.

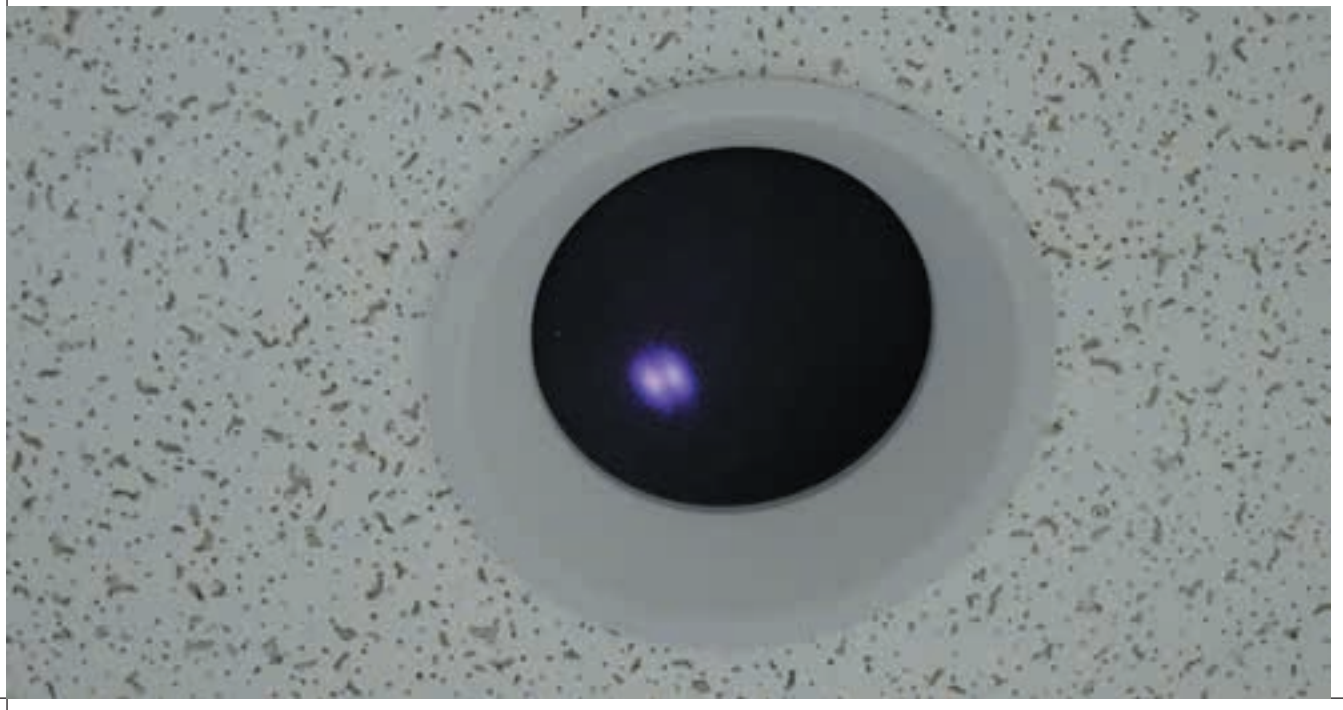
Multiple radio, multiple band operation is a powerful feature and supports combined simultaneous capture of RF, optical and facilitates power line analytics. The ability to cascade optical + optical, radio-frequency + radio-frequency, radio-frequency + optical and radio-frequency + power line is a powerful and innovative technology milestone. This level of diversity qualifies as a standards-based deployment process in support of live event monitoring and autonomous, extended Remote Spectrum Surveillance and Monitoring (RSSM) and Optical Spectrum Surveillance and Monitoring (OSSM) techniques; easily accomplished in a highly-scalable deployment process, providing an agile and highly focused collection platform.

IQ RECORD AND PLAYBACK

Software defined-radio provides an industry-unique TSCM ability to capture and playback IQ samples for post analytical analysis and review. IQ capture is an essential TSCM capability at all operational threat levels. IQ record can be used to capture a sample IQ file for detected optical emissions during the demodulation process and is used for signal-level analytics. The software must provide the ability to support a variety of IQ capture and playback formats. IQ based Time Reference Sub-Sampling (TRSS) provides a powerful editing resource to achieve analytical efficiency.

In conclusion, cascaded passive optical sensor probes deployed directionally across individual operator-defined target areas; utilising software-defined radio technology advances the probability of detection within a modern moving-target threat model. It is vital that operators seek professional training to better understand the importance of optical detection within a TSCM role ●

Paul D Turner, TSS TSI is the President/ CEO of Professional Development TSCM Group Inc. and is a certified Technical Security Specialist (TSS) and Technical Security Instructor (TSI) with over 40 years of experience in providing advanced certification training, delivery of TSCM services worldwide, developer of the Kestrel TSCM Professional Software and manages the Canadian Technical Security Conference (CTSC) under the operational umbrella of the TSB 2000 (Technical) Standard.



Infrastructure LIFI device image taken with camera with its IR cut filter removed so that the illuminators that aren't visible to the human eye (the purple spots) can be seen

Picture credit: TSCM Group Inc

NEW TTK TACTICAL TSCM KIT

Compact, Portable, Tactical

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

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

**Kit contents may vary*

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

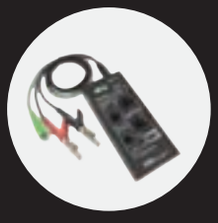
lbs/kg

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

MESA® hand-held Spectrum Analyzer

ANDRE® Broadband Detector

ORION® 2.4 HX
Non-Linear Junction Detector



CMA-100 Countermeasures Amplifier

Picture credit: Marshalls Landscape Protection

PROTECT DUTY

Paul Haggerty *looks at the results of the UK Government's consultation on the Protect Duty and what the planned legislation will mean for businesses.*

With a number of high-profile terror attacks in the UK in recent years, in February 2021 the Government launched a public consultation on the implementation of a legal 'Protect Duty' for public places. In particular, the type of attack carried out at the Manchester Arena in May 2017, which killed 22 people and injured hundreds more, was a focus of the consultation. In both the initial consultation document and the Government response published in January this year, the attack is mentioned as well as the Martyn's Law campaign that followed, named after Martyn Hett, one of those who died.

These attacks present an ongoing threat to public safety in the UK. The initial Protect Duty consultation notes that between March 2017 and February 2021, the UK police and security services stopped 27 plots. The response document opens by noting that in the less than one year between the publication of the two documents, four additional plots were stopped, but sadly two attacks had been carried out, one of them claiming the life of the MP Sir David Amess in his Southend constituency.

There is currently no legislative requirement for businesses and other organisations that operate in the publicly accessible spaces to protect people from deliberate attacks or even the dangers posed by accidental vehicle collisions. There are small exceptions

Protective versions of planters, seats, cycle stands and litter bins can be used to discreetly provide hostile vehicle mitigation

to this, such as security for transportation and some sports grounds. When made law later this year, as the Government has pledged, the Protect Duty legislation will be the first of its kind in the UK to apply to the vast majority of public spaces.

In the statement that accompanied the publication of the consultation response document, Home Secretary Priti Patel said the legislation will aim to: "strike the right balance between public safety, whilst not placing excessive burden on small businesses". This should be encouraging news for businesses concerned about the financial burden that this may place on them.

The consultation, which sought views from all groups that a 'Protect Duty' would potentially affect, including organisations who own or operate at publicly accessible locations, covered four key areas: where should legislation apply, what should the requirements be, how compliance should work and how Government can best support and work with organisations. There were several key points from the consultation that should be highlighted.

The first thing to note is that the idea of introducing a Protect Duty was strongly supported in the consultation, with 70 percent of respondents agreeing that those responsible for public locations should take appropriate measures to protect the public from attacks. As defined in the consultation, a publicly accessible location is: "Any place to which the public or any section of the public has access, on payment or otherwise, as of right or by virtue of express or implied permission".

This covers a range of locations including high streets, parks, beaches, public squares, retail stores, shopping centres and markets as well as hotels, pubs, clubs and bars. Schools, universities, hospitals and places of worship are also included under this umbrella as well as music venues, festival grounds and sports stadia.

Based on the responses to the consultation, it seems likely that a large number or even all publicly accessible locations will have some degree of responsibility under the Protect Duty legislation. In the consultation, when asked which specific places a Protect Duty should apply to, many suggested: "all publicly accessible locations" or: "all locations in general". In addition, the majority (58 percent) said there should be no exemptions to the Protect Duty. This would seem to align with the sentiment shared in the introductory section of the document that reiterated that attacks cannot be predicted and could occur at any location, making them difficult to prevent.

However, the consultation also asked for views on setting criteria to decide which venues the duty should apply to. The capacity of the venue was the most popular, with other factors also suggested such as the evaluated risk of the location, the geographical location (such as in a rural area) and the type of event being held at the venue. Additionally, the idea of using the average, rather than maximum, capacity of the venue as the criterion was also put forward.

The exact requirements of the legislation have not yet been defined. However, it is clear that the overarching focus will be on ensuring that organisations carry out risk assessments to evaluate their vulnerability and then take action to mitigate these risks. This includes training staff to identify potential threats and respond correctly as well as implementing effective and appropriate physical security measures. It is also clear that as a legal requirement, organisations will have to demonstrate compliance or incur penalties.

The statement issued by the Government alongside the consultation response explained that the Home Office is working with the National Counter Terrorism Security Office (NaCTSO) and Pool Reinsurance to create a new interactive online service. The platform, which is scheduled for launch later in the year, will provide a central hub for advice, guidance, e-learning resources and other relevant content. It is intended to provide support for all organisations in creating a safer environment, whether or not the Protect Duty applies to them.

ORGANISATIONS WILL NEED TO CARRY OUT RISK ASSESSMENTS AND TAKE APPROPRIATE ACTION

One of the key themes of the Protect Duty is that measures should be appropriate, proportionate and affordable. In effect this means that smaller organisations and venues will not be expected to implement the same level of security as larger organisations. For example, with regard to physical protection, there are costly and complex options that might be necessary for larger venues or higher risk areas but are excessive for smaller organisations.

A further important part of the legislation is likely to be collective duty if there is shared responsibility for a venue or multiple organisations operate within an area. More than 80 percent of respondents in the consultation agreed that where this is the case, the parties should collaborate to meet the Protect Duty requirements.

For many businesses and organisations, adopting a collaborative approach may help to reduce the financial burden and lessen the impact on customers, visitors and staff. Take for example, the implementation of hostile vehicle mitigation (HVM) measures in a pedestrianised street where multiple shops, restaurants or cafés operate. It will often be easier, more cost effective and less obtrusive to introduce protective features at each end of the street than try to protect each business separately.

An important element for any organisation addressing the Protect Duty requirements will be the evaluated risk of its location. A place where people are dispersed across a relatively large and open space may be considered a lower risk than a location where people are concentrated into a smaller area. Also, certain types of buildings or areas of a structure may require additional protection, such as data centres or server rooms.

For this reason, working with specialists to meet the requirements is important. They can provide advice and guidance on designing a strategy that is appropriate based on the risk assessment. For example, if the layout of a street makes it unlikely or impossible for a large vehicle to approach the area,

then HVM features that are designed and tested to stop a smaller vehicle may be suitable instead of those engineered for larger 7.2 tonne vehicles and are therefore more expensive.

For many businesses, the Protect Duty will not require a completely new approach, but an enhancement of what is already in place. Of those who responded to the consultation and are working in an organisation that would come under the protect duty, 50 percent already undertake a risk assessment for terrorism, with 83 percent of that group carrying it out in-house. Also, the majority (78 percent) said they already review this risk assessment at least once a year.

ORGANISATIONS WILL HAVE TO DEMONSTRATE COMPLIANCE OR INCUR PENALTIES

One important element of the Protect Duty that has not received attention in the discussion around the consultation is the other benefits that implementing these measures will have. In particular with regard to physical security. Protective barriers and other features designed to prevent attacks will also help to minimise the risk from accidental hazards such as out of control vehicles.

One challenge when making public places safer is to do so without affecting the operation of the site or the experience of visitors. It is also important to avoid making people feel unsafe by giving the impression that the area is heavily defended. One possible solution is to replace features such as street furniture with security versions. For example, protective versions of planters, seats, cycle stands and bins can be used to discreetly provide hostile vehicle mitigation while maintaining the design intention for the area. Often there will be a relatively small cost difference between standard and protective options.

GET PROACTIVE

In addition, for businesses that do need to implement additional measures, it is important to do so in the most cost effective way. As mentioned above, working with specialists to find the most appropriate solutions is a key part of this, but being proactive and looking ahead is also essential. If a new project or refurbishment is currently underway it may be valuable to look at how additional measures can be integrated now rather than retroactively when the Protect Duty becomes law. Physical barriers will often require reinforcements to be sunk into the ground and it will be more cost effective and less disruptive to do this during the initial construction activities.

Similarly, if a refurbishment is planned for the near future it may be best to wait until then to implement any permanent changes. In the meantime, effective temporary measures can be used to fulfil the requirements of the Protect Duty.

Terrorist actions are unfortunately not a new occurrence in the UK, but the events of recent years have underlined how important it is to make public spaces as safe as possible and the Protect Duty legislation will be a key part of this. By utilising the publicly available resources, approaching the requirements strategically, engaging with specialist partners and carefully considering the most appropriate solutions, businesses can ensure they comply with minimal financial impact or disruption to operations ●

Paul Haggerty is the Hostile Vehicle Mitigation Business Development Manager for Marshalls Landscape Protection and has more than a decade's experience in the protection of public spaces.

One challenge when making public places safer is to do so without affecting the operation of the site or the experience of visitors

Picture credit: Marshalls Landscape Protection

Kestrel TSCM ® Professional Software

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

Signals Intelligence Support System ™

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

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

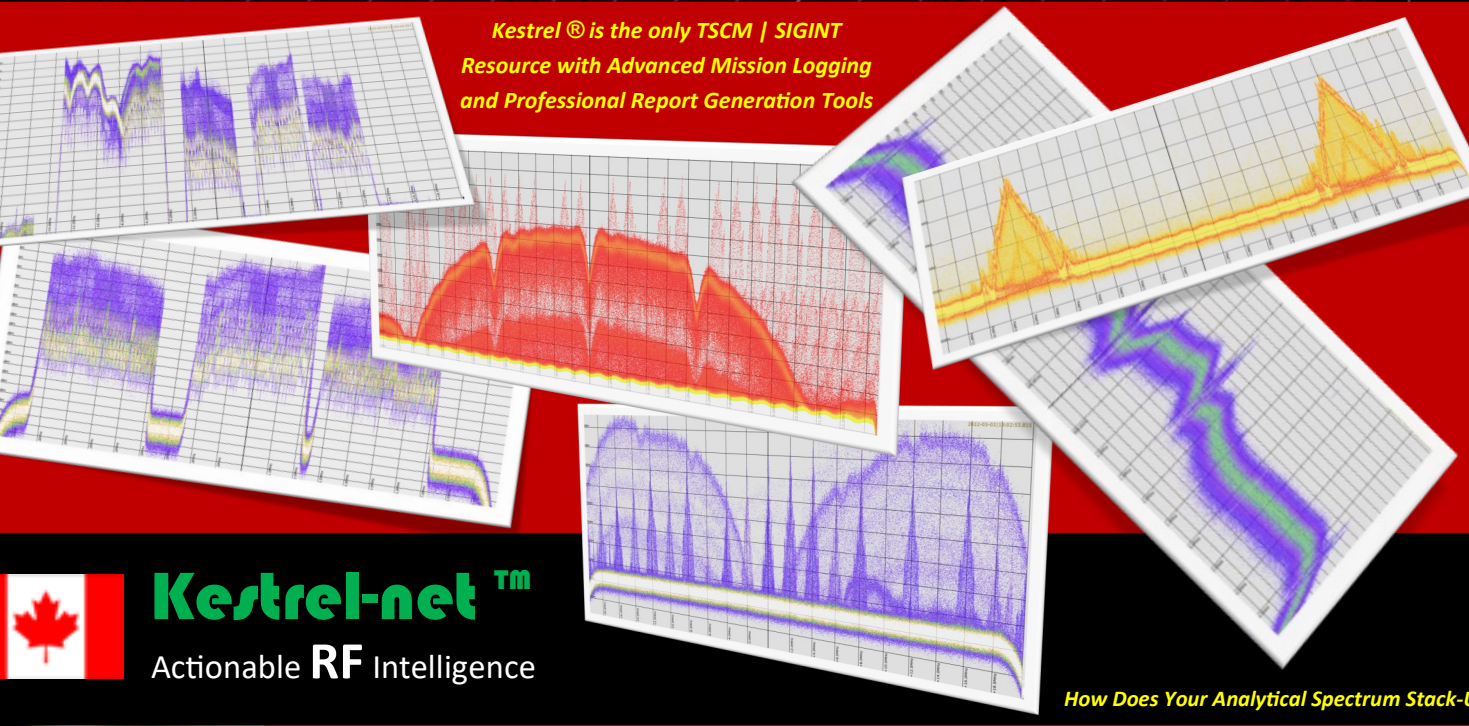
Kestrel TSCM ® Professional Software

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

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

The Kestrel TSCM ® Professional Software is by Definition and Reputation the Leading Next Generation, Mission Critical TSCM | SIGINT Technology for Scalability, Flexibility Ease of Use, Low Procurement Cost and Powerful Near Real-Time Deployment Ready Modern Features that Address Today's and Tomorrow's Emerging Threat Technology

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



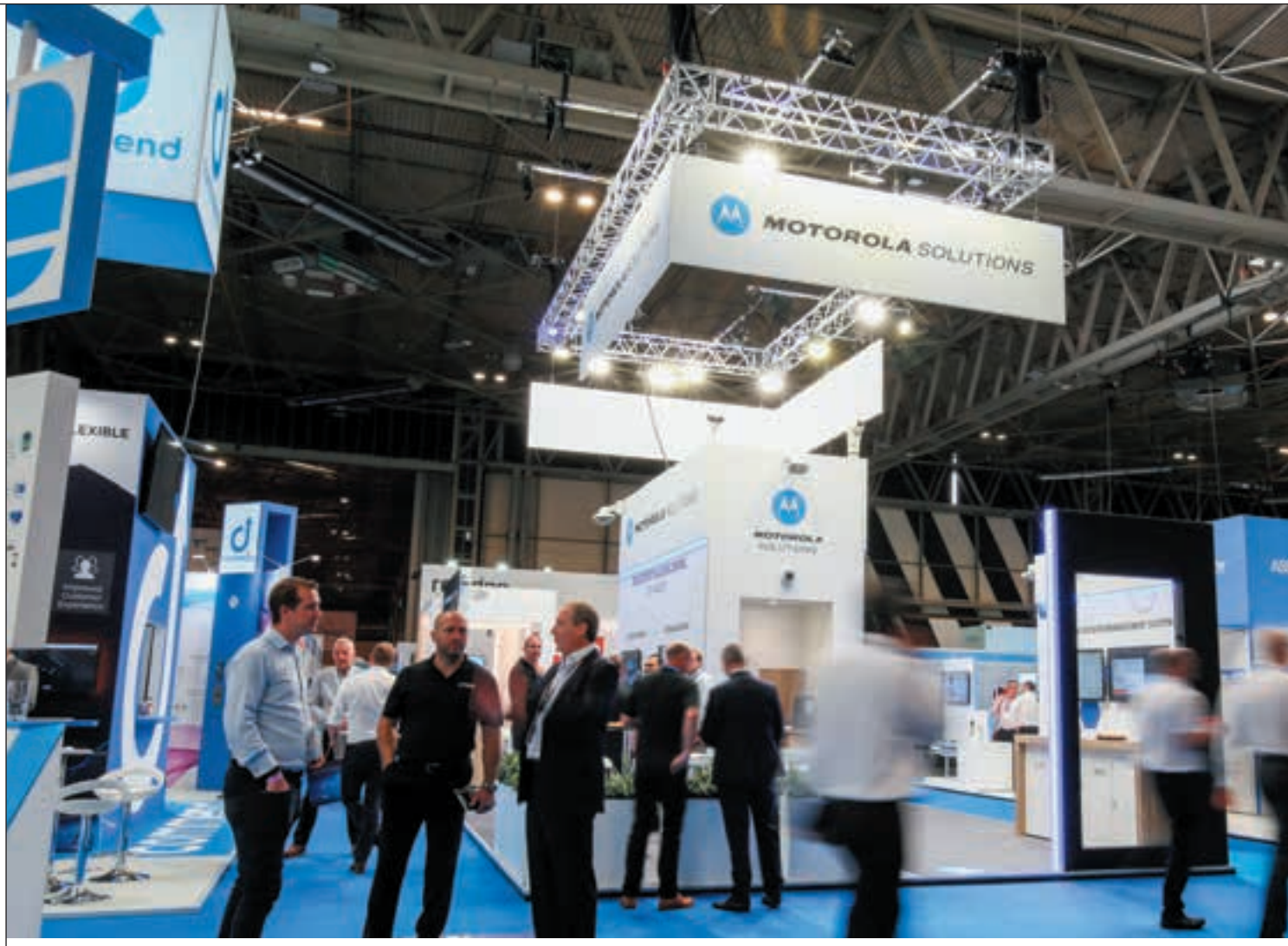
Kestrel-net ™

Actionable **RF** Intelligence

How Does Your Analytical Spectrum Stack-

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

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



THE SECURITY EVENT 2022

The Security Event is back and bigger than ever!

The Security Event (TSE), the UK's number one commercial, enterprise and residential security event returns back to its natural home – the NEC Birmingham – on 5-7 April 2022. This year's event is set to bring even more product exclusives and launches of the latest security products and solutions, 50+ hours of CPD content, live demonstrations and workshops, plus a host of networking opportunities across the three days.

SHOW EXCLUSIVES AND LAUNCHES

Spearheaded and supported by its Founding Partners – Anixter, ASSA ABLOY, Comelit, Honeywell, TDSI, Texecom, Tyco and Videcon – who will be exhibiting some of their latest launches, products and projects that are revolutionising the sector right now. Event exclusives will include TDSI showcasing its latest update to its GARDiS integrated access management software solution, ASSA ABLOY's next generation of digital access control and cloud technology and Comelit-Pac exhibiting for the first time since its acquisition presenting its all-encompassing door entry, access control, CCTV and compliant fire safety systems, and much more. This is in addition to the 200+ exhibitors that will be joining its roster this year.

The show has grown threefold since its launch in 2019 and covers a massive 11,000+m² at the NEC. Delegates will also see 100+ brands such as ADI Global, Aritech, Calipsa, CheckMySystems, CIE Group, CDVI, Deister Electronic, Fermax, Gallagher Security, GJD, Hytera, ICS Security, Oprema, Optex, QED, Reconeyez, Risco, Secure Logiq, Winsted, ZKTeco plus many more, as well as Aiphone, Golmar, Hanwha Techwin, Ksenia Security, Lenel, Veracity,

The Security Event brings together the best installers, integrators, manufacturers, distributors and end users in the business

WEC CCTV and many others who will be making their debut for the first time in the UK and will not be exhibiting at any other trade show.

INDUSTRY UPDATES AND GUIDANCE

Revamped and tailored to upskilling and providing the latest insight on the security sector, The Security in Practice theatre sponsored by Cloudview returns with a fresh new concept of topical themes and sessions. The highly focused programme will investigate the evolving challenging and opportunities involved in the delivery of security projects throughout the supply chain including topical themes such as:

Case Study – Commonwealth games – Shining the spotlight on the biggest sporting event in the country, hearing from industry experts and the personnel behind the event on what it takes to organise a large-scale event, looking at the key considerations and measures to keep venues, employees and the public safe.

The new 'Protect Duty' – With the introduction of the new Protect Duty, experts will delve into what this means for security professionals and the responsibilities that lie ahead to deliver, manufacture or install. Hear from speakers involved in both the campaign and implementation of 'Protect Duty'.

Regulations – 2022-2023 will see major regulatory changes for security professionals and businesses. Topics will include the rules of 'Protection of Freedoms Act' and the implications of CCTV and biometrics devices, the regulatory rules on and around cyber and countering the cyber threat, and much, much more.

Specially curated for the needs of fire and security installers and integrators, we will also see the return of the Fire & Security Installer Theatre sponsored by Resideo – which in partnership with NSI will provide important updates and guidance for practitioners and business owners. With a focus on standards, regulations and industry best practice, these sessions will be vital to ensure businesses remain compliant and are best equipped to meet the needs of their clients.

KEY SESSIONS INCLUDE:

CROSS – Collaborative Reporting for Safer Structures
BS 8418:2021 for Detector-Activated Surveillance Systems – The Game Changer For Police Response
Cyber Security – are security systems affected?
Fire system installation quality, takeovers and verification
Automatic Opening Smoke Vents – Are You Compliant?

INDUSTRY SUPPORT

In partnership with Police Crime Prevention Initiatives, run in association with Secured by Design and Police Crime Police Academy (PCPA), the hugely popular 'Designing Out Crime' zone will showcase the latest police techniques to reduce crime and keep local communities safe. Visitors will be able to discover the pioneering work that has been undertaken to raise the security standards and the practices of designing out crime within planning procedures as well as being able to attend a series of content sessions. Sessions include:
Alarms -Project ECHO & The New SBD Alarm Standard
PANEL SESSION: How can the Government best approach future threats that are on the horizon?

PCPA Snapshots: How can you access police qualifications through the Police Crime Prevention Academy?

INTERNET OF THINGS AND YOU!

CSAS – Community Safety Accreditation Through Police and Private Security Collaboration

The Security Institute will be hosting a new networking lounge where the team will be on hand to provide the tools and opportunities to further your career. Facilitating a number of specialist interest workshops throughout the three days, they will be inviting fellow members and guests to share their experiences and to grow their professional network.

Dedicated to driving industry standards and guidelines, specialised training and certifications to advance security in the UK and beyond, ASIS will also be onsite with its dedicated lounge providing the perfect forum to connect and build a network of support.

NEW! HOSTED MEETINGS PROGRAMME

New for 2022, visitors will be able to benefit from a new hosted meetings programme – CONNECT+ Live. Matching the visitors' buying requirements and needs with carefully selected exhibitors, their team of match-making experts will help delegates fast-track access to suppliers, providing a more exclusive and concierge service. A dedicated meeting lounge will be onsite, providing even more added benefit to the visitors.

NETWORKING

Back by popular demand, The Security Event will be hosting two networking reception drinks from 16:30 on day one and day two. With a host of networking initiatives in and around the show throughout the three days, the reception drinks is the perfect opportunity to unwind and meet with your peers, colleagues and friends in a relaxed and informal setting.

CO-LOCATED EVENTS

As part of the Safety & Security Event Series, The Security Event will once again be uniquely co-located with The Fire Safety Event, The Health & Safety Event and the new relaunch of The Workplace Event, formally known as The Facilities Event. Covering the entire buying chain of the safety and security of property, people and assets, visitors will be able to attend all four events and access over 1,000 exhibitors and CPD content for FREE.

Don't forget, there is FREE PARKING for all visitors!

For more information or to register for your FREE visitor pass visit: thesecurityevent.co.uk

TIME TO UPSKILL?

James Hadley *reveals why the defence sector must optimise its workforce with cybersecurity upskilling*

We know that a single phishing email is all it takes for bad actors to launch an attack that could take down a multi-billion-dollar enterprise. This is one of the reasons cybersecurity professionals often talk about humans as a weakness in the defences of otherwise well-protected organisations. We disagree. In fact, humans are not a security liability but an untapped defence asset.

We believe that a workforce can be optimised to become the ultimate defensive asset, with every single member of staff empowered with the skills, knowledge and judgement to tackle new and emerging cyber risks. Today, advanced simulations available in web browsers offer the ability to develop the cyber capabilities of every staff member. When simulations are built to reflect realistic environments and updated to reflect a changing threat landscape, they offer an unparalleled way of battle-testing resilience and preparing for emerging risks. Simulations are one part of a wider cyber optimisation strategy that develops capabilities across an organisation.

Immersive Labs recently announced that it is working with the British Army to continuously assess and optimise the cybersecurity capabilities of its entire workforce. Like any organisation, the Army can improve every aspect of its capabilities by focusing on the security skills of human employees, from soldiers fighting on overseas battlefields to digital deliverers or technical specialists working behind the scenes here in the UK.

Upskilling the British Army sets an example for the wider defence industry – as well as other sectors. Here, we will set out the argument that exposing staff to cyber workforce optimisation is the best way to prepare them for battle in the cybersecurity arena. Arm all human employees with the right cyber skills and they can all do their bit to defend every organisation they work with.

Traditionally, it was the job of the IT department to face down threat actors and mitigate cybersecurity risk. Today, everyone should be involved. When an adversary is looking for a way into a target network, they do not distinguish between ranks or divisions, but simply search for any method of achieving their goal.

In an era when everyone within an organisation is a target, it makes sense to argue that all members of staff can play a part in mounting a defence. Once an organisation has made this shift in thinking and started to recognise the role every employee, team or department can play in both risk and resilience, it must set about developing the individual skills of each person.

The first step in making the transition to a better security posture is an honest, in-depth assessment of cyber capabilities. Older methods of proving cyber resilience could include an external audit, which tend to be paper-based examinations of an organisation's ability to cope with a particular range of threats. These legacy techniques are now inadequate. They are static snapshots that cannot hope to stand up against the ever-changing threat landscape. They are unable to measure individual proficiency or assess important aspects of resilience, such as the ability of staff members or full teams to cope with a crisis or deal with a new situation that has never been faced before.

Certification schemes have a similar weakness. They offer accreditation that relates to a point in time, without measuring performance related to emerging threats. Classroom exercises are also insufficient, once again passing on lessons that relate to dealing with one threat and exposing staff to unengaging race-to-the-finish content.

UPSKILLING THE ARMY SETS AN EXAMPLE FOR THE WIDER DEFENCE INDUSTRY AND OTHER SECTORS

These methods of assessment are slow to adapt and hard to scale. They cannot be measured accurately and are limited in their breadth. Without data on the ability of the teams and individuals to respond to cyber risks and no way of building knowledge, skills and judgement at pace and scale, resilience is unachievable. When an organisation is reactive, exposed and on the back foot, its confidence in cyber risk mitigation is diminished.

A reliance on technological solutions is also not enough. While they can operate extremely effectively when faced with old or known threats, if the situation changes the tech is rendered temporarily

Picture credit: US Dept Defense

Like any organisation, the army can improve every aspect of its capabilities by focusing on the security skills of its employees

ineffective as vendors rush to issue patches and fixes. What organisations need is a way to gain a broader and deeper view of human cyber capability across all departments. This can be achieved by exercising cyber workforces to produce insights, which can then be used to reduce the risk of attacks of breaches originating from inside or outside the business. This data can also be deployed to provide evidence of an entire organisation's cyber resilience at any given moment and used to form board packs, reduce insurance premiums and improve security or credit ratings.

To begin turning its staff into a defensive asset, an organisation must first move beyond a one-size-fits-all approach towards a new paradigm, which not only continuously assesses human employees' skills and knowledge but also their ability to make decisions and judgement calls in the heat of the moment.

The use of targeted, updated simulations offers the ability to gain visibility of an entire organisation's cyber resilience. By exposing every member of staff within an organisation to realistic simulations, which mimic the real-life situations that they are likely to face, a realistic picture of risk can be created. Data gathered during simulations can be analysed to reveal granular details of weaknesses or points of strength, allowing decisions about further exercising to be made in the most informed way possible.

The upskilling process should follow a strategy which can be summed up in three parts: exercise, evidence and equip.

Firstly, teams and individual members of staff should go through realistic exercises that are role-specific yet incorporate cross-organisational aspects to mimic an incident that has impact across the entire organisation. These exercises should be adapted to reflect the nature of the organisation involved, as well as the current threats. In a defence industry context, a simulation could focus on a scenario in which criminals have stolen classified secrets. Participants could also undergo an exercise that evokes a situation in which nation-state threat actors have launched a devastating ransomware attack.

After exercise comes evidence. Data gathered during the exercise should be used to demonstrate confidence in cybersecurity or discover risk levels across all business functions. When simulations are performed regularly, data can be mapped against industry-standard frameworks to provide a real-time picture of risk.

Finally, the evidence can be used to equip individuals and departments with the knowledge, skills and judgement needed to tackle cybersecurity threats they are likely to face while working in their role. All data points can be benchmarked against peers or mapped against accepted cybersecurity frameworks. Senior leaders can also use the insight to make better-informed operational decisions and strategic investments.

Simulations are not a 'one-and-done' exercise. When using a cloud-based simulation platform and repeating the exercises, data can be continuously

generated. A cyber workforce optimisation solution should also collate insights and deliver quantitative analysis and visualisations of capability, expertise, confidence and improvement in individuals and teams.

Simulations and realistic exercises offer other benefits. If job applicants undergo simulated scenarios during their applications, they can be hired based on their ability to do the role, rather than previous experience, academic qualifications or professional certifications. This addresses the problem of unconscious bias in hiring and can drive increased diversity across security roles. It helps to identify untapped talent, improve social mobility and help neurodiverse individuals during job application processes.

HUMANS ARE NOT A SECURITY LIABILITY BUT AN UNTAPPED DEFENCE ASSET

We use the phrase cyber workforce optimisation to describe the continual testing, measurement and improvement of cyber knowledge, skills and judgment. Cyber workforce optimisation is a philosophy that focuses on upgrading each member of staff. It grants organisations the ability to test every aspect of their defence, ranging from the performance of incident response teams to the ability of non-technical staff to play their vital roles in preventing and responding to an attack.

The constant evaluation offered by a cyber workforce optimisation solution can be used to prepare for landmark events such as meeting the regulator or speaking to the board, providing actionable, understandable data that is real-time evidence of the organisation's efficiency in dealing with cyber threats, compliance and strategic security risks. These data-driven insights can then enable an agile cycle of development, which improves cyber capabilities across the organisation. Staff may even enjoy the exercises and simulations, meaning they are much more likely to engage with the lessons and take on the best practices taught within them.

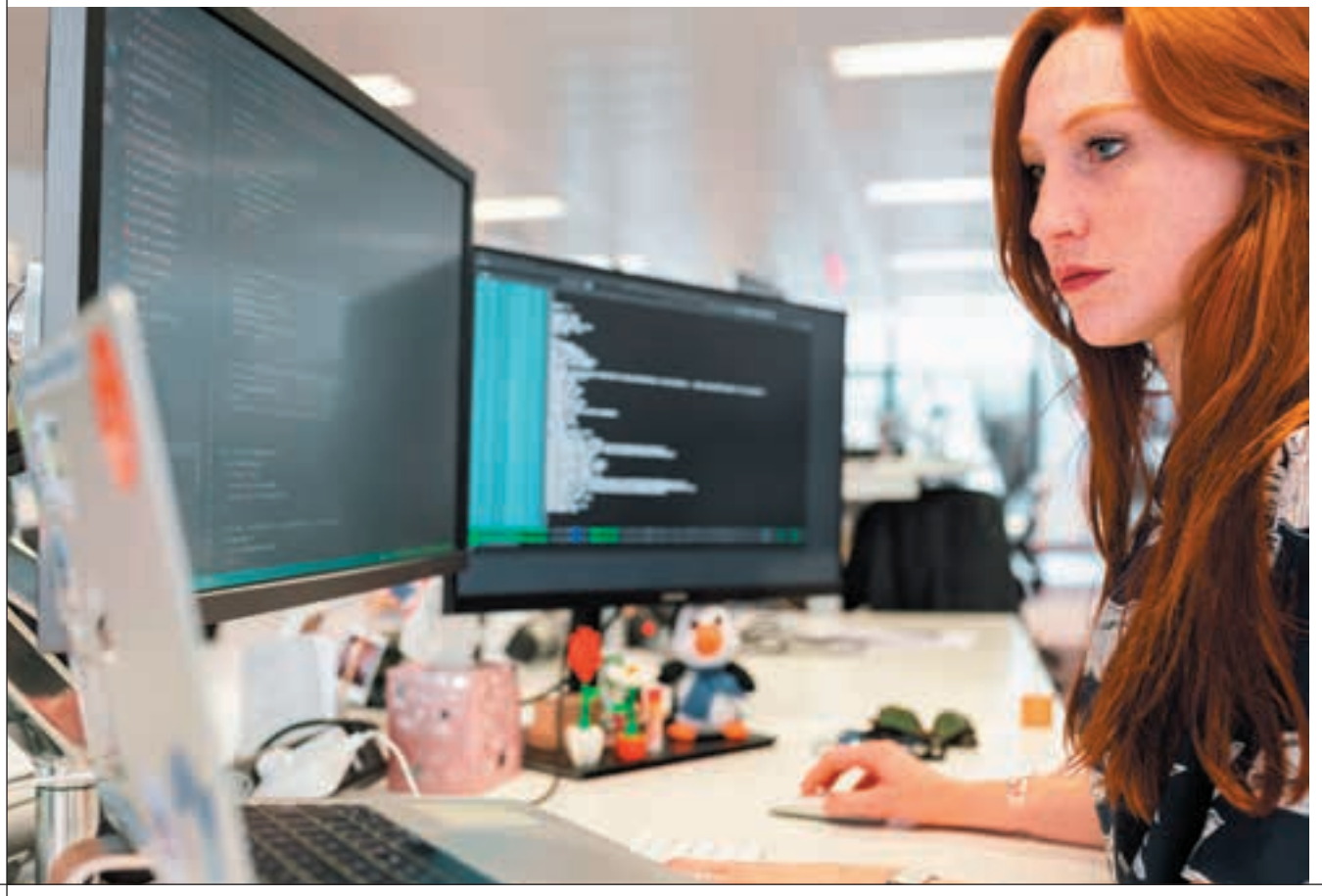
The defence sector is unique in the nature of its work. Yet it faces similar threats to any industry holding sensitive data or other information of interest to external threat actors. We know that nations including Russia, China and North Korea are always seeking opportunities to target the defence industry, whether it is to steal secrets, gain actionable military intelligence or simply cause damage. Cybercriminals are also looking for opportunities to make money.

When the stakes are high, the response must be appropriate. We have established that legacy methods of ensuring, proving and demonstrating resilience are ineffective. Traditional defences are suitable for known dangers of the past, but are unable to cope with a changing threat landscape and therefore cannot add to overall resilience.

Too many organisations in the defence industry and beyond are blind to their preparedness for the cyberthreats of today and have no way of demonstrating resilience. But leaders now have access to the tools to allow them to upskill and optimise their entire workforce, turning them into a valuable strategic asset. Optimise the workforce and together every member can build stronger defences ●

James Hadley is CEO of Immersive Labs.

Advanced simulations offer the ability to develop the cyber capabilities of every staff member



2022

EUROSATORY

13-17 JUNE 2022 / PARIS

THE GLOBAL DEFENCE & SECURITY EXHIBITION

SECURITY, A MAJOR COMPONENT OF THE EXHIBITION

86
Official Delegations
from security domain

725
exhibitors
with security activities

14
conferences
dedicated to security topics

30+
media partners
from this domain

The presence of **the Ministry of the Interior since 2014**

2 clusters
"Critical infrastructures and sensitive facilities security"
"Civil Security, crisis management and people security"

Outdoor live demonstrations by institutions: Prefecture de Police inter-services, RAID and GIGN

For the first time, **indoor live demonstrations** only dedicated to security

GICAT

www.eurosatory.com

COGES EVENTS

It’s An Open & Shut Case.

Introducing the new TTK Tactical TSCM Kit

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

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

*Kit contents vary

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

IPS

THE HALLMARK OF SECURITY

Looking For The Most Extensive Mobile Sweep Kit Available?

MACHINE LEARNING

Tim Wallen *discusses what is needed to lay the foundations for the success of next-gen cybersecurity technologies.*

The expanding scope and sophistication of cybercrime is a significant problem. When we hear the word 'cybercriminal', there's a tendency to picture a single individual hidden away in a dark dingy garage, operating from an old-school laptop. And while this may have once been the case, modern cybercrime looks entirely different.

Today we're faced with incredibly organised and highly sophisticated criminal operations backed by vast resources and often nation states. It is these networks that are intensifying the threat landscape, making cybercrime a much more real, fierce danger to organisations of all shapes and sizes around the world. You only have to glance at some statistics from 2021 to get a sense of the bigger picture.

According to IBM, the average cost of a data breach rose to $4.24 million in 2021 – the highest this figure has been for 17 years. Meanwhile, further research also shows that corporate networks saw a 50 percent increase in attacks per week when compared with 2020. Given the uptick in both the volume of attacks and associated damages, it should come as little surprise that a leading US insurance company paid out a record $40-million ransom last year after attackers stole the firm's data and blocked access to its network.

We're starting to see the true power of RPA and AI in predicting when and where attacks might happen

The unfortunate reality is that cybercriminals are continuing to be successful in their efforts, creating a snowball effect that is fuelling the determination of threat actors to innovate their attack methods in an attempt to secure lucrative rewards.

Resultantly, unprecedented pressures are being placed on cybersecurity professionals at a time when the sector is struggling with a severe skills deficit. Indeed, one report estimates that the number of unfilled cybersecurity positions grew from one million in 2013 to 3.5 million in 2021. Within this context, cybersecurity is always fighting an uphill battle. Attacks continue to come thick and fast and security professionals are forced to scramble in order to protect their systems wherever possible, forever playing catch up. Of course, this isn't a sustainable way to operate. It just takes one successful attempt for threat actors to succeed, and – operating under such stressful circumstances – security teams will sooner or later slip up.

Fortunately, to the benefit of many industries, technologies are beginning to mature and are now showing their potential in turning the tide in the fight against cybercrime. We're starting to see the true power of robotic process automation (RPA), machine learning and AI, not only in providing real-time insights but also in predicting when and where attacks might happen.

There is an argument to say that such technologies will be the only way to keep pace and counter the ever-changing methods of cybercriminals. It's not enough just to detect incidents anymore. Instead, a holistic approach is needed, and these advanced solutions are critical to achieving that.

Through AI and machine learning, automated threat detection and response can be achieved, taking much of the pressure off security teams in spotting and acting upon threats and incidents. Leveraging these technologies allows security teams to be fully armed and forewarned, facilitating transparency, enhancing clarity and reducing the potential for panic in critical moments. In other words, they can make security a much smoother, more seamless operation.

The old adage 'time is money' is never truer than in a security sense. Using automation, security professionals can dramatically reduce the time taken to not only detect but equally deal with a threat – and in turn save significant sums induced by downtime, ransomware demands or the many other adverse effects of an attack. Further, these technologies don't just save money. They also drive down costs in a proactive manner.

Right now, solution saturation is a huge issue plaguing the cybersecurity market, with reports showing that companies may have up to 70 different security vendors installed at any one time. In such instances, many overlapping solutions might be running simultaneously that paint a complex picture, leaving organisations incapable of determining which of their many tools are providing actual value and which are not.

Historically, security investments have been reactionary and, therefore, immediate. When a firm may realise it has a gap, they plug it by investing in tools that are built for that specific purpose. However, over time this approach can create inefficiencies. You can end up with two or three technologies that are all doing the same thing. If one of those is effective 99 percent of the time, organisations should be able to ask themselves if they need those other two technologies to deal with the one percent, and if that's worth it for the price.

Automated analytics and correlation technologies can provide key insights here. Using data, they can determine when one technology covers all bases and if the two are simply not needed, helping firms to minimise their operational overheads with meaningful automation.

In security, human-driven detection and response and automated detection and response are night and day. If done right, the latter can deliver a host of benefits, be it cost efficiencies or improved transparency of operations. However, there is a catch. Machine learning models aren't a case of plug-and-play. There are many factors influencing the effectiveness of these technologies, and companies need to create the solid, comprehensive foundations from which they can thrive.

A critical issue here is the availability and reliability of data that is being used to teach machine learning models. Are there any external data sources that can be cross correlated with? How many do you have access to? What's the bias on those data sources? If you're only taking a small subsection of data, your machine learning models will fail to have the adequate information needed to develop adequate intelligence and in turn, power accurate and informed actions. Companies therefore need to consider ways in which they can expand their datasets and, in effect, begin to develop and run a data lake – even if it's just for security purposes.

THE AVERAGE COST OF A DATA BREACH WAS $4.24 MILLION IN 2021 – THE HIGHEST FOR 17 YEARS

This data lake should include mapping users. For machine learning to truly work in a security context, you need to understand what your users are doing, what applications they use, at what times and in what ways. This will ensure that anomalous activities can be spotted immediately, triggering an automated response.

Without trying to sound like a broken record, this requires patience. For intelligence to really understand and prioritise whether certain anomalous activities are a genuine risk to an organisation, a lot of history and a lot of data points are required. This simply needs to be accounted for – much like an employee, if we give a machine learning model just 30 days to get 100 percent up to speed, it is simply not going to happen. Companies must start slowly and treat these technologies as if they are a new starter, rather than expecting them to deliver overnight.

Given this opportunity, machine learning and AI can become game-changing weapons in the fight against cybercrime – yet providing this environment may require a mindset shift. Firm's need to shift from being policy-led to data-led. Indeed, policy remains a critical component, helping dramatically in achieving compliance and ordering the operating environment, but given the current threat landscape, security decision-making must be data-driven.

Internal data generated by everything from user activity to threat feeds can provide critical insights, showcasing where a company may or may not be vulnerable. Most organisations will have this data – whether they're listening to it, or have the ability to

interpret it, is another matter. Companies need to have a way to visualise their data easily. Only then can they start to tap into the power of automation. It is for this reason that AI presents a quantum leap forward.

Moving from detect and response security protocols that rely on human cognition to a fully automated security posture is a major jump and may involve the leapfrogging of many technologies in between. It is a process that might seem a little overwhelming, but with a data-led mindset it won't be difficult to achieve. It is easier today than ever before to take this quantum leap into automated detection and response, and many larger firms are already on this pathway and talking in these terms, building data lakes and incorporating AI and machine learning.

AUTOMATED THREAT DETECTION AND RESPONSE REDUCES THE PRESSURE ON SECURITY TEAMS

In the grand scheme of security, having complete visibility of an organisation's network and an appropriate response for any given threat level is a vital step to take. To deal with sophisticated threats, security responses need to be dynamic to be effective. In order to achieve this, we need to leverage cutting-edge technologies and, therefore, need effective data-led foundations.

So, what can we expect for 2022? As the effectiveness of AI, machine learning and RPA technologies continue to come into greater focus, I anticipate that firms will begin to iron out additional issues that will further enhance security ecosystems. We are seeing obstacles now in regard to partner technology, so interoperability is perhaps the next big hurdle that needs to be overcome.

Further, the mass shift to the cloud that we have witnessed during the pandemic has also complicated security for many companies where migrations may have created blind spots. While the cloud is undoubtedly the future – a key technology in which flexible and hybrid working models can be built, unlocking a host of operational benefits and efficiencies – security teams are now tasked with ensuring that hybrid environments are as secure as the on-prem environment was.

Simply put, the perimeter doesn't exist any more. That's a reality that we're still navigating, with users interfacing and accessing data in different ways. As an example, it's led to the introduction of new policies such as zero-trust and questions surrounding authentication. If you're talking about intelligence, intelligence needs access, so how do you trust your intelligence engine to have access to everything if there's no trust by design? With these developments and considerations, the landscape has undoubtedly become a bit more complicated.

Yet security teams still need to monitor activities and make informed, logical decisions. Therefore, just as the cloud has become a critical component in improving the effectiveness of company operations, machine learning must equally become a vital pillar of security. If it does, and in the right way, then a massive burden will be lifted from security teams and the resulting benefits will be numerous ●

Tim Wallen is Regional Director UK&I, LogPoint

Automated analytics and correlation technologies can help firms to minimise their operational overheads

Sentinel

A TSCM BREAKTHROUGH

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

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

Designed for TSCM Engineers by TSCM Engineers.

FEATURES

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

SENTINEL KIT INCLUDES

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

For further details: contact@qccglobal.com

LONDON

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

SINGAPORE

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

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

Picture credit: US Dept Defense

STRATEGIC PLANNING

Jawhar Farhat *examines the need for a national security plan in light of the Russian invasion of Ukraine*

The establishment and maintenance of a secure society requires a strong, and professional security state. As a result, governments will strive to integrate law enforcement agencies' work and coordinate it to increase impact, focus duties and reduce unnecessary complexity. About the Russian-Ukrainian war, risk analyses are more accountable for assessing data related to introducing a wide range of instability-related events that are critical to the governments and its various operations which can abuse public security.

The national security plan is a strategy that the highest levels of government sign and promote. That considers the international, regional and domestic contexts to determine what is in a nation's best interests, sets objectives to advance or protect those interests, and then finds innovative ways to use the means at the nation's disposal, or if those aren't available, to generate the means

Two Air Force F-35 Lightning II aircraft arrive in Lithuania in late February to support NATO's collective defence

and resources necessary to implement the strategy at a later date. A national security plan process also entails analysing the costs and risks of a chosen course of action, as well as continuously scanning the environment for changes that could jeopardise your approach. However, there are many variations in this description, but it is an ends-ways-and-means structure that is widely acknowledged in the national security community, even though many people use it in different ways or change it. As a result, we're not simply talking about military strategy, economic growth plan, negotiating strategy or environmental strategy; we're talking about a strategy that considers these factors.

An outward-facing strategy may be concentrated on your country's neighbours or the worldwide environment, whereas an inward-facing strategy is focused on your own country and what's going on internally, as well as the ability to generate funds to ensure that outward-facing plan.

THE RATIONALE FOR HAVING A NATIONAL SECURITY STRATEGY

On some occasions, a break from the past may be necessary. A change in the worldwide environment, the regional environment, the domestic environment or the individual leader, for example, could all be factors. There are various more reasons for these environmental changes. A country may seek to develop a strategy to create a shared vision of the future to achieve national unity of effort and to prioritise resources.

At the same time, a nation might want a strategy to maintain a strong vibe going, keep a government in place, bring hope or confidence, manage risk, gain access to a system, change a system or tear down the entire system.

Governments may not want to inform their adversary what they are up to in secret. You may not want it written if you have one in your head. Furthermore, governments may not want a strategy, since it will bind them if they tell everyone what they're going to do, and they will lose credibility as senior strategists if they do so. Governments may not want a strategy if public opinion opposes it, if it violates international law or if it fails because they cannot plan, and they may not want a strategy because it allows them as a leader to have a force of their personality, a cult of their personality. Furthermore, it places them in charge, establishing them as the leaders in charge and decision-makers.

THE MEANS FOR IMPLEMENTING A NATIONAL SECURITY STRATEGY

When we talk about means, we might think of them in three different ways: institutions, people and things. Objects which can be touched or palpable things, is a term we might use to describe them. Treaties, accords, communication resolutions, summits cables, verbal notes and marshes are also included. These are all diplomatic tools that can be used in a variety of ways. When we think of institutions and think tanks that disseminate information, we think of universities and think tanks. The intelligence communities deal with both information and people; they have spokespersons, reporters and analysts.

Newspapers, televisions, radio broadcasts, satellites, intelligence concepts and symbol logos are all examples of things. These are tools for gathering information. On the military side, we can have defence ministries, interior ministries, institutions, regional organisations and military command. There are also planes, ships, tanks, troops, commanders and police, as well as paramilitary law enforcement.

Furthermore, there are government ministries, the World Bank, the UK Infrastructure Bank, regional economic communities, grants and loans, scholarship help and stock exchanges. As a result, a country has a lot of things, a lot of means and a lot of resources at its disposal. Finally, the art form is figuring out how to put them together over time to achieve the goals that governments set for themselves.

WHO'S RESPONSIBLE FOR STRATEGY DEVELOPMENT?

From my perspective, everyone handles strategy creation. It's also a reflection of growing democratisation and democracy. So, in a democracy, the planning process appears different from how it is in a country with a powerful leader or a dictatorship. However, servant leadership is one approach to positive strategy creation. It fosters agreement by educating individuals about the nation they serve, the goals they are attempting to achieve and the importance of putting people's interests ahead of the nation's.

ANY NATIONAL SECURITY POLICY IS A WORK IN PROGRESS THAT MUST BE REGULARLY UPDATED

The triangle of interests, which includes dangers, opportunities and objectives, is used to assist identify some of the key components. Furthermore, as part of the context of assessment, an honest understanding of what the government's national interests are, as well as the risks and opportunities that affect those interests: internal dangers, external threats and opportunities are all factors to consider. Governments can then decide what objectives they need to meet to serve those interests and address risks or opportunities, such as seizing or mitigating them.

Moreover, this aids governments much when they jump ahead to objectives, determining whether these aims are serving their interests and whether they will minimise threats or seize opportunities. Otherwise, if the aim is okay, this is a fantastic aim, but if it's not supporting their interests, then it's not so significant, or it seems like a nice aim, but it will not help them deal with that threat, then it's not so vital. In this situation, they'll need to change their goal to ensure that it's accomplishing that. As a result, after they've proven it, they can go on to the details of their methods and means.

In terms of methods and means, consider economics, intelligence, diplomacy and ties with other neighbouring countries, as well as the United Nations. To summarise, much of this is outside the military's purview, thus it's critical to combine civilian dialogue with those outside the government. Governments can, for example, bring in national security councils and business leaders to get their input, as well as civil society leaders from think tanks and advocacy groups, to get their input and give them some ideas, as well as military and neighbours, so that everyone can be a part of the process.

Government leaders should take visions and turn them into an end-goal means package that can then be implemented by patents. For developing a strategy, decision-makers need a reaction from visionary members and actionable members (military), and then each government needs a leader who can think about how to bring these pieces together, which is why having all of those aspects is important.

IT'S CRITICAL TO COMBINE CIVILIAN DIALOGUE WITH THOSE OUTSIDE OF THE GOVERNMENT

Then it becomes intimate ties, and it's important to cultivate those interactions not only within services but also between military and civilians. Furthermore, while there are many various sorts of national strategy, they all follow the same core principles: developing an assessment of context; defining interests; defining threats and opportunities; defining ; assessing risks; developing ways and means; and determining costs. When deciding on a strategy, it's necessary to evaluate factors such as feasibility, sustainability, affordability, assumptions, strengths, and weaknesses of your competitors' strategies, continuous evaluation, and measurement of performance, adjustments, and adaptability. To summarise, any national security policy is a work in progress that must be updated and changed regularly.

The Russian cyber threat is not only serious, but it's also unexpected, so policymakers prefer to warn the world that cyber weapons can be used as weapons and have the same rules that would prohibit or regulate the use of a missile. We've seen in the past that Putin isn't interested in moving on to the second stage of analysis and considering whether he might start using a cyber weapon in a way that violates those rules, something that isn't focused on Ukraine but could, by design or by accident, spread to companies around the world.

We could see a kind of catastrophic set of attacks that would hit indiscriminate companies all over the world if the Russian government didn't inflict billions of dollars in losses in American and European companies during a stage when he wasn't in a kinetic war.

Those attacks might not be obvious, and they might not have a definite goal in mind. As a result, one thing we witnessed from the Colonial Pipeline ransomware attack this past summer was a rather particular ransomware targeted attack, which brought the pipeline's activities to a halt for a period. Also, we saw an assault that took use of a Microsoft weakness to prevent anyone from utilising the infected PCs, therefore rendering them worthless. If that's what indiscriminately takes down any computer using this software that hasn't been patched, we have to consider how disruptive that could be. Therefore, it may not be a targeted attack, but an indiscriminate attack that shuts down systems all around the world. As a result, the entire cyber community is on high alert right now, with cyber security companies and all of their partners, including those who would normally compete, cooperating to collect as much data as they can or any technical information with any customers who want it, and they're normally attempting to identify the Russians' tactics quickly so that people can patch against them and then share effective skills ●

Jawhar Farhat is a certified security management professional (CSMP) Level 6 diploma who graduated with a Master's degree in Military Sciences from Fondouk Jedid Military Academy of Tunisia. He gained his expertise both in his current employment as a Risk Analyst and during his service in the military as a First-Lieutenant. Now, he is assisting security and risk professionals in making an obvious influence on their firms and helping them prevent potential concerns.

The entire cyber community is on high alert against Russian cyber attacks

Picture credit: US Dept Defense

PLAY IT SAFE

Craig Swallow *wonders how, in an age of hybrid working, organisations can ensure employees are safe*

Every employer organisation has risks and a duty of care to ensure its employees are safe within the workplace. Many employees do not work in one fixed place and this situation can change day to day, a factor that organisations need to consider when assessing the risk to staff and how to reduce it. Do employers need to consider the potential risks to changing working environments?

The concept of what comprises a workplace has changed significantly. Research shows that since the pandemic began, some 60 percent of people in the UK began working from home. Many have now adapted to this working style and are likely to continue this way. Some organisations might incorporate a mixed model of home and office working or using hot-desking at work or in shared workspaces away from the office. When a working environment changes, new risks to employees need to be assessed. Where the workplace is not fixed, employers need to consider the potential risks in the various workplaces, as well as in any travel environments.

Risk assessments are a historic way of helping to ensure health and safety regulations are met or, where desired, exceeded. They are useful to management for identifying any patterns of risks, allowing security or HR/H&S personnel to investigate ways to reduce and better manage potential hazards to employees. Where employees work in various places, at different times, it is crucial for employers to ensure management can

Employers have duties under health and safety laws to assess risks in the workplace

communicate effectively with staff when required. This is particularly important in cases of emergencies or expected emergencies (a weather storm or terrorist incident, for example), where staff might not be checking their emails and/or SMS or WhatsApp messages on a regular basis.

An increasing number of employees spend more time on their own than before the pandemic. Whether they are working from home on their own or visiting clients in the community alone, employees can feel more isolated. Organisations should ensure measures are in place to check on their well-being. Involving employees in this process can help organisations understand how they can ensure the process will work effectively.

Working from home or remotely as a lone worker is a two-way street as it can be beneficial to both employers and employees. One well-noted advantage to the employee is increased productivity, since workers don't have to spend a considerable amount of time commuting to and from the office. Another advantage is that employees can enjoy flexible working hours, giving themselves a sense of freedom as well as trust from their employer.

On the flip side, and focusing on the employer, by having workers at home and not in the office, companies can save on costs if they don't have to maintain a large office. Another perk for employers is that a remote working structure can help companies expand their presence in strategic locations by having more workers in numerous locations at one given time. This does have its downside, however, for remote employees because working at home can make them feel isolated from their colleagues; and, of course, they have no direct supervision unless virtual one-to-one or group meetings are held.

In all working environments, the employer is responsible for the health, safety and welfare of its employees and this applies to any contractors, volunteers, or self-employed workers. It's often perfectly safe to work alone. However, the law requires employers to think about and deal with any health and safety risks before employees are allowed to do so. Establishing a healthy and safe working environment for lone workers can be different from organising the health and safety of other in-house workers. One thing to consider when ensuring the safety of a lone worker is assessing areas of risk. Assessment could cover such issues as is the employee fit, do they have the medical suitability to work on their own and does their workplace present a risk to them?

Another consideration is having systems in place to always keep in touch with staff and respond to any incident. Employees and some self-employed workers also have responsibilities to take reasonable care of themselves and other people affected by their work activities, and to co-operate with their employers in meeting their legal obligations.

An employer must protect the health, safety, and welfare of their employees and other people who might be affected by their business. Employers must do whatever is reasonably practicable to meet health, safety and welfare obligations to achieve this. This means making sure that workers and others are protected from anything that may cause harm, effectively by controlling any risks to injury or health that could arise in any of the workplaces. Employers have duties under health and safety laws to assess risks in the workplace. Risk assessments should be carried out that address all risks that might cause harm in your workplace.

Employers must give staff information about the risks in the workplace and how they are protected, as well as instructing and training them on how to deal with the risks. Employers are also obligated to consult employees on health and safety issues. Consultation can be done directly by management/line managers or via a safety representative who is either elected by the workforce or appointed by a trade union.

To recap, lone working can negatively impact employees' work-related stress levels and their mental health. Management standards for work-related stress exist and include such factors as relationships with, and support from, other workers and managers. Being away from managers and colleagues could mean a good level of support is more difficult to achieve. Therefore, putting procedures in place that allow direct contact between

SINCE THE PANDEMIC BEGAN 60% OF PEOPLE IN THE UK STARTED WORKING FROM HOME

the lone worker and their manager should be the first step and will definitely be helpful.

Managing work-related stress relies on understanding, by management, what comprises 'normal' employee behaviour and therefore being able to recognise abnormal behaviour or symptoms at an early point. If contact between management and the lone worker is poor, employees may feel disconnected, isolated or abandoned. The best way for management to keep in contact with lone workers is to agree on a time to keep in touch, whether that is by one-to-one meetings using Microsoft Teams, Zoom *etc*. or meeting face-to-face.

In the meetings, the lone worker can be updated with all the latest office news and invited to social team events and activities. Moreover, it's vital to ensure lone workers are included in any consultation about changes that may have implications unique to them. Consultation could include training courses that are essential for improving the employee's standard of work, and/or it changing.

Feeling overwhelmed, poorly managed or mistreated in the workplace can aggravate pre-existing mental health conditions. Problems at work can bring on symptoms or make their effects worse, even in best-performing staff. Whether work is causing the health issue or aggravating it, employers still have a legal responsibility to help were reasonably possible. Interventions can include those required by the Equality Act 2010. Mental health issues are on the rise in the workplace, as exampled by the following information from mental health charity, Mind UK: more than one in five (21 percent) of employees admitted they called in sick to avoid work when asked how workplace stress had affected them; 14 percent agreed they had resigned and 42 percent had considered resigning when asked how workplace stress had affected them; 30 percent of staff disagreed with the statement: "I would feel able to talk openly with my line manager if I was feeling stressed"; and 56 percent of employers said they would like to do more to improve staff well-being, but don't feel they have the right training or guidance.

The reality of budgeting pressures is not new to companies when it comes to their employee safety departments, which often must handle the duty of care obligations within a dwindling budget. Employee health and safety budgets have reduced even more during the Covid-19 pandemic, making it vital for safety professionals, HR and middle management to showcase and justify their activities. One of the best

WHERE THE WORKPLACE IS NOT FIXED, EMPLOYERS NEED TO CONSIDER THE POTENTIAL RISKS

ways to highlight the activities to senior management is to make invisible success… visible.

Subjects including employee turnover, absenteeism and well-being questionnaire results are great starting points to assess how safe the workforce feels, and should be completely transparent to the business owners, CEOs and other executives without necessarily giving away the personal identities of the participants. If senior management can be shown success achieved on the current budget, it might remain intact. Note the "might". More research is required to showcase true ROI, which leads nicely onto the second variable – financial analysis.

What are the financial aspects – including cost outcome analysis, cost-benefit analysis or cost-effective analysis – of health and safety programmes? All these analyses work the same way, but one may be more appropriate to use than the others. First, management should estimate the net cost of a programme by determining how much it costs to implement, before subtracting the cost savings that are associated with it. Determining cost savings can be challenging, so it's crucial to be able to demonstrate quantitatively that the programme is having a direct positive impact. Matching visibility, that is built on solid foundations, with financial clarity and accuracy, is key.

Introducing and reinforcing risk reduction and associated health and safety programmes nationwide or internationally can be made easier by modern technology. Examples include app-based tools linked to a server-based 'dashboard' at head office, enabling the employer to build and maintain better communications with employees regardless of where they are. Communications can include mass-mailouts to staff of messages alerting them to actual or anticipated risk to well-being (including risk to life) incidents. At a more mundane, but still important level, mass communications can be about new health and safety guidelines or simply psychologically supportive messages designed to optimise employee mental well-being.

Employees can proactively use such apps at any time, wherever they are, to alert their employer – eg the HR or security department – about a risk-to-health-or-life situation they find themselves in or expect to find themselves in. Staff can also use an app to communicate with their line manager or the HR department about levels of stress or unhappiness they are experiencing.

To summarise, in an age of hybrid working organisations can take steps to ensure – as much as is reasonably possible – that employee well-being is optimised to the maximum. For a comprehensive end-to-end approach, the steps can start with risk assessments and move on to GPS, app-based tools that address all employee – senior executives included, let's not forget! – possible eventualities ●

Craig Swallow is Vismo CEO and has over 18 years direct experience of developing and delivering lone worker solutions to clients across the globe. He has a passionate focus on achieving valued solutions that deliver meaningful benefits to both employer and employee. Craig has always been an active member of standards boards, with a focus on worker safety solutions, alarm receiving centres and body-worn video

When a working environment changes, new risks to employees need to be assessed

INTERNATIONAL SECURITY EXPO

27-28 SEPTEMBER 2022. OLYMPIA LONDON

THE CRITICAL LINK IN YOUR BUSINESS STRATEGY

Celebrating 20 years, International Security Expo, the market-leading security event, provides the vital link between Government, industry, academia and the entire end-user community, strengthening the relationships that are essential to improving our safety and security.

No other event delivers such a high-level of buyers, specifiers and decision-makers making it the perfect platform for launching new products, showcasing the latest innovations and generating new leads.

10,000+
SECURITY BUYERS

350+
INTERNATIONAL EXHIBITING COMPANIES

SECURE YOUR STAND **TODAY**

VISIT: www.internationalsecurityexpo.com

CALL: +44 (0) 208 947 9177 | EMAIL: info@internationalsecurityexpo.com

INCIDENT BRIEF

Europe

5 March, Germany and Central Europe
Thousands of internet users across Europe were thrown offline after what sources said was likely to be a cyberattack relating to Russia's offensive in Ukraine.

5 March, Brussels – Belgium
Morocco's General Directorate for the Surveillance of the National Territory provided Belgian authorities with information on a Belgian citizen of Moroccan origin suspected of involvement in the preparation of a terrorist plan with cross-border ramifications.

9 March, Ajaccio, Calvi and Bastia – Corsica
Violent clashes broke out between protesters and police amid anger over the assault in prison of Claude Érignac by a fellow detainee serving time for terror offences.

13 March, London – UK
A group of two dozen environmental activists attempted to storm the entrance to the red carpet VIP area of the Baftas, but were prevented from getting inside by police and security.

15 March, UK-France Channel
More than 900 people were intercepted in small boats crossing the Channel in what is thought to be the largest number of migrants attempting to reach the UK this year.

15 March, Milton Keynes – UK
Roads were closed after an unexploded grenade was discovered in a cemetery. A specialist bomb squad safely detonated the device and no one was harmed.

Americas

5 March, Querétaro – Mexico
Twenty six people were injured – three critically – as a soccer match descended into violent clashes between opposing fans.

7 March, Iowa – USA
One person was killed and two others critically wounded in a shooting outside a school that appeared to come from a passing vehicle. Potential suspects were detained, but no charges were immediately filed.

8 March, California – USA
A 30-year-old US citizen was arrested by US border agents as he attempted to smuggle some 52 lizards and snakes hidden in his clothing into the country.

13 March, New York – USA
A 60-year-old man entered the lobby of the Museum of Modern Art, leapt over the reception desk and stabbed two employees as they tried to flee. Police are investigating.

13 March, Quintana Roo state – Mexico
Two gunmen opened fire on a businessman from Cornwall who was driving on a highway near Playa del Carmen. The 54-year-old died in front of his teenage daughter.

14 March, Nuevo Laredo – Mexico/US border
Gunfire and burning vehicles following the arrest of a leader of the Northeast Cartel led US officials to close the consulate and briefly shut down close border crossings.

15 March, Michoacán – Mexico
Armando Linares López became the eighth Mexican journalist to be killed this year when he was shot outside his home.

Asia

4 March, Peshawar – Pakistan
As many as 57 people were killed when a suicide bomber detonated their device in a crowded Shia mosque during Friday prayers. Islamic State is suspected.

9 March, Mian Channu – Pakistan
India said that it accidentally fired a missile into Pakistan because of a "technical malfunction" during routine maintenance. The missile was unarmed and no one was harmed.

11 March, Waziristan – Pakistan
Security forces killed four terrorists as they conducted intelligence-based operations in the district. Arms and ammunition were recovered.

13 March, Erbil – Iraq
Iran claimed responsibility for a missile barrage near a US consulate complex, saying it was retaliation for an Israeli strike in Syria that killed two of its Revolutionary Guards.

14 March, Delhi – India
A passenger train was stopped and a bomb disposal team called in to check a suspicious bag left in a carriage. The bag was safely destroyed and no one was harmed.

15 March, Kirkuk – Iraq
Two Islamic State suspects who were plotting to carry out a suicide attack during the month of Ramadan were arrested by Iraqi and Kurdish security forces.

16 March, Erbil – Iraq
The Kurdistan Region's counter terrorism department confirmed the arrest of two "active members of ISIS" wanted by the Iraqi counter-terrorism service.

16 March, Balochistan – Pakistan
An IED strike in the Sibi district killed four Pakistani soldiers and badly injured 10 more. Islamic State of Khorasan Province (ISKP) is suspected.

18 March, Adelaide – Australia
A 15-year-old boy was arrested for possession of information for terrorist acts, extremist material and taking part in the manufacture of explosives.

Africa

3 March, Benishangul-Gumuz region – Ethiopia
Eleven people, including nine ethnic Tigrayans, were killed in the region. Ten of the people were shot dead while the 11th, a Tigrayan man, was burnt alive.

5 March, Tunis – Tunisia
Tunisian security forces arrested a female jihadist suspected of planning to kidnap the children of members of the security forces and the military to try to force the release of people convicted of terrorist offences. The woman was also suspected of planning to attack a security facility using an explosive belt.

5 March, Mondoro – Mali
Terrorists looted 21 vehicles and killed 27 soldiers as they carried out an attack on a military camp near the Burkina Faso border. Seventy attackers were killed by the Malian army.

6 March, Gqeberha – South Africa
A 28-year-old man was arrested after he attempted to hijack a man and his vehicle using a toy gun. Two other suspects remain at large.

10 March, Darfur – Sudan
At least 19 people were killed and five wounded as clashes broke out between armed groups in the Jebel Moon mountains, close to the border with Chad.

11 March, Tema – Ghana
An employee of G4 Group Security was sentenced to eight years' imprisonment and hard labour for causing damage to and stealing electronic train parts.

16 March, across the country – Morocco
Five suspects affiliated with Islamic State who were planning attacks on security forces and government officials were arrested in simultaneous anti-terrorism operations.

16 March, Borno State – Nigeria
A health worker was abducted by ISWAP militants while unloading food and fuel from a humanitarian aid truck.

17 March, Borno State – Nigeria
A newly recruited soldier was killed by ISWAP militants when they attacked a military base with gun trucks.

NEWS

Europe

UK police should work "under licence" says review

The Strategic Review of Policing in England and Wales has recommended that officers should work under a licence that's renewed every five years and subject to strict conditions. The review, chaired by Sir Michael Barber and carried out by the Police Foundation thinktank, contains 56 recommendations urging radical reform to police culture, skills and training, and organisational structure. Barber, a former adviser to Tony Blair and an expert on implementation of large-scale systems change, said: "There is a crisis of confidence in policing in this country, which is corroding public trust". The licence should be renewed every five years, subject to an officer demonstrating professional development through achieving relevant qualifications, passing an interview or presenting a portfolio of activities and achievements, the report said. Any officer who fails the assessment could receive further support including mentoring, but successive failures would see their licence removed and they would no longer be able to work. Barber also called for improved training and support for sergeants and inspectors so that they are equipped to provide stronger supervision, tackle poor conduct and call out bad behaviour among officers. Police chiefs have described the report as being: "thorough and thought-provoking"..

Exterro extends digital forensics offering to public sector

Exterro – the industry's first provider of Legal GRC software, which unifies digital forensics, cybersecurity compliance, data privacy and e-discovery – has partnered with Blue Lights Digital (BLD) to deliver next-generation digital forensic technology. Under the new partnership, BLD will actively market Exterro's full Forensic Toolkit (FTK) solutions to its existing customer base and to law enforcement, intelligence agencies and military organisations to assist them with their digital investigations and intelligence-building capabilities. In addition, BLD will also make available Exterro's wider product portfolio, including its Incident and Breach Management and Smart Breach Review, to offer Digital Forensics and Incident Response (DFIR) – useful given that police forces will be required to obtain accreditation to conduct on-scene DFIR examinations by October this year. DFIR also enables other organisations to comply with regulatory requirements such as data breach notification and to pro actively mitigate the risk of a breach.

Doubts raised over Royal Navy controlling Channel crossings

The credibility of the government's plan to put the Royal Navy in charge of coordinating efforts to control small boats in the Channel is expected to be questioned by a parliamentary committee. A report by the defence select committee raises doubts over whether plans to put the Royal Navy in charge have been rigorously tested. John Spellar, the Labour vice-chair of the committee and a former defence minister, observed:"This is a PR-driven policy which is without any coherent detail, but also poses significant difficulties and has the real risk of reputational damage for the [Ministry of Defence] and the Royal Navy." Another witness, the former Royal Navy officer Commander Tom Sharpe, said: "Arriving in Dover full of migrants and with a white ensign on the back is (likely to cause) reputational damage to the Royal Navy."

German court rules far-right AfD party threat to democracy

A German court has ruled that the far-right Alternative for Germany party (AfD) can be classified as a suspected threat to democracy, paving the way for the domestic intelligence agency to spy on them. The administrative court in Cologne found that there were: "sufficient indications of anti-constitutional goals within the AfD" and as a result, the BfV is allowed to officially classify the anti-Islam, anti-immigrant party as a: "suspected case of right-wing extremism". The classification authorises intelligence agents to tap the party's communications and use undercover informants.

Nearly 30 percent think China spread Covid-19 on purpose

More than a quarter of people believe that Covid-19 was a biological weapon intentionally spread by the Chinese state, according to a new UK poll highlighting the spread of conspiracy theories. The findings came from a report by the campaign group Hope Not Hate (HNH) warning that the rise of Covid conspiracy theories and the antilockdown movement are recruiting young people to far-right ideas and movements. It also says the economic hardship of the past year and worries about the future have created an environment in which far-right activists may return to the streets. The same poll, commissioned as part of the annual State of Hate report, highlighted that faith in democracy and the political establishment is extremely low. A total of 1,492 people were surveyed by Focaldata on 25-26 February, though it remained to be seen whether Russia's invasion of Ukraine would affect support for democratic values. More than half of people asked (57 percent) were not satisfied with the way democracy is working in the UK, while 6 percent thought it was definitely true that: "coronavirus is a bio-weapon intentionally spread by the Chinese state", with a further 23 percent thinking it was probably true. Nick Lowles, the chief executive of Hope Not Hate, said: "The crises we've collectively faced over the past two years have emboldened cynical far-right activists to exploit our fears and uncertainties and return to traditional methods of campaigning."

NEWS

Americas

Woman who ran propaganda centre charged as Russian agent

A woman who ran a Russia propaganda centre in New York has been charged for acting as an unregistered foreign agent for the Russian government. Elena Branson, 61, who has both US and Russian citizenship, ran the Russian Center New York, which she founded in 2012, receiving thousands of dollars from the Russian government. The centre reportedly coordinated activities such as an I love Russia campaign aimed at American young people to promote Russian history and culture. Branson also serves as chairperson of the Russian Community Council of the USA, which supports: "organisations of Russian compatriots, to preserve and popularise the Russian language and cultural and historical heritage in the United States". Branson has been charged with conspiring to act as an agent of a foreign government without notifying the US attorney general as well as taking part in a visa fraud conspiracy. She is also being accused of helping others illegally avoid registering as foreign agents. During an interview with the FBI in September 2020, Branson said that she had never been asked by Russian officials to arrange meetings with US officials. However, the following month, she told a Russian-state controlled TV station that she left the US because she thought she would most likely be arrested.

US accuses North Korea of escalation in missile tests

The US believes North Korea is testing a new intercontinental ballistic missile (ICBM) in what the Biden administration called a: "serious escalation" that would trigger more sanctions. Pyongyang conducted two recent missile launches which it claimed were for putting satellites into space. After scrutinising them, however, US intelligence believes the real intention is to test parts of the new missile. The US believes the ICBM being tested was first displayed by the Pyongyang regime in October 2020, and then again at a defence exhibition a year later. The US made its assessment in conjunction with Japan and South Korea, and a senior US official revealed that it would share the conclusions with other allies and partners, including the United Nations. US forces have stepped up their monitoring and intelligence collection in the region, and new sanctions have been introduced to further restrict North Korea's access to advanced technology that it could use in its weapons programmes. Some experts believe North Korea could launch a spy satellite or test an ICBM in April to coincide with the 110th anniversary of the birth of the country's founder, and Kim's grandfather, Kim Il-sung.

US considering dropping Iran's IRGC from terrorism list

The United States is considering removing Iran's Revolutionary Guards from its foreign terrorist organisation blacklist in return for assurances about reining in the elite force, according to a Reuters source. The source claimed Washington had not decided what might be an acceptable commitment from Tehran in exchange for such a step, which would reverse former President Trump's 2019 blacklisting of the group and draw sharp Republican criticism. The source claims the Biden administration is weighing whether to drop the terrorist designation: "in return for some kind of commitment and/or steps by Iran, with respect to regional or other IRGC activities". Multiple sources have said that dropping the designation remains one of the last, and most vexing, issues in wider indirect talks on reviving the 2015 deal under which Iran limited its nuclear programme in return for relief from economic sanctions.

Chicago doubles security guards

The Chicago Transit Authority (CTA) has announced its plans to double the number of security guards on its trains and buses and the city will be deploying more police officers on transit vehicles in an effort to curb a rise in violent crime on public transportation. The CTA has had many issues during the pandemic, including an increase in crime and breaches of CTA rules on trains and buses. The Chicago Transit Board approved contracts which allow the CTA to spend $71-million on security resources on 9 March. According to a statement released by the mayor's office, security guards will receive conflict resolution and de-escalation training, will enforce CTA rules and will be trained to assist customers with questions about CTA service.

DHS report on violent extremism

The Department of Homeland Security has released a report on how it can best prevent, detect and respond to domestic violent extremism threats within the Department. The report highlights the steps DHS should take to identify and address such threats. Among the key recommendations, the report highlights the need for clear guidance as to what constitutes violent extremist activity and how to address it, improved workforce training for how to identify and report this activity and the development of a centralised, DHS-wide investigative case management system and information sharing mechanism for investigating related allegations. "Every day, the more than 250,000 dedicated public servants at DHS work to ensure the safety and security of communities across our country. To ensure we are able to continue executing our critical mission with honour and integrity, we will not tolerate hateful acts or violent extremist activity within our Department," said Secretary of Homeland Security Alejandro N Mayorkas. "The findings of this internal review highlight key steps that our Department will continue to take with urgency to better prevent, detect, and respond to internal threats."

NEWS

Asia

Chinese adviser calls for law to ban fake news

An adviser to the Chinese government has called for new laws to ban: "fabricating and disseminating fake information online", blaming the rampant disinformation on the internet for polarising Chinese public opinion. Jia Qingguo, a member of China's highest political advisory body, said he also believed the proliferation of misinformation online had fuelled tensions between China and other foreign countries. The former dean of Peking University's School of International Studies added that the spread of fake news could harm national interests and lead to public confusion and social division. He called on Beijing to introduce specific measures to: "severely punish" those who create false information to: "cause serious harm to society".While Jia's proposal appears to be more domestic-focused, critics question any tangible impact of a: "fake information law" when China's internet is already heavily censored and often scrubbed of information Beijing wants to disappear. Some also worry that, if not properly implemented, such a law could have a profound impact on journalistic activities in China by both domestic and foreign news outlets, given Beijing's poor track record when it comes to press freedom.

Surge in hate against Muslims after Christchurch attack

The Islamophobia Register Australia (IRA) recorded a fourfold increase in reports of in person incidents of anti-Muslim hate, while reports of online incidents were 18 times higher in the two weeks after Australian white supremacist Brenton Tarrant murdered 51 people in an attack on two mosques in Christchurch, New Zealand. The report draws on verified incidents of anti-Muslim hate in Australia in 2018 and 2019, with recorded incidents including that of a patient in the chair of a Muslim dentist calling all Muslims: "terrorists", a family physically assaulting a woman at the zoo and a pregnant woman being repeatedly punched by a stranger in a cafe. Released by Charles Sturt University and the Islamic Science and Research Academy, the latest report analyses 247 incidents of Islamophobia across 2018 and 2019, 138 of which occurred in person, 109 online. The data shows that anti-Muslim hate is deeply gendered, with women comprising 82 percent. Of those women, 85 percent were wearing hijab and 48 percent were alone when the attacks occurred, while 15 percent of them were accompanied by children. Most of the perpetrators (74 percent) were male.

Islamic State unveils new leader

Islamic State has named a new leader after confirming that its previous head was killed by the US in north-western Syria back in February. In an audio message IS spokesman Abu Omar al-Muhajer confirmed the death of previous leader Abu Ibrahim al-Hashimi al-Qurayshi as well as that of former spokesman, Abu Hamza al-Qurayshi, in the US raid. Muhajer went on to reveal that IS has named a successor, identifying him as Abu Hassan al-Hashimi al-Qurayshi and saying the late IS chief had chosen him. Information about the new leader remains scant and it isn't known whether or not he is Iraqi – like his two predecessors. One thing we can confirm, however, is that none of the Qurayshis are believed to be related. Al-Qurayshi comes from Quraish, the name of the tribe that Islam's Prophet Muhammad belonged to, and which serves as part of an IS leader's nom de guerre.

Kuala Lumpur beefs up train security

In Kuala Lumpur, Rapid Rail has announced that security will be improved at all of its LRT, MRT and monorail stations for the safety of passengers. The rail operator is also calling on train passengers to immediately report any criminal attempts or suspicious activities taking place within the stations. "We will be beefing up efforts to assist passengers in making it more convenient for them to report such activities without delays, as well as adding more notifications, along with telephone numbers to be contacted in the platform area," said the company in a statement. It revealed that it will also be increasing its cooperation with the police with more monitoring and patrols, especially in areas with suspicious activities. "Our passengers can also report any suspicious activities to the station's officer on duty at the counter if the auxiliary police personnel are absent or they're on patrol," said the statement.

IBM launches cybersecurity hub for Asia-Pacific region

IBM has announced plans to introduce a cybersecurity hub in India to help Asia-Pacific companies protect their data in the: "most-targeted" region for cyber attacks. IBM Security Command Center will help address the most: "pressing need of the hour" for companies to accelerate their security strategies and align business priorities with a security-first approach, according to the company. No region was targeted for cyber attacks more in 2021 than Asia (26 percent), according to a report by IBM Security. The new hub will offer training in cybersecurity response techniques through simulated attacks, using audio and visual effects as well as live malware, ransomware and other hacker tools. IBM designed the simulations after emergency and disaster response training models, in consultation with experts from industries, including emergency medical responders, active duty military officers and its incident response experts. The cybersecurity hub can deliver custom experiences and workshops, including virtually, through the IBM Cyber Range Design consulting team.

THE SECURITY EVENT

5-7 APRIL 2022
NEC BIRMINGHAM UK

THE UK'S NO.1 COMMERCIAL, ENTERPRISE & RESIDENTIAL SECURITY EVENT

FIND OUT MORE: WWW.THESECURITYEVENT.CO.UK

Co-located with:

THE HEALTH & SAFETY EVENT

THE FIRE SAFETY EVENT

THE WORKPLACE EVENT

Lead Media Partner:

Security MATTERS

Founding Partners:

ANDOVER · ASSA ABLOY · AVIGILON · Comelit · Honeywell · TDSi · Texecom · tyco · Videcon

NEWS

Africa

Nigeria improves ranking in global terrorism index

Nigeria has dropped from fourth to sixth position in the latest Global Terrorism Index (GTI), following successes in the fight against Boko Haram insurgents. The country dropped two places from the position it has occupied since 2017. Published by an independent and non-profit think tank, the latest updates to the GTI indicate that Nigeria, Syria and Somalia are the only nations among the 10 most affected by terrorism to get an improved score from 2020 to 2021. According to the report, there was a decline in the number of terrorism-related deaths in Nigeria, thanks in part to the death of Boko Haram leader Abubakar Shekau and the federal government's efforts at defeating the group. "Total deaths from terrorism in Nigeria fell to 448 in 2021, the lowest level since 2011. Terror-related casualties dropped by almost half compared with the previous year. However, the number of terrorist attacks increased by 49 percent between 2020 and 2021. 36 percent of attacks were claimed by ISWAP, Boko Haram being responsible for eight percent and 44 percent not attributed to any group. In 2020, ISWAP became the deadliest terrorist group in Nigeria. The decline of Boko Haram continued into 2021, with Boko Haram responsible for only 69 deaths, a decrease of 77 percent from the previous year. This is the lowest number of deaths by the group for a decade" the report claimed.

Nigeria can end Boko Haram insurgency using drones

Retired US Army Colonel Wisdom Osemwende has claimed that Nigeria can bring about a speedier end to Boko Haram's reign of insurgency by employing warhead drones. A presidential aspirant on the platform of the All Progressives Congress with dual citizenship of Nigeria and US, Osemwende insists that Nigeria has a bright future, noting: "For some years now, Nigeria has been suffocating on the unbearable weight of insecurity and terror, perpetrated by the dreaded Boko Haram. This crisis has caused a lot of pain and suffering to the victimised communities and has been one of the country's biggest challenges. This should never have been happening to Africa's giant. We can redress these security challenges." The presidential aspirant, who also stated that his dual citizenship would be an added advantage to Nigeria, noted that the American government would always come to his aid if he ever needed their assistance.

94 percent of South African companies subject to phishing

In its latest State of Email Security 2022 report, Mimecast surveyed 1,400 IT and cybersecurity professionals across 12 countries and discovered that an astonishing 94 percent of South African companies have been targeted by an email-related phishing attack in the past year, with nearly two-thirds citing an increase in such attacks. The cost of ransomware attacks are also piling up, with three in five organisations (60 percent) citing damage from a ransomware attack and of companies paying the ransom, the average payment breached 3.2-million South African Rand, despite nearly half (43 percent) of payments resulting in companies being unable to recover their data.

Namibia's cyber security given boost by Check Point Software

Check Point Software Technologies Ltd. has announced it will be collaborating with the Faculty of Computing and Informatics at Namibia's University of Science and Technology (NUST), in an attempt to enhance the level of cybersecurity competency and skills shortage in the country. The collaboration between Check Point's SecureAcademy and the NUST will see the university's faculty members complete Check Point Certified Security Administrator training, enabling them to teach a range of cybersecurity courses to NUST's students, starting this year. "Through this collaboration, we are strengthening Africa's cybersecurity landscape, as our lecturers will be passing the crucial cyber skills they have learned onto the next generation of professionals," according to Dr Mercy Chitauro, Cyber Security Program Coordinator at NUST. "Achieving Check Point SecureAcademy status within Namibia is an important step forward in developing a new talent pool of qualified security professionals and a sustainable breeding ground for this talent pool in the country," said PJ Kotze, General Manager of CES.

Ghana to lend cyber security support to other countries

Ghana is prepared to lend support to other countries on the African continent to help protect their digital infrastructure. Speaking at the Africa Cyber Experts Community kickoff meeting in Accra, Deputy Minister of Communications and Digitalisation, Ama Pomah Boateng, said since Ghana is leading its peers in the implementation of many policies to safeguard the digital space, the country will offer a hand to others as well. The Africa cyber security experts' community kickoff meeting was on the theme, setting the scene for cyber security status in Africa. It was aimed at attracting private sector support from the African Union, in dealing with the threat of cybercrimes on the continent. Deputy Minister of Communications and Digitalisation, Ama Pomah Boateng assured that Ghana is making efforts to collaborate effectively in supporting the fight against cybercrime: "Ghana is one of the few countries that have signed and implemented the Budapest Convention on cyber security and we as a country keep learning from each other. I urge all other countries to sign on to the convention to improve upon the fight."

DIARY DATES

2022 Conference and Exhibition planner

5-7 April The Security Event 2022
NEC, Birmingham
Organiser: Nineteen Group
Tel: +44 (0)20 8947 9177
www.thesecurityevent.co.uk

10-12 May CBRNe Summit EMEA 2022
Sofia, Bulgaria
Organiser: Intelligence-Sec
Tel: +44 (0) 158 234 6706
Email: info@intelligence-sec.com
www.intelligence-sec.com/events

17-19 May IFSEC International 2022
ExCel, London
Organiser: IFSEC International
Tel: +44 (0)20 7921 8166
Email: ifseccustomerservice@ubm.com
www.ifsec.events/international

17-19 May RFID LIVE! 2022
Mandalay Bay, Las Vegas
Organiser: RFID Journal
Tel: +1 (212) 584-9400 ext. 03915
Email: LiveReg@rfidjournal.com
www.rfidjournallive.com

24-26 May Explosive Ordnance Seminar 2022
Budva, Montenegro
Organiser: Intelligence-Sec
Tel: +44 (0) 158 234 6706
Email: info@intelligence-sec.com
www.intelligence-sec.com/events

24-26 May Milipol Qatar 2022
Doha, Qatar
Organiser: Comexposium
Tel: +33 017 677 1314
Email: visit@milipol.com
www.milipolqatar.com

7-9 June Undersea Defence Technology 2022
Rotterdam, The Netherlands
Organiser: Clarion Events
Tel: +44 (0) 207 384 7788
Email: team@udt-global.com
www.udt-global.com

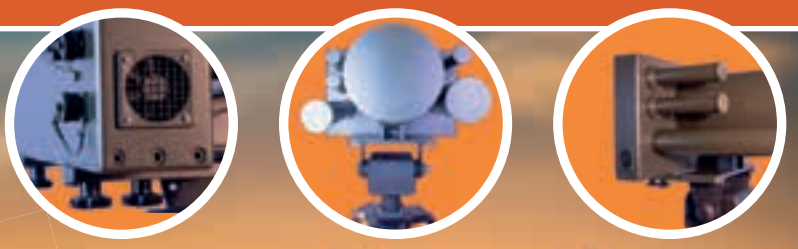
7-10 June Gartner Security & Risk Management Summit 2022
National Harbor, USA
Organiser: Gartner Inc.
Tel: +1.866.405.2511
Email: globalconferences@gartner.com
www.udt-global.com

14-17 June Electronic Security Expo 2022
Fort Worth, USA
Organiser: Electronic Security Association.
www.esxweb.com

MGT europe

DroneTERMINATOR

USING EVOLUTION JAMMER TECHNOLOGY



- **DETECTS**
- **TRACKS**
- **NEUTRALIZES**

DroneTERMINATOR utilizes RADAR on the Ku / X band, 2 Watt, 1 GHz bandwidth

Long-Range Radar System to detect UAVs at a distance of up to 6 km,

with micro-drones typically detected at 1-2 km realistically

JAMMING FREQUENCIES:

400 MHz - 900 MHz - 1500 MHz - 2.4 GHz - 5.8 GHz in n. 2 bands

FEATURES:

- *Fully modular smart design*
- *Precise and fully programmable operation mode for each R.F output*
- *Wideband, clean and precise band occupation*
- *Very good Narrowband and Wideband spectral purity*
- *Flexible and multiple User interface options*
- *Standard USB and Ethernet interfaces available for multiple purposes*
- *Software oriented approach allows for long product life expectations*
- *Careful D.C. Power source design choices for efficient power supply utilization*
- *Waterproof cabinet, rugged and reliable construction*
- *Linux based, User friendly Graphical User Interface with 7" LCD color Multitouch Display*

MGT Europe www.mgteurope.com

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 · BG 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

3DX-Ray 3DX EOD Suits

3DX-Ray, specialist in X-ray imaging technology for the security and military markets, has announced the launch of a 3DX range of EOD Bomb Disposal Suits: the 3DX-EOD Bomb Disposal Suit and the 3DX-Search Suit. The 3DX-EOD Bomb Disposal Suit is a contemporary up-armoured suit designed from the outset to be 3E (Economic, Efficient & Effective) compliant, the 3DX suit arguably provides the best value and the highest level of protection of any comparable bomb suit currently manufactured, offering maximum comfort and flexibility to the operator. The 3DX-Search Suit has been designed for personnel involved in the searching for, and clearing of, suspected terrorist explosive devices. This suit does not offer the higher protection of the EOD Bomb Disposal Suit, it is much lighter in weight, provides all-round 360° protection, while at the same time being comfortable to wear and allowing virtually unrestricted movement.

Survitec micro Liferaft for more demanding flight missions

Global Survival Technology specialist Survitec has unveiled a smaller and lighter single seat liferaft (SSLR) to better equip military fast jet pilots on more challenging missions or when forced to eject from their aircraft over water. The Micro SSLR has been developed in response to increased requirements for a lighter and compact liferaft, resulting in a 20 percent reduction in weight. The liferaft has over 50 percent less packed volume than existing market products and as a result the pilot's personal survival pack (PSP) has additional room available for mission-critical equipment. Designed to form a critical component of a fighter pilot's ejection seat, the Micro SSLR is created from the latest generation of advanced lightweight coated fabrics with an inflatable canopy and floor for maximum buoyancy and thermal insulation. Additional features include a transparent visor, external handles to aid boarding, an internal equipment pocket for essential survival aids, a sea light mounting point and a PLB antenna sleeve in the canopy.

GA-ASI announces Evolution class of UAS

General Atomics Aeronautical Systems, Inc. (GA-ASI) has announced its new category of future-forward unmanned aircraft systems, focused on information dominance and airspace supremacy. Leveraging three decades of experience across millions of successful combat flight hours, the new Evolution line of advanced UAS joins GA-ASI's existing Predator-class and Mojave-class aircraft in delivering next-generation UAS offering advanced, affordable, attritable and autonomous combat power. In the past three decades GA-ASI has launched more than 25 UAS variants, beginning with the Gnat in 1992. Evolution establishes a third aircraft class within GA-ASI, joining the Predator line and recently announced Mojave line of expeditionary UAS featuring short-takeoff and landing capability. Evolution includes the development of GA-ASI's next-generation UAS solutions designed to meet the needs of the US Air Force's vision for its future force, as well as new UAS concepts such as Defender, Sparrowhawk and the recently announced Gambit.

Meprolight introduces Mepro Tru-Vision and Mepro Evergreen

Meprolight has announced the Mepro Tru-Vision red dot sight for optimal tactical advantage and the Mepro Evergreen LED-based illuminated pistol sight for daytime and night-time operations. The Mepro Tru-Vision sight has a built-in light sensor and automatic and manual brightness control system that enables clear visibility of the red dot in any lighting conditions; a combination of an integral motion sensor and configurable sleep time (preset) of 4-8 hours, saving power for extended operation; a non-reflective optics without light signature toward the target; improved, rugged MIL-SPEC mounting mechanism and a protected three-button control keypad. Its short length and lightweight design addresses the need for co-mounting several tactical devices on today's weapon rail (eg magnifier, laser pointer, NVGs, *etc.*) The innovative Mepro Evergreen pistol sight utilises micro super bright LED light sources inserted into both front and rear metal housings to ensure a clear, sharp illuminated three-dot picture. It does not contain any hazardous material and complies with European standards.

i-PRO Introduces multi-sensor camera range

i-PRO EMEA has announced the introduction of its new multi-sensor camera range with deep learning intelligence at the edge. As the next step in i-PRO's AI-ification strategy of the security industry, these new cameras come pre-installed with four powerful AI analytic applications but are also open for customisation with other third-party analytics to meet customers' needs. The new i-PRO multi-sensor cameras are available with three or four imaging sensors in 4K, 6MP and 4MP resolution, ensuring exceptionally detailed image capture for 180° or up to 360° vision adaptable to the installation environment. All these features come in the thinnest and most discreet design currently available on the market. The new i-PRO multi-sensor cameras incorporate a built-in AI processor enabling deep learning analytics to detect people and vehicles. Following i-PRO's open AI strategy, the SDK makes the new range fully open for third-party application developments. The models offer wider coverage capabilities with a larger tilt range than other comparable models on the market, as well as IR LED lighting on selected models to ensure image capture in very dark environments.

3DX-RAY

INSIGHT WHERE IT MATTERS

SECURITY IN A BACKPACK

Rapid deployment.
High quality images.
Fast decisions.

Introducing the new, robust and powerful **ThreatScan®-LS3**. Designed in collaboration with first responders, this is a small, lightweight and compact unit that's designed to be rapidly deployed.

High quality, real-time X-ray images (305 x 256mm), materials discrimination, pan, zoom, DeepFocus™, 3D Emboss, measurement and annotation all enable rapid and accurate decision-making.

Optional tablet PC shown.

The complete system fits in a backpack.

www.3dx-ray.com

An **IMAGE SCAN** company

Milipol Qatar
Exhibition 2022

International Event for
Homeland Security & Civil Defence

14th Edition

24 - 26 May 2022

DECC - DOHA

@Milipolqatar

www.milipolqatar.com