www.intersec.co.uk

intersec

The Journal of International Security

January 2023

RADIO FREQUENCY INTERCEPT

A balanced approach to TSCM

CYBER THREATS 2023

The main security trends for the year ahead

BLOK N MESH

DEFENDER INTERMEDIATE FENCING™

A **robust** and **revolutionary** temporary fencing system, our **DEFENDER INTERMEDIATE FENCING™** is an on-ground relocatable temporary perimeter with the strength of a rigid mesh fence.

Utilising **"V mesh"** and supported by our range of ballast options, this system completely removes the necessity of excavating the ground surface to install a strong, temporary fence, minimising the risk of accidental service strikes, saving time and labour costs with a simple and fast installation.

Available in either **2.4m** or **3m** heights Defender Intermediate Fencing is ideal for site environments requiring a temporary perimeter stronger than standard temporary mesh fencing with no trip hazards on the pedestrian side of the fence.

SCAN TO FIND OUT MORE

UK +44 1226 712500

Blok 'N' Mesh Global Ltd, 10 Christleton Court, Runcorn, WA7 1ST

FR +33(0)3.20.02.00.28

Batisec, 67 Rue Du Creusot, 59170, Croix

www.bloknmesh.com

From the makers of POLMIL®

intersec
Volume 33 Issue 01
January 2023

Cover photograph: Crown Copyright

Editor
Jacob Charles

Principal Consultant Editor
Maj. Gen.
Julian Thompson CB OBE

International Arctic Correspondent
Barry Scott Zellen

Design & Production
jellymediauk.com

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

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

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

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

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

EDITORIAL COMMENT

Barely a day goes by without another major corporation or institution revealing that it has fallen foul of a cyber attack or ransomware. Though it might lack the visceral impact of, say, an explosion, its implications have the potential to be far more wide reaching. Which is why it is fast becoming the weapon of choice for everyone from bedroom-based criminals to state-sponsored actors.

TWC IT Solutions, which describes itself as one of London's leading IT companies for SMEs, revealed in its UK Cybersecurity Report 2022 some worrying trends. According to its research, as much as 41 percent of the most significant UK cyber attacks since 2006 were recorded last year, with malware proving to be the most popular form of attack (with just under 50 percent share) and ransomware the biggest threat to UK business. Of these targets, the retail (12 percent), finance (11 percent) and healthcare (9 percent) sectors were the most affected. Astonishingly, the average number of accounts affected during a data breach was revealed to be 58,317,303. But arguably the most timely revelation to come from the report is the fact that, historically, the first quarter has been the most dangerous period of the fiscal year in terms of hacking activity.

Commenting on the findings, Paolo Sartori, CEO of TWC IT Solutions, told *intersec*: "The alarming increase in business-related cyber attacks has no doubt been caused by poor security management within hybrid working environments, as companies still struggle to deal with the fallout of the pandemic and the extra financial burden this places upon them".

Meanwhile, Jon Fielding – managing director EMEA of Apricorn – sees cyptocurrency as a major area of concern going forward, noting: "I predict in the coming year it's likely there will be an increase in ransomware attacks driven by instability in the global cryptocurrency market. Ransomware attackers have often demanded payments in bitcoin and other cryptocurrencies for their data ransom schemes and the weakening of the crypto market will likely push fraudsters to try and make up their losses with additional attacks."

Simon Chassar, CRO at Claroty, is expecting more state involvement, predicting that: "Governments are going to continue to increase regulations in order to improve the standard of cybersecurity, particularly in the critical infrastructure industry. The US took the lead in implementing regulations after the Colonial Pipeline attack and Biden's 100-day sprint initiative. We are now seeing other nations such as Australia, UK, Germany and Japan following suit and implementing their policies and regulations for critical infrastructure and healthcare environments."

Finally, Andy Harris, chief technology officer of Osirium, highlights that it's not just the major corporations that need to have a robust cyber security plan in place, noting: "We can expect smaller scale attacks, for lower amounts of money, but which target a much broader base. The trend will probably hit education providers hard: education is already the sector most likely to be targeted by a malware, cryptojacking or encrypted attack, according to SonicWall's 2022 Cyber Threat Report." You can read our feature on some of the other main cyber trends in the year ahead on page 8.

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: January 2023

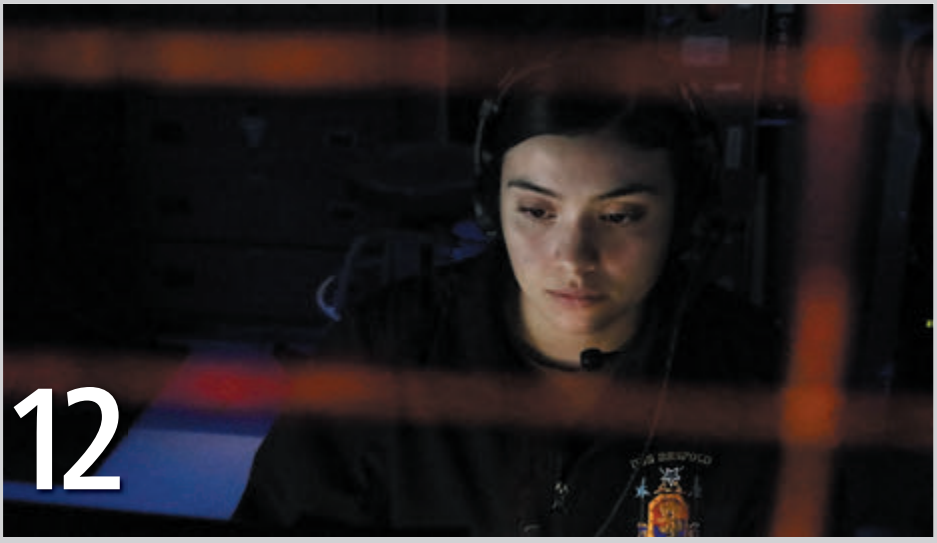
CONTENTS

January 2023 www.intersec.co.uk

intersec

Features

Regulars



Major General Julian Thompson CB OBE Principal Consultant Editor

Lure of the High North

The war in Ukraine and increasing tension caused by Chinese claims involving Taiwan have dominated much of the reporting by security experts in the media over the past year. Hence the spotlight of publicity has swung away from a theatre of potential conflict that was of considerable interest in the days of the Cold War, an era when the West confronted the Soviet Union and the Warsaw Pact and the high Arctic was the scene of much activity over six decades – mostly covert and highly classified. British and American submarines regularly conducted long patrols under the ice and played cat-and-mouse games of deadly seriousness with Soviet boats. These sorties included 'bombers' from both sides using the ice as cover for their missile launch positions.

The Americans and British carry out polar ice cap exercises about every two or three years, but there are calls in some quarters for these to be carried out annually as at the height of the Cold War. Another factor affecting the significance of the Arctic will become increasingly manifest: global warming and the melting of the ice pack. In areas which were thickly iced over all year round, ice has become seasonal. NASA, which monitors ice from space, has stated that the Arctic Ocean ice is declining at a rate of 12.8 percent per decade. Eventually this ocean will be ice free despite all the efforts of the climate change community.

New shipping routes will be opened. Russia will have the most to gain from this, followed closely by China. By skirting the coast of Siberia using the Northern Sea Route (NSR) across the 'roof of the world'; shipping can avoid the choke points of Gibraltar, Suez, Bab-el-Mendeb (the 'Gates of Grief') and the Malacca Straits. Needless to say, the opportunity has not gone unnoticed by President Putin who is putting a major focus on the High North. In July 2022 he signed the latest Russian Naval Doctrine, which stated that the Russian Federation intends to intensify maritime activities in the Arctic and to expand operations in that region and in the wider Pacific.

The USA's response to increased Russian activity in the High North was muted until Russia's invasion of Ukraine and China's increased aggression over the Taiwan issue and their openly expressed ambition to take advantage of the opening of the Arctic Ocean to shipping. Now new resources are being diverted towards Alaska and American submarines are spending more time deployed in the Arctic to train. There have also been calls for more US Coast Guard activity in the High North and the construction of a deep-water port in the region.

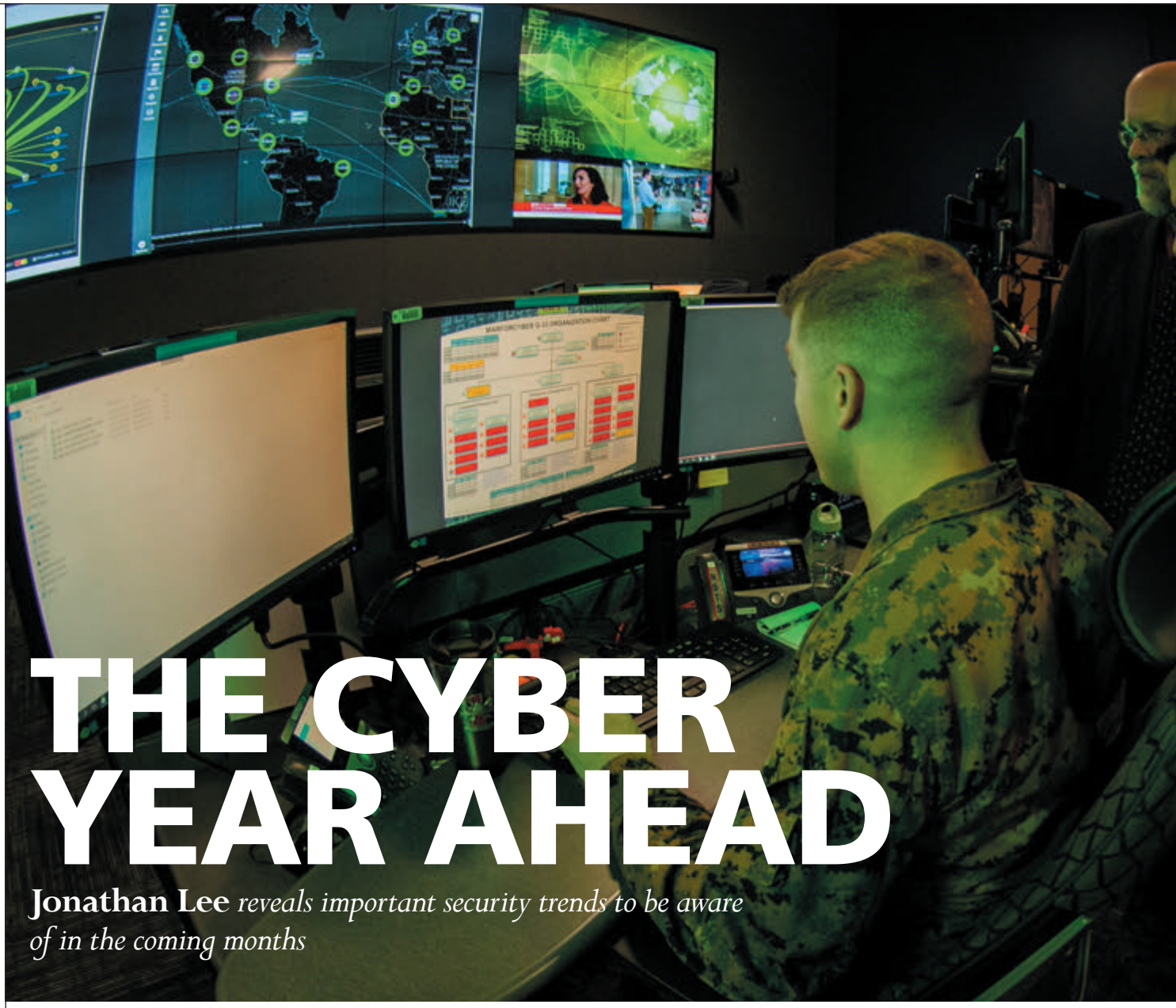
Despite the prospect of less and less ice in the High North in the years to come, there is still a need for icebreakers by those nations that wish to operate in the Arctic Ocean, and the first of three new US Coast Guard icebreaking cutters will enter service in 2027. As an aside these were ordered during the Trump administration and provide a practical example of the lead time involved when ordering new vessels – something not understood by many politicians and members of the public who sometimes call for instant changes of defence policy. It should also be noted that Russia already has a fleet of over 40 icebreakers in response to changing climatic conditions in the NSR.

The High North includes a resource-rich seabed, and this alone means that it has become an area for competition. There are eight states with claims on the resources of the Arctic Region: the USA, Canada, Denmark, Finland, Iceland, Norway, Russia and Sweden, all Arctic Council members. Their geographical locations give them direct access to the north polar regions. Lack of this has not deterred China from announcing a wish to access the region's vast resources by claiming 'Near Arctic State' status, much as the UK could if it wanted to.

The effect of Russia's invasion of Ukraine was to provoke Sweden and Finland into applying to join NATO, changing the geographical balance of power in the Baltic, which in its turn has a knock-on effect in the Arctic. One effect of increased interest and activity in the High Arctic is the likelihood of conflict in that region, which might spill over into other parts of the world. Watch this space.

There are calls for the US to carry out polar ice cap exercises more regularly

Picture credit: US Dept Defense



THE CYBER YEAR AHEAD

Jonathan Lee *reveals important security trends to be aware of in the coming months*

2022 has been yet another year of immense unpredictability. The expanding digital footprints of modern organisations have transformed the security landscape, both in shape and size. And unfortunately, the average enterprise has found itself ever more vulnerable to attack.

In today's environment, traditional cybersecurity controls have become increasingly obsolete, while hybrid work and cloud-based business models have introduced a series of new risks. At the same time, threat actors have continued to develop and deploy highly advanced attack methods – from ransomware to sophisticated digital supply chain attacks – exposing both skills shortages and technology gaps.

We've seen ubiquitous pieces of software become the subject of attacks, the uncovering of the Log4j vulnerability having caused mass concern. And the proliferation and commercial availability of cyber capabilities via ransomware-as-a-service markets has made disruptive cyber tools even more widely accessible to malicious actors. This is all before we mention the impact of the war in Ukraine. Indeed, the conflict has brought the threat of highly organised and sophisticated nation state-backed actors into ever sharper focus as Russia continues to lean heavily into digital warfare as a means of supporting its on-the-ground invasion.

In all spheres, security threats remain as severe as ever. And it seems there is no simple resolution in sight as threat actors continue to adapt their techniques and unlock new and sophisticated ways to take advantage of uncertain situations.

The threat landscape will undoubtedly continue to evolve in 2023. Here, we outline some key security trends to keep an eye on.

INTELLIGENT AND EVASIVE ATTACKS

Threat actors continue to expand their understanding of the security methods and technologies being deployed by enterprises and are adapting their techniques to find ways around them. We expect to see attacks becoming increasingly evasive and intelligent, focused on bypassing commonly used defences.

We're already seeing several methods such as HTML Smuggling and websites with previously benign

Picture credit: US Dept Defense

Russia's invasion of Ukraine has added immensely to the threat landscape

reputations being used to evade existing layers of protection such as firewalls, secure web gateways, malware analysis including sandboxing, URL reputation and phishing detection tools. These methods will only expand and we'll see the layering of multiple detection evasion techniques moving forward. This will make the outdated 'detect and respond' defence that many organisations rely upon as not fit for purpose.

BASIC SECURITY FAILURES WILL CONTINUE

Unfortunately, much of the task is being made easier for adverse actors. The attack on Uber in September 2022, for example, reiterated that basic security failures are continuing to provide wide open doors for threat actors to simply step through. In this specific instance, the perpetrator was able to obtain administrative control over the company's IT systems and security tools by exploiting an exposed PowerShell script, which contained admin credentials for the firm's privileged access management (PAM) platform.

It's a core example of the fact that threat actors often don't need to use highly sophisticated tools or techniques to gain entry to an organisation's network. Sticking to the same tried-and-tested social engineering techniques such as phishing, they continue to find success.

Interestingly, the breach did reveal that Multi-Factor Authentication (MFA) push notifications are exploitable, with the industry now demanding that passwords should be replaced completely in favour of alternative security methods such as FIDO2 passkeys and hardware tokens. However, this is unlikely to happen anytime soon owing to the heavy lifting that would be required to implement such policies at scale.

EXPECT TO SEE AN INCREASE IN BROWSER-BASED ATTACKS

Almost all work is now carried out on the internet. Indeed, Google has reported that end users spend an average of 75 percent of their working day using a web browser. As a result, the web browser has become a ballooning attack surface, and the security industry is now working to respond.

Traditionally, browser-based security controls have been deployed either as a separate endpoint agent or at the network edge, using a firewall or secure web gateway. Now, however, vendors are looking at ways to add security controls directly inside the browser. Google and Microsoft, for example, are offering built-in controls inside Chrome and Edge to secure at a browser level rather than the network edge.

With that said, as browser attacks increase with threat actors exploiting new and old vulnerabilities and using novel attack methods like code obfuscation, file encryption and HTML Smuggling, the need for innovative security technologies is clear.

PURSUE VENDOR CONSOLIDATION WITH EXTREME CAUTION

Gartner recently highlighted that organisations are looking to consolidate their security toolkits, cutting down on the number of vendors they use to reduce complexity, cut costs, boost efficiency and, ultimately, improve security.

Many firms are particularly focussed on working with fewer vendors to satisfy their security needs in areas such as secure access service edge (SASE) and extended detection and response (XDR) to improve risk posture. And while any effort to reduce risk and shore up security defences should be encouraged, we equally advise that organisations proceed with caution in pursuing vendor consolidation. Through vendor consolidation, firms could be at risk of unknowingly removing best-of-breed solutions from their security stack, which may lead to overall weakened security postures.

END USERS SPEND AN AVERAGE OF 75 PERCENT OF THEIR WORKING DAY USING A WEB BROWSER

WEAPONISED FILES

Malicious payloads remain a prevalent feature in most attack sequences. Interestingly, these are increasingly taking the form of weaponised files that have been altered with the intent of infecting a target endpoint.

Specifically, there has been a striking uptick in the use of weaponised decoy documents during template injection attacks. A threat that initially emerged after Microsoft introduced the new Office Open XML File Format specification in 2007 (which made it possible to embed resources directly within a document), attackers today are now injecting URLs hosting malicious templates into XML files. As a result, they're able to execute a form of attack that uses legitimate software to perform nefarious actions – when weaponised documents are opened, they attempt to download and execute a malicious template.

What is particularly concerning about the use of weaponised documents and template injection attacks is the fact that they can appear to be completely benign to many security tools. Indeed, they leave no trace of malicious URLs or exploit markers, enabling them to bypass traditional detection-led solutions.

INTERNATIONAL TENSIONS

As mentioned, the Russian invasion of Ukraine has added a concerning dimension to the threat landscape, paving a path of greater activity among nation state-backed actors. Indeed, Russia has ramped up its use of cyberattacks in the international arena. And as relations between Putin and the west continue to sour, many believe that a full-scale global cyber war could begin to open up.

Time contributing editor and retired 16th Supreme Allied Commander at NATO, Admiral James Stavridis, recently voiced his views that NATO should: "strongly consider a response in the world of cyber, particularly going after Russian military capabilities aggressively" in the face of Russia's cyber escalation.

This, of course, could be an extremely dangerous new frontier for either side to begin exploring more actively. The consequences of a full-scale cyber war would no doubt be far reaching and devastating. However, given the current level of international tensions, it's not out of the question, with several nation-state-lead cyberattacks already making the headlines multiple times in recent years.

POISON COOKIES

The role of the cookie is likely to come under greater scrutiny as awareness over the use and management of personal data continues to heighten. Yes, cookies can make our online lives easier by saving browsing information, keeping users signed into frequently used websites and remembering specific site-related preferences. However, there is growing concern that organisations could be collecting more information than many would typically be comfortable with.

Cyber concerns are naturally beginning to creep in as well. Indeed, it is becoming more feasible for threat actors to poison cookies, leading to session hijacking, the exposure of sensitive information, or even the full-scale takeover of an account that could have catastrophic consequences for user and organisation alike.

EXPECT TO SEE ATTACKS BECOMING INCREASINGLY EVASIVE AND INTELLIGENT TO BYPASS DEFENCES

DEVELOPING DEFENCES

In 2022, the cybersecurity threat landscape has continued to evolve and diversify. And there is nothing to suggest that this momentum will slow in 2023 – a year that's anticipated to provide yet more turbulence. Given the uncertainty, it is important that organisations work quickly to build in the policies, technologies and capabilities required to protect themselves properly.

Unfortunately, many common security solutions have been rendered largely ineffective against current threats, let alone future ones. To be proactive in defending against increasingly frequent and advanced cyber threats, firms need to adopt innovative and progressive approaches to cybersecurity.

While continuous improvement will be key in continually adapting and responding to any changes, vital policies such as Zero Trust will go a long way in improving security postures.

Fortunately, this is a positive trend that we can expect to see in 2023, with many organisations already exploring Zero Trust as a policy in a more active manner. According to a survey from Verizon, presented in its 2022 Data Breach Investigations Report, 82 percent of respondents revealed that they had adopted or were considering adopting a Zero Trust approach to security.

What is the benefit of Zero Trust? Unlike outdated detect-and-respond solutions that weren't built for cloud operating models and browser-based operations that now dominate our working world, Zero Trust has been designed to address risks in the current environment.

It recognises trust in a network as a vulnerability, demanding that all traffic (be it emails, documents, websites, videos or other) should always be scrutinised and verified. Equally, it advocates the 'principle of least privilege' where users are only given access to the enterprise resources and applications they truly need to carry out their daily tasks effectively.

Together, these policies build resilience. Should attackers gain access to a network, they won't be able to move freely, mitigating or limiting the potential damages of any attack. Indeed, there are tools available to support organisations in achieving Zero Trust in the truest sense, with isolation technology being a prime example.

Isolation works by moving the browser execution process away from the desktop and into the cloud, rendering only safe web content on the endpoint. As a result, no active content from the internet – be it good or bad – is ever downloaded directly to the endpoint. Unlike other technologies, isolation isn't 'almost safe'. Rather, it can wholesale stop cyberattacks at source, 100 percent of the time by ensuring that attackers never have an opportunity to execute their payloads ●

Jonathan Lee is Senior Product Manager at Menlo Security.

As tension between Putin and the west increases, a full-scale global cyber war is a distinct possibility

Picture credit: Shutterstock

THE QUEEN'S AWARDS FOR ENTERPRISE: INNOVATION 2020

eskan™

OFFER!

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

Increasing security. Reducing risk.

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

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

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

RADIO FREQUENCY INTERCEPT

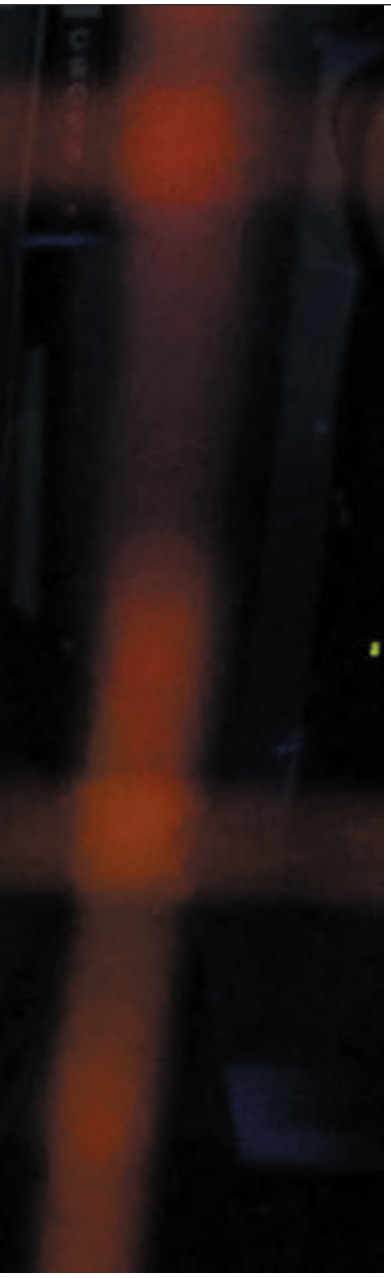
Paul D Turner *explores the symmetrical 360-degree logic, beginning with the threat actor, the professional spectrum warrior and the role of the technical analyst*

The almost over-whelming increase and persistence; not to mention the aggressive nature of state-sponsored threat actors involved in espionage tradecraft and insidious intelligence-gathering efforts across the free world, is a growing concern. All industry sectors; government, law-enforcement, military and national security entities are being infiltrated and attacked from within, under a barrage of continuous attack posturing using multiple methods.

Law-enforcement in particular is being discredited by the same threat actors who spread false, misinformation and activist views across social media channels, all under the banner of so-called free speech, as a megaphone to the masses. The definition of espionage has not kept pace with the reality of new threat actor attack methods; with a shift, and significant variations in tradecraft, for which industry stake-holders have failed to adequately respond to with an updated methodology. Modern threat actors have everything in common with historical forms of espionage, sabotage, infiltration, and the capacity to undermine and bring havoc to the sanctity of democracy, however, thankfully new tactics, methods, tradecraft and the players themselves have evolved.

Social media has become a powerful influence of legitimate information and unfortunately disinformation! A new and very destructive insider class of threat actors has evolved, which no longer needs to infiltrate the society or way of life they wish to destroy. The need to refocus and sharpen the skills of the professional spectrum warrior, therefore, must take on a new approach to every aspect of the role they play in

Picture credit: US Dept Defense



The analyst can extract significant evidence of threat patterns over time that can lead to the surfacing of technical compromises

effectively conducting Technical Surveillance Counter Measures (TSCM) inspections.

New and emerging threat technology has mandated the introduction of a standards-based, focused and balanced approach to Technical Surveillance Counter Measures from the ground up.

It is essential that a structured approach and an entirely different perspective be taken, as part of a modern moving target threat model and risk assessment strategy. There are many aspects of the TSCM inspection process; starting from a position of risk assessment and management, to the rigors of a competent physical inspection, and a demanding radio-frequency, total energy capture requirement.

Total Energy Capture (TCP) is the only modern method of accurately identifying all active emitters within the Operator Defined Target Area (ODTA), and into the extended Functional Target Area (FTA) to capture threat relevant radio-frequency spectra.

Private sector operators are often slow to respond; however, public sector technical security teams are at even greater risk; the higher the classification food chain, the more likely the road to change is virtually non-existent. The ability to hide behind plausible-deniability; a disclose nothing mandate under the banner of classification, and a practice of drinking the cool-aid when it comes to procurement of resources and certification training, results in a progressive erosion of the capability of the entire team or entity.

Corporate boardroom, government offices, military battleground, or within a counter-intelligence, counter-espionage national security role; radio-frequency intercept and signal analysis is a growing national security concern worldwide. Yes, it is all about perspective! The process is only as good as its component elements that include a coordinated effort across a 'winner takes-all' high-stakes game of espionage.

Equipment resources and the technical operator must work in parallel to beat a cunning threat actor, by not only understanding the threat, but utilising defensive and offensive tradecraft as a weapon against the threat actors' brazen and often outwardly obvious objectives.

The modern threat actor fits into one of three general profiles, all of which are just as dangerous when insidious activities are not uncovered by a competent TSCM program. Threat actors can be characterised as amateurs with little or no tradecraft experience; with access to the many surveillance devices sold openly on the internet and plenty of do-it-yourself advice, along with the fact that almost everyone these days qualifies as tech savvy.

The professional threat actor is often a technically skilled individual who utilises dual-use technology and has a remarkable success in blending into society (maybe an insider) and can facilitate the diversion of technology and protected information for personal and/or professional gain while remaining totally under the radar.

The highly skilled state-sponsored threat actor has received specialised training in many aspects of tradecraft from facility penetration, social engineering, cyber-vulnerabilities and often knows more about TSCM offensively and defensively than many technical operators. This category of threat actor has the financial support of the state-sponsor. Careful approach and persistence often yield remarkable success in the compromise, theft or diversion of seemingly unimportant, unconnected, unprotected information to highly protected sensitive or classified information. Unfortunately, in a modern-day threat management reality, the definition of a state-sponsored threat actor must include individuals or entities that elevate or recruit, if you will, themselves to the position of a state-sponsored threat actor. This new type of threat actor is already embedded, trusted and is often more difficult to detect. We are seeing more reports of detected espionage incidents worldwide and often pat ourselves on the back for a job well done. But not so fast, technical operators falsely believe that their defensive countermeasures are working.

My extensive experience, leads me to believe that the successful detections are a drop in the ocean; and that there are so many active threat actors across a larger more diverse and highly structured attack posture that it simply makes sense that a few threat actors are bound to be detected, leading to a false sense of national security.

ALL INDUSTRY SECTORS ARE FACING THE VERY REAL PROSPECT OF BEING INFILTRATED FROM WITHIN

We are seeing state-sponsored threat actor detection across the private sector and we as an industry are driving both a change in approach and are no longer willing to accept obsolete methodology as an approach to TSCM in today's complex threat environment.

There is considerable misinformation resulting in limiting factors and unknowns that continue to be perpetuated by key industry players. When the technical operator buys a product that claims to decode signals for example, the excitement builds until the realisation hits that the intelligence provided has little or no value whatsoever from a TSCM perspective.

When the operator fails to understand their role in the mitigation of technical vulnerabilities and real-world functional compromises, the entire process will fail leaving a false sense of accomplishment for the operator and unfortunately a false sense of security for the end-user. Understanding capabilities, limitations, and more importantly, the differences between the technical operator and technical analyst role is also crucial!

The role of the analyst is not seen as a common TSCM function, but rather a SIGINT or counter-intelligence role – separate to, and on an entirely different level, apart from the field operator role. The analyst can extract significant evidence of threat patterns over time that can lead to the surfacing of technical compromises. Operator activities on their own merits simply cannot identify such threats in the immediate here and now, during limited, time-on-target inspections. It's the technical operator that feeds the analyst by providing maximum effort, raw and first cut filtered data for analytical consideration.

This all-important data is derived from many functional tasks, including, understanding the threat, the anticipated risk, the context in which data is captured, while understanding gaps in the raw data source files provided by automated collection

strategies and operator-assisted capture is essential. However, without active intelligence beyond the spectrum reference data, the mission will likely fail to identify deeply buried threat activity.

THE DEFINITION OF ESPIONAGE HAS NOT KEPT PACE WITH THE REALITY OF NEW ATTACK METHODS

Knowing what to look for and where to look for it, is the analyst's role; not that of the technical operator, who is primarily tasked with providing the analyst with the widest possible range of radio-frequency and operationally relevant counter-intelligence data. Detecting something in the here and now, versus the long-term strategy of remote spectrum surveillance and monitoring, are distinctly different functions shared across the operator and analyst.

The analyst's job is to put it all together and extract actionable radio-frequency intelligence that will provide clarity and focus for the technical operator in deploying and redeploying resources relative to the risk identified. This process leads to a more relevant intelligence focus by the analyst, often resulting in a positive-finding of compromise; with the identification of the threat actor as a definitive objective.

This is all a rather circular process in which the technical operator and analyst work in parallel to achieve a positive outcome. Unfortunately, many analysts are not field deployed and lack a practical appreciation of the actual circumstances of the data for interpretation or the target environment in which the data was derived.

It is recommended that in a standards-based approach the analyst must be trained in the operational deployment process of a competent technical inspection before being tasked with the analytical evaluation of captured reference data.

Field decoding and competent signal level analysis of potentially thousands of ambient signals is simply not realistic, let alone the fact that many threat-specific signals are highly encrypted; and is therefore a waste of valuable time-on-target. Capturing field IQ and feeding the analyst from a maximum effort approach allows the technical operator and the analyst to share the responsibility of threat identification by the application of individual skill-sets that differ across the roles. The currently accepted minimum standard for IQ capture is 160MHz of real-time radio hardware bandwidth to address a modern threat reality ●

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' 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.

TSCM EQUIPMENT RESOURCE LIFE-CYCLE

The effective life-cycle has decreased during the past four decades, but operators continue to deploy resources well beyond the effective life-cycle.

1980 to 1990 | Effective Life-Cycle ..... 7 to 10 Years
1990 to 2000 | Effective Life-Cycle ..... 5 to 7 Years
2000 to 2010 | Effective Life-Cycle ..... 3 to 5 Years
2010 to 2020 | Effective Life-Cycle ..... 1 to 3 Years
2020 and beyond | We are seeing the effective life-cycle drop to 12 to 18 months for this coming decade.

Radio-frequency intercept and signal analysis is a growing national threat, from the corporate boardroom to the military battleground

Picture credit: NATO/IMS

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!

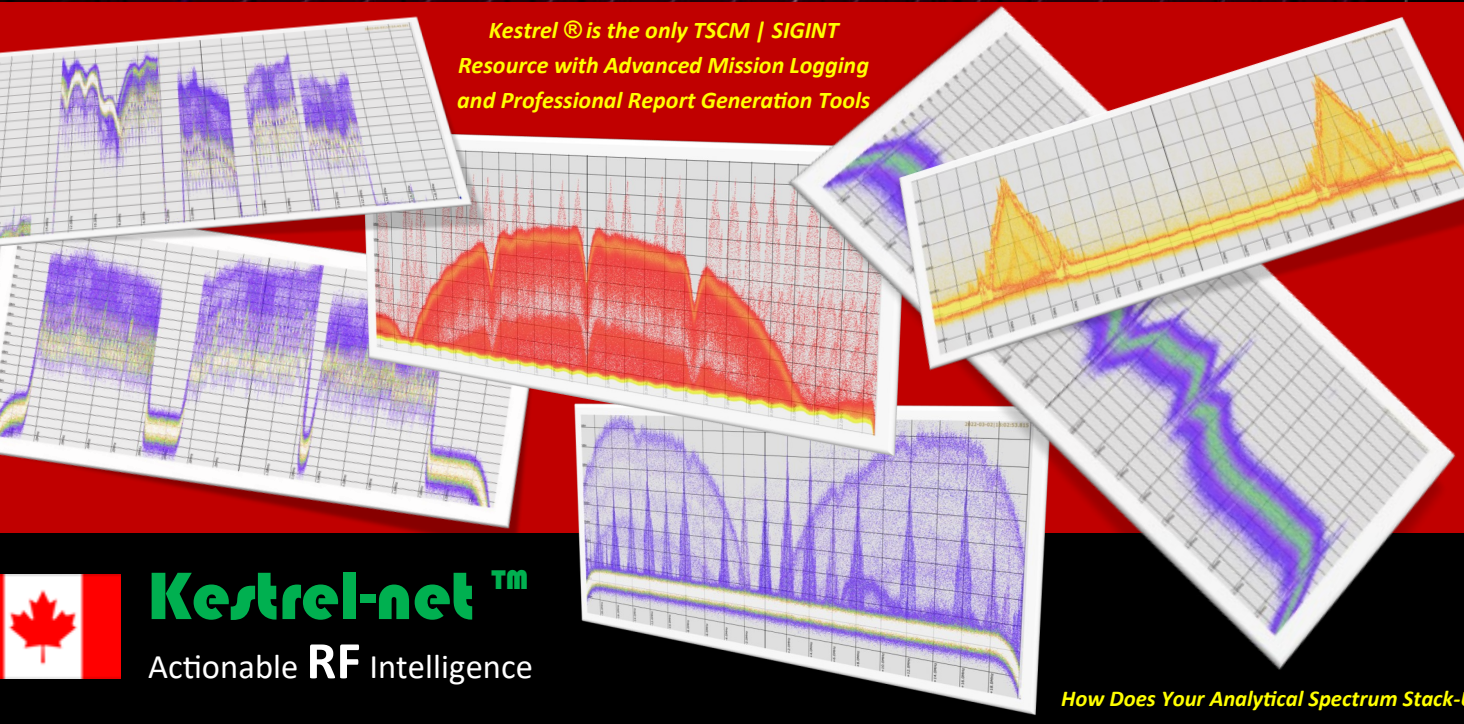
Kestrel TSCM ® Professional Software

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

NATIONAL RESILIENCE

Robert Hall *considers the important lessons learnt from Finland's Winter War and the parallels that can be drawn with the current conflict in Ukraine*

Several commentators have highlighted the similarities between the first Finnish Winter War (1939-40) and the ongoing Russo-Ukrainian War. While not absolutely a case of history repeating itself – it never does – the two conflicts do have many uncanny parallels. While it is premature to compare and contrast the outcomes, it is possible to draw some lessons for today on the nature of national resilience as revealed by two defenders facing a much larger aggressor at different historical moments.

The value of the analysis here is in not just the historical significance but also the applicability of elements to a national resilience strategy. This is perhaps particularly true for the UK, which launched its long-awaited national Resilience Framework in December 2022. As anticipated, the framework addresses aspects of transparency, preparedness and a whole-of-society approach.

The first Soviet-Finnish War took place between the Soviet Union and Finland in 1939. In spite of a Soviet-Finnish Non-Aggression Pact, Joseph Stalin thought that the pro-Finnish movement in southern Finland posed a direct threat to Leningrad (now St Petersburg) and that the local area of Finland could be used to invade the Soviet Union or restrict fleet movements. He saw an invasion as the way to prevent this.

The war began with a sudden Soviet invasion of Finland, three months after the outbreak of the Second World War: it ended three-and-a-half months later. The capital, Helsinki, was one of the first Soviet objectives. Despite superior military strength, especially in tanks and aircraft, the Soviet Union suffered severe losses and initially made little headway, failing to take the capital. The League of Nations deemed the attack illegal and expelled the Soviet Union.

In the end, the aggressor's larger forces prevailed. Finnish concessions and territorial losses exceeded pre-war Soviet demands. Finland ceded 9 percent of its territory with the largest portion of land close to Leningrad, as well as its second largest city, much of its industrialised territory, and 30 percent of its economic assets relative to March 1938. About 12 percent of

Picture credit: Ukraine MOD

Ukraine has survived with considerable support in armaments from Western nations

Finland's population (at least 422,000 people) were evacuated and lost their homes, but all were taken in by fellow Finns and were provided with their own homes by 1945.

The belief by the aggressor that a short war with the early capture of the capital would ensue because the opponent was weak, unprepared and ill-equipped proved wrong in Finland's past as well as Ukraine's present. The latter has survived with considerable support in armaments from Western nations, an asset that the former was denied particularly towards the end of its war and part of the reason for it seeking a settlement. In both settings, the belligerent's fear that his territory was (falsely) under threat was the cause of the hostilities.

The initial assessment that the aggressor would not attack also proved unfounded in both cases. Finland's ferocious resistance in the Winter War convinced Stalin to leave Finland independent even though some territory was surrendered. This may well be one outcome in Ukraine if a negotiated settlement materialises.

Another common feature is that when small tactical groups are defending local territory, they can have disproportionate effects on a much larger attacker. Finnish soldiers were fighting for their country, their families and their independence, just as Ukrainian soldiers are today. Finnish forces initially deployed tactics that were suited to fighting an inflexible foe. Russian forces invading Ukraine have been prone to similar inflexibility from the start of the current conflict. The common experience has shown the value of task-oriented or mission command as an operating principle whereby units have the agility to apply orders depending on the circumstances on the ground. Western armies have adopted this concept for many years but Russia has long resisted in line with its political indoctrination.

THE UK LAUNCHED ITS NATIONAL RESILIENCE FRAMEWORK IN DECEMBER 2022

At the top levels of leadership, there are also parallels. In Finland's case, General Mannerheim was a master of allocating scare resources, judging relative dangers posed by Soviet threats on different fronts, keeping a cool head in difficult circumstances, and retaining the confidence of his troops. President Zelensky of Ukraine is a latter-day proponent. Nonetheless, because of its resistance and tenacity, Finland did retain its sovereignty over most of its territory and certainly elevated its international reputation. Yet, the war had a profound effect on Finnish psyche and subsequent political positioning: Ukraine may experience a similar outcome today.

National motivation based around homeland identity and core values generates a force multiplier of immense proportions. The Finnish and Ukrainian experiences are cases par excellence of national resilience. Both nations are based not on institutions or ethnicity but on self-reliance, national identity and solidarity. These are important factors that in the final analysis trump wealth and prosperity, and are worth preserving and nurturing in other countries.

As Finland and Ukraine demonstrate, national resilience is most focused when it is in response to a clear and present danger, and the population can be readily mobilised and motivated to resist. The danger can be internal or external, environmental or human. When the danger is not so apparent or a 'slow burn', the task becomes more difficult, but nevertheless still demands careful preparation, planning and communication.

Resilience begins with a strategy, but it can only be effective when translated into meaningful actions for those on the ground to apply. These actions must be accompanied by resources and clear plans. Other essential requirements include: sound leadership at all levels; trust in politicians and decision makers; partnerships across the public, private and voluntary sectors; subsidiarity as localism is where tactics are best applied; and a wide communication network with consistent, clear messaging.

Finland and Ukraine prove that resilience is about individuals, communities and organisations working together for the national good. It is more than simply having emergency measures in place: it is about a collective mindset in the civil society that can be translated into agile and adaptive behaviours across the board when circumstances demand and the spirit wills. As Lord William Hague wrote in the press: "An individual can prepare for the new age of resilience by buying a generator, storing water purification tablets and fortifying the garden gate in readiness for the apocalypse". He describes that as retrenchment. It is better, he argues, to adopt a principle of developing contacts with neighbours, communities and partnerships so that everyone knows how help can best be delivered thereby allowing the whole community to stand together: that is reinvention. Quite simply, Finnish history and the latest events in Ukrainian reveal that we can be greater than the sum of our individual parts but those parts need to be oiled and motivated in advance. That is one reason that Finland (together with Sweden) decided to apply for NATO membership and Ukraine is keen to do likewise.

NATIONAL MOTIVATION GENERATES A FORCE MULTIPLIER OF QUITE IMMENSE PROPORTIONS

Ukraine reinforces the lesson that the classic forms of armed warfare on European soil have not become redundant and that in spite of modern weaponry, brutal, attritional military operations still play a key role in deciding sovereignty. This will cause planners to rethink the scale of ammunition stockpiles and logistics, the veracity of the rules of war (the Hague and Geneva Conventions) and the role of the public-private sector in equipping forces for sustained battles. It also raises the question of how we prepare all parts of our societies for national emergencies that we thought had receded into history or chosen to ignore.

As public safety is the number-one task of any government, it is incumbent on those in authority to communicate to the population at large the need to prepare for shocks and stresses, as well as the importance of a social contract whereby individuals are aware of their societal responsibilities in a national emergency. As Covid-19 vividly illustrated, we are all in a national crisis together. Without such a focus, there is a danger of introspection – which can easily result in divisions along political parties, as well as ethnic and single-interest groups. That can only diminish our national resilience ●

Robert Hall is an independent consultant on resilience. He is the former Executive Director of Resilience First. His book 'Building Resilient Futures' will be published by Austin Macauley in early 2023.

Finland and Ukraine prove that resilience is about individuals, communities and organisations working together for the national good

Picture credit: Ukraine MOD

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

INTERNATIONAL SECURITY EXPO

26-27 SEPTEMBER 2023. OLYMPIA LONDON

EVOLVING SECURITY THROUGH INNOVATION

With innovation in security more important than ever, International Security Expo offers the ideal platform to showcase the most cutting-edge products and solutions.

Exhibit and meet a high-level audience of global security professionals responsible for protecting people, businesses, critical national infrastructure and nations, all looking to source the latest innovations from across the sector.

10,000+
SECURITY BUYERS

350+
INTERNATIONAL EXHIBITING COMPANIES

SECURE YOUR STAND **TODAY**

VISIT: internationalsecurityexpo.com

CALL: +44 (0)20 8947 9177 | EMAIL: info@internationalsecurityexpo.com

HEALD®

DESIGNERS, MANUFACTURERS AND INSTALLERS OF AWARD WINNING PERIMETER SECURITY PRODUCTS

Secured by Design
Official Police Security Initiative

PSSA
Perimeter Security Suppliers Association

SafeContractor
SafePQQ
VERIFIED

OSPA WINNER 2022
Outstanding Security Equipment Manufacturer

MADE IN BRITAIN

Constructionline
Gold Member

SafeContractor
APPROVED

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

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

@healduk Heald Ltd Heald Ltd HealdLtd

Picture credit: Jacksons Fencing

PROTECTING THE PUBLIC

Peter Jackson *outlines his physical security trends for 2023*

Security managers responsible for the physical protection of people and property must be aware of significant trends coming into play in 2023. King Charles III's coronation and countrywide celebrations on 6 May are events which many security professionals will need to prepare for. Equally, with industrial action and international terror threats likely to be ongoing through the year, our sector must adopt the latest tools to ensure security and peace of mind.

As we head into a recession, it will also be a tough year of economic-driven crime, materials and labour shortages, and rising costs. Here are my trends predictions for 2023, with some tips on how to address physical security and the protection of people in the year ahead.

MAJOR EVENTS

Temporary and permanent security measures for public and private sites being used during big events, such as the coronation in May, should be a consideration for security managers. It will be vital to ensure any temporary measures are robust enough to withstand large crowds.

Be ready for new legal requirements to protect the public. The counter-terror Protect Duty bill – otherwise known as Martyn's Law – moved ahead another step in the legislative process in December, with draft legislation set to be published this spring. There is no doubt that this will bring huge changes to the way venues, public spaces and the people who use them are protected.

Currently, apart from at some sports grounds or on public transport, there is no requirement for anyone to take any steps to prevent such incidents, whether by installing

Property owners need to consider building and maintaining a security-conscious culture

security measures such as Hostile Vehicle Mitigation (HVM) barriers, having an action plan or giving training. However, in the wake of the attack at the Manchester Arena in 2017, when 23 people died after attending an Ariana Grande concert, this is about to change. Following a campaign by Figen Murray, whose son Martyn died in the incident, the Government is now seeking to introduce new laws that will make it an offence not to take preventative action or know what to do should an attack take place. The Protect Duty introduces a duty to protect.

SECURITY-CONSCIOUS CULTURE

It's increasingly important to consider security as a combination of physical and behavioural measures. Security professionals hired to make sites safe should consider installing physical measures such as fences, bollards, CCTV and blast-resistant glazing. Certainly, the property owner will need to consider building and maintaining a security-conscious culture.

Choosing a security product, such as fences, bollards or CCTV, and hoping for the best is not enough. Responsible building firms will recommend a fencing and gating system, which does not contradict other safety measures – such as fire regulations and health and safety codes.

As the year progresses, I'd advise organisations and their chosen security partners to adopt a fully integrated approach to security. I'd also advise using the information and recommendations made accessible by the government and police services in order to be ready and able to comply with the weighty new responsibility of the Protect Duty.

At Jacksons, we support the investment in integrated security in public areas. With our security gates, fencing and access systems we have demonstrated that it's possible to design a venue that is both secure and aesthetically pleasing; integrating into its surroundings. It is now well known that user experience of venues can be dramatically enhanced by sensitively applied security measures.

In 2023, the general public is more likely to feel at ease and reassured when they attend events where physical safety has been seamlessly incorporated. Finding the right balance between comfort and protection is crucial. And by working closely with specialist suppliers of security products, venues can be reassured that offering a safe environment is not as challenging as it may appear.

CONTACTLESS SECURITY

Post-Covid, the use of contactless technology has boomed, as it removes the need for physical contact. People want instant and effortless ways to gain access and go about their daily lives. While tech can pose risks of hacking and connectivity failures, there is an unstoppable drive to automate and digitise most walks of life.

Contactless security for location access is therefore becoming more commonplace. Biometric access, using facial recognition, fingerprints, iris scans and facial recognition to identify authorised personnel for physical access into a building or site, is already becoming the norm. During 2023 we will see more adoption of technologies such as Bluetooth Low Energy (BLE) and smartphone Near Field Communication (NFC) keyless entry, as well as QR code scanning for temporary access.

For added security, multi-factor authentication (MFA) – the use of more than one method of identification – is likely to become more widely adopted, making it much harder for unauthorised individuals to gain access.

SUSTAINABILITY

Sustainability continues to be a huge trend and businesses of all sizes are facing more intense pressure to improve their sustainability initiatives and achieve carbon reductions. In 2023, Ministers will launch a consultation on implementing a proposal from the Environmental Audit Committee (EAC), which has the potential to address the source of 25 percent of the UK's greenhouse gas emissions – from the built environment.

IT IS VITAL TEMPORARY MEASURES ARE ROBUST ENOUGH TO WITHSTAND LARGE CROWDS

As a new legal framework for net zero in the built environment is drawn up, it's important that sourcing more sustainable materials for new builds becomes the norm. When it comes to security and perimeter measures, look for eco-friendly, sustainable fencing and gates, which use responsibly sourced and regulated timber.

The right species of timber for the purpose should be selected by manufacturers before the all-important preservative treatment, design and construction process. If all these elements are right first, then any sustainability/responsible sourcing certifications have a more meaningful context as the best use has been made of the timber and a product that provides a long life ultimately means less deforestation.

VALUE AND CARBON-EFFICIENCY ARE INTERLINKED

When it comes to decisions around perimeter and security fencing for residential and commercial property developments, there's recognition now that lower-quality panels and gates are less sustainable, and probably more expensive in the long run. This is because replacements and repair are more likely, increasing waste.

In 2023 as recession bites, we will see construction firms and security managers thinking carefully about the lifetime cost of fencing and gating solutions, looking beyond upfront product costs to get the best value and lowest carbon impact in the longer term. The length of the guarantee matters enormously in this context.

RECESSION-DRIVEN CRIME

A major trend affecting the UK is the cost-of-living crisis which will likely become a recession. Usdaw, the retail workers' union, has reported that shoplifting is up 21 percent this year, largely driven by the economic downturn and people struggling financially. For many large town centre stores, supermarkets and units on retail parks, the rear doors and delivery areas can be targeted by criminal gangs. It's not uncommon for thefts to be perpetrated from pallets or cages that have been unloaded off lorries and are waiting to be moved into the building. After-hours break-ins are a risk for all store and warehouse owners, particularly over the festive season when a lot of high-value stock has been delivered to shops and supermarkets.

While more help from the Government to support retail workers and the businesses shoplifters target is certainly needed, boosting practical security measures can go a long way to deterring these kinds of crimes in the first place. Many businesses will increase their level of perimeter security to help prevent an expected crime level increase. Commercial properties and public use sites may need to have this factored in. Specialist fencing for high-value residential properties may also be a wise consideration for property managers.

MULTI-PURPOSE FENCING

Effective perimeter security for these sites should be specified in line with the potential threats, the site itself and its topography. One of the key challenges when establishing security fencing for retail sites is deterring intruders while making access easy for customers and staff. What's needed is fencing that isn't too austere in appearance, but nevertheless, does a good job of shielding external parts of the site from harm and intrusion.

Difficult-to-climb security fencing provides an obstacle that will deter thieves, vandals and other intruders from gaining access to a retail business. It's therefore important to select a fence high enough and sturdy enough for the job.

Supermarkets, in particular, represent the end of the supply chain and need to be protected from theft. Measures should also be taken to reduce noise pollution to surrounding areas and control access during times when the shop is closed to the general public, but delivery vehicles still need to be on the site. One solution is to install sliding gates and noise-reducing acoustic barriers around supermarket delivery areas.

Another challenge is minimising the attention drawn to a site with potentially high-value stock inside. Security fencing can sometimes make a site more of a target and attract unwanted attention. If the site is close to residential areas it's also important to avoid an imposing presence, which may negatively impact its surroundings, and put people on edge. Adding timber fencing and a traffic barrier to car parks can make the site secure, but still welcoming to shoppers while delaying any quick vehicle getaways in the event of shoplifting. Slowing traffic in car parks is a sensible way to keep pedestrians safe too.

GOODS, CARGO AND BORDER PROTECTION

In 2023, with supply chain disruptions and delays still causing havoc for businesses post-Brexit, measures will need to be taken to ensure ports and shipping containers are better protected.

Unfortunately, goods held at the border between the UK and Europe will still be an issue going. The likelihood is that demand will rise for perimeter security fences and gates at major ports. Jacksons supplied fencing and gates at the Eurotunnel terminal at Calais for a 14.5km stretch of its 41.8km perimeter, with the aim of keeping people safe and out of harm's reach – whether it's those attempting to enter the Eurotunnel site unauthorised or those responsible for preventing them from doing so. The fencing and gates specified for the project were based on the proven '358' wire mesh panel system, a versatile design with welds at each intersection for strength and small apertures to eliminate foot and finger holds and prevent objects being passed through its fabric. It also provides resistance to cutting by conventional hand tools and is employed extensively in higher security applications where it is supported with detection and surveillance technologies. As mentioned earlier, taking an integrated, holistic approach is paramount for the success of these high-security fencing products.

As the government attempts to clamp down on small boats crossing the Channel shipping immigrants – at great danger to themselves – into the UK, it's highly likely we will see a return of other kinds of attempts to gain entry, perhaps through rail, road and shipping transport hubs once again. Security fencing will be in demand and security professionals will need to collaborate closely with government and border force agencies to meet new challenges in a timely manner.

Security and safety contingencies must be baked into operations at these key sites. Professionals in our sector will certainly have their work cut out in 2023 ●

Peter Jackson is managing director of Jacksons Fencing.

It's important to avoid an imposing presence, which may negatively impact its surroundings

Picture credit: Jacksons Fencing

MGT SST-33

DATA SHEET

STEREOPHONIC DIGITAL RECORDABLE STETHOSCOPE - WITH PERSPEX DUST COVER

OVERVIEW

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

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

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

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

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

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

TECHNICAL SPECIFICATIONS

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

262 Chamberlayne Road NW10 3LN - London - UK
Telephone: +44 (0) 208 451 3024 - Mobile: +44 (0) 777 039 0324

ELECTRONIC COUNTERMEASURES

IPS EQUIPMENT & SWEEP TEAM SERVICES

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

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

Looking for a

VIDEO POLE CAMERA
2.0 INSPECTION TOOL

EDD-24T NON LINEAR
JUNCTION DETECTOR (HANDHELD)

TSCM TRAINING
COURSES &
CERTIFICATION
UK/US/GLOBAL

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

International Procurement Services (Overseas) Ltd,
118 Piccadilly, London, W1J 7NW Email: sales@intpro.com

Phone +44 (0)207 258 3771 FAX +44 (0)207 724 7925

Rapid Quote:

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

needle in a haystack?

ORION HX DELUXE (TWIN-HEAD), NON LINEAR JUNCTION DETECTOR

***OSCOR BLUE* FULL 24GHz SWEEP IN 1 SECOND**

***TALAN 3.0* DIGITAL PHONE ANALYSER**

RAKSA IDET SELECTIVE RF DETECTOR (MICRO TSCM DEVICE)

ORION 2.4 HX NON LINEAR JUNCTION DETECTOR

TSCM Equipment supply, training and de-bugging services

The preferred choice of Government & Law Enforcement Agencies worldwide.

Web: www.intpro.com

Picture credit: US Dept Defense

CROWD-SOURCED CYBER ARMY

Ziv Mador *reveals the significance of the Ukrainian cyber counter-offensive*

Over the last year, the ongoing Russia-Ukraine war has brought geopolitical unrest and associated nuclear threats. This has been one of the most intense European conflicts of recent times with the crippling economic impact of this war being felt by nearly every country across the globe. However, the conflict hasn't panned out according to the traditional trajectory of military warfare. While the mainstream media is significantly focused on the ground proceedings, the war is also being fought in the cyber field. This has very much been an active, hybrid war being fought in both cyber and physical domains.

Cyberwarfare isn't new. We have seen a wide range of state-sponsored and hacktivist attacks amidst global conflicts. However, the scale of the Ukraine war has provided a window into how war and cyberwarfare will look in the future. During the initial phases, Ukraine was mostly on its back foot in the cyber domain, as Russia came into this war with a strategically planned cyber offensive. As earlier reports from Trustwave and other security researchers show, Russia has been using a wide range of targeted attacks to either destroy or gain control over critical information and communication systems in Ukraine.

It is unsurprising that Russia gained the initial upper hand in cyberwarfare due to its existing networks

Ukraine's cyber operations are carried out by an open collective of remote hacktivists and more specialist professional operatives

of highly skilled state-backed groups such as APT28, SANDWORM, SVR, DRAGONFLY and more. These groups have been active for several years and have contributed to some of the most infamous cyberattacks in recent history.

Ukraine's counter-offensive strategy was based on several loose collective efforts. Unlike Russia, the country was less known for its state-sponsored cybercriminal activity, rather Ukraine's counter-offensive tactics included the efforts of its individual hackers and security professionals. Surprisingly, however, these isolated and scattered groups of digital talents and hackers have now grown into a fully-fledged IT army – an army which is continuously foiling Russia's cyber warfare tactics through strategically coordinated defensive and offensive tactics.

Ukraine's counter-offensive efforts started with a cry for help from Yegor Aushev, one of the leading Ukrainian entrepreneurs in the cybersecurity industry. On 24 February, when Russia began its invasion, Aushev and other security professionals across the world knew that it was going to be a hybrid war. He went onto several hacker forums, calling for the help of all security professionals and individuals with any offensive cyber skills.

This initiative was also followed up by Mykhailo Fedorov, the country's Minister of Digital Transformation, as he called for digital talents on social media to join Ukraine's IT army. What followed was a large number of volunteers and hacktivists coming together to serve Ukraine's cyber front.

Aushev, along with other defence ministry officials, has been coordinating the groups, assigning specific roles to everyone and dividing the team into specific defensive and offensive units to conduct cyber espionage campaigns against Russian forces, according to Stefan Soesanto's CSS Cyberdefense Report. This translated into the development of a well-organised group that has been critical in Ukraine's advancements and achievements so far in this war.

Currently, Ukraine's state-backed cyber operations are divided into two groups: an open collective of remote hacktivists, responsible for carrying out DDoS attacks against Russian infrastructure and an in-house team of operatives which plots and carries out more complex cyber operations.

Ukraine's counter-offensive operations have been largely based on DDoS attacks against critical infrastructure like airports, government facilities, public transport and private enterprises in Russia. Some of their biggest achievements so far include disrupting Moscow's Stock Exchange site, federal tax services and breaching the Central Bank's database. Ukrainian cyber operatives exfiltrated thousands of internal documents from the Central Bank of Russia and publicly leaked 2.6GB of sensitive data. Most attacks did not last long and had a short-term impact.

The Ukrainian IT army also targeted Sberbank, one of the largest state-owned banks in Russia. Although the attack didn't have any major impact, it significantly disrupted the bank's payment system services for 24 hours and triggered a small loss of funds.

Most notably, Ukrainian cyber operatives were able to successfully launch a continuous succession of DDoS attacks against Mir, Russia's national online payment system. This attack resulted in the suspension of major payment services in the country, including Mastercard, Amex, Visa and PayPal.

The continuous success of these attacks was largely a result of Ukraine's efficient information and resource pipeline. From the outset, Ukraine wasn't just recruiting the best hackers and security professionals, rather the leaders that have been transforming digital talents into highly skilled cyber operatives through a continuous supply of resources, information and guidance. They have been launching social media campaigns to urge anyone with basic computer skills to join the IT Army of Ukraine and then equipping them with complete step-by-step tutorials, toolsets and guidelines on crafting targeted DDoS attacks.

WHILE THE FOCUS HAS BEEN ON THE GROUND, THE WAR IS ALSO BEING FOUGHT IN CYBER SPACE

Trustwave's SpiderLabs researchers came across several Ukrainian Facebook, Telegram and Twitter advertisements that included extremely detailed guidelines and toolsets for launching DDoS attacks against specific Russian targets. This incredibly extensive resource pipeline allowed even the most novice computer operative to join Ukraine's cause and contribute to its counter-offensive cyber measures.

Beyond the discussion of warfare, there is an important lesson in Ukraine's offensive cyber strategy. Its tactics have demonstrated that an effective flow of information and resources is critical for the field of cybersecurity. This is very relevant from a business or industry perspective as well. No matter what technology and solutions we implement, without an effective allocation of information and resources, even the most advanced cyber strategy will fail. Of course, crowd-sourced cyberwarfare isn't new. In the last decade there have been many instances of global conflicts, when a country's cyber offensive and defensive operations were reliant on collective cybersecurity talents. For instance, during the Rohingya conflict between Bangladesh and Myanmar, several cyber collectives from both sides targeted critical infrastructures and disrupted government networks and services.

However, Ukraine's IT army is the most prominent example of crowd-sourced cyberwarfare to date. Never has crowdsourcing been used at such a scale in an active war. What's more exemplary is how this crowd-sourced IT army of Ukraine's operations has matured during the past year.

Initially when the call was made by Aushev in February, Ukraine's cyber operations were managed through Telegram. The platform's end-to-end encryption and high media compression features made it the perfect central communication point for thousands of cyber collectives that wanted to be a part of Ukraine's cyber frontier.

In addition to tasking the IT Army of Ukraine with launching DDoS attacks against specified Russian targets, other attack types encouraged on Telegram's 'itarmyofukraine2022' channel include reporting Russian Youtube propaganda channels and signing petitions to block PayPal, GitHub and similar services in Russia. New targets and operational methods continue to be posted in the 'itarmyofukraine2022' channel.

The growth in size and mission scope created a need to support the IT army of Ukraine's members by furnishing them with scripts to run and highlighted an opportunity to develop and introduce educational materials and hacking guidelines, which could be accessed and shared via an educational portal. This led to the development of HackYourMom – a community-driven portal, lab and academy to equip the cyber army of hackers with sufficient guidelines, scripts and other resources.

The HackYourMom team introduced multiple educational articles, from OSINT basics to reverse engineering articles and important lessons on Youtube. The wide range of materials on the platform included everything someone needed to go from a novice programmer to an experienced hacker and security operative. This is how Ukraine systematically used its crowd-sourced group of volunteers and hacktivists to form a well-organised and fully operational nation-state actor.

THIS WAR HAS PROVIDED A WINDOW INTO HOW CYBERWARFARE WILL LOOK IN THE FUTURE

In order to stay competitive, a key goal for Ukraine was efficiency, and this is where building a robust educational process became a key part of the country's counter-offensive strategy. On 1 April, 2022, the IT army of Ukraine launched an automated chatbot on Telegram that responds to questions and provides an instruction guide detailing how to execute DDoS attacks. Not long after the chatbot became active, the IT army of Ukraine created a website sharing its target list and details on how to launch a DDoS attack. The aim was to significantly reduce the time it takes to develop, script and deploy a DDoS attack.

In May, an attack automation function was introduced to the Telegram chatbot, which allowed volunteers to grant bot access to their cloud resources. This action could allow a coordinated attack from all available servers, maximising the scale of a DDoS attack. To prevent proactive fixes on the attacked resources, the IT army of Ukraine closed sourced its mhddos_proxy tool to gain better operational security against abuse from hostile threat actors. The cyber collective also stopped publicly sharing their target list to make it more difficult for Russian organisations to know who the next target would be.

Overall, Ukraine's efforts and strategies to date in this hybrid war have demonstrated the power and potential of the 'crowd-sourced' methodology in the cybersecurity domain. It is indeed a reminder that effective distribution of resources and the proficient coordination of skills can create significant traction in the cyber space. Ukraine's strategies will indeed become a case study and a guideline in future cyberwarfare, but it will also inspire governments to develop a resilient cyber community ●

Ziv Mador is Vice President of Security Research at Trustwave SpiderLabs.

Hacktivists and volunteers are provided with guidelines, which are accessed and shared via an educational portal

Sentinel

A TSCM BREAKTHROUGH

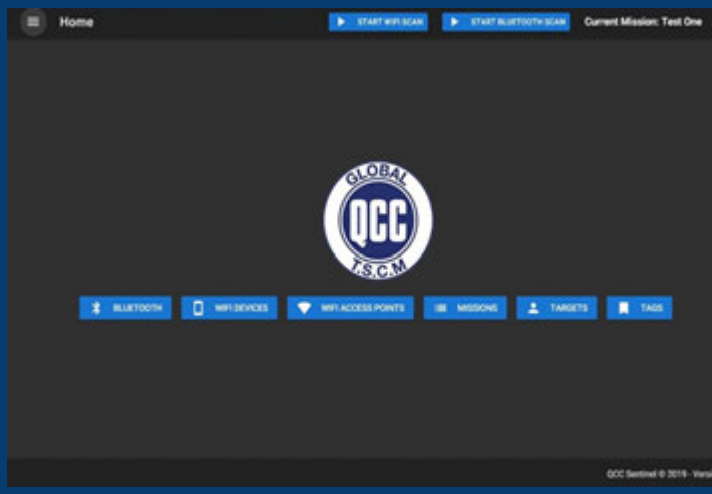
QCC Sentinel is the most advanced TSCM portable system for the detection & location of Wi-Fi 2.4GHz - 5GHz Devices & APs. Also with detection & location of all Bluetooth devices with full direction-finding. Software for TSCM & Tactical use.

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: Blok 'N' Mesh

UPDATING A CLASSIC

Tim Stewart *reveals how Blok 'N' Mesh went about improving its Defender fence system*

The frequently repeated cliché of: 'if it isn't broke, don't fix it!' is often rolled out as manufacturers strive to update products over time. The results can range from 'evolution' to 'revolution' and this was on our mind when we spoke to Blok 'N' Mesh's Head of Product Design, Tim Stewart about updating the company's popular V-mesh, Paladin-style fencing system, Defender.

Tim, you were instrumental in the development of the original Defender system, how did that come about?

"It was a system that was already being called for by customers. We had the industry-standard temporary fencing product, which uses mesh panels and rubber blocks – which you'll see on most construction sites. At the other end of the scale, we had developed a very high-security product called PolMil for the 2012 Olympics and that has since been approved for use at all manner of sensitive locations such as airports, government facilities and licensed nuclear sites.

"What was being asked for was something in between these two extremes. A competitively priced, on-ground system, which was more secure than standard temporary fencing but not as heavy duty as PolMil.

"The National Grid was in contact with us, looking for such a system as it was embarking on a major upgrade of substations around the country. In addition to wanting this intermediate system, it also specified all components, including the ballast, should be hand portable as many locations would not be accessible by a forklift."

And that was how the system was developed?

"Yes. The National Grid's engineers and security personnel twice visited our factory and test facility in Knowsley during development, which included physical 'mob' attack testing, before the design was

finalised. They selected 2.4 and 3m high Defender fencing with 200kg ballast every 2.5m giving optimum balance between portability and the level of security required."

But how could 200kg ballast be hand portable?
"We developed a stackable, 50kg, plastic coated ballast block called BraceBlok, which is a two-person lift. Four of these blocks stacked together provided the 200kg ballast required. We also have water-filled ballast options using tanks made from recycled plastic, which provide an environmentally friendly alternative to concrete and uses locally sourced water. Weighing only 20kg when empty, these are easy for a single person to carry and position."

Do clients install the system themselves?
"It's a three-way split. Some customers install themselves; some will have agreements with their preferred contractors who will install as part of a larger framework contract and some ask our own nationwide installation team to do so."

What was the industry's reaction to Defender?
"Pretty much all positive. Contractors for the National Grid were naturally the early adopters, and many are still using the same components they bought five years ago. Contractors working on high-profile civil engineering projects such as HS2 are drawn to the flexibility of the system combined with the extra stability and security that it provides against physical assault."

So, why update the system?
"Simply, customer feedback. Firstly, while hand portability is still an important consideration for some users, for others it isn't. For them, we have developed a more environmentally friendly, 275kg, cement-free ballast block, which saves 35tonnes of embodied carbon per 1,000 blocks. Because a single lift 275kg block needs to be correctly placed from the outset, provision for the use of a setting out space bar is incorporated into the new Base.

"Secondly, the Base units are now stackable – saving space on haulage and, when stacked, they can be fork-lifted off its transport and carried directly to the fence line. These Bases also accept our full range of ballast blocks from 40kg to 750kg. Next, the posts have additional slots which provide more flexibility when stepping the fence on sloping ground, and we have reduced the number and variety of fixings.

"In all, the changes enable a significantly quicker and simpler installation, reducing labour and associated costs, which results in further considerable savings when installing hundreds of metres."

So, it's very much evolution, not revolution?
"Exactly!" ●

With over 20 offices and depots in the UK, Ireland and mainland Europe, Blok 'N' Mesh is a market-leading manufacturer, supplier and installer of temporary fencing, site hoarding and barriers. Every year it manufactures more than 1.6-million units, leading the industry in both innovation and sustainability to suit a wide range of industries, from construction to security.

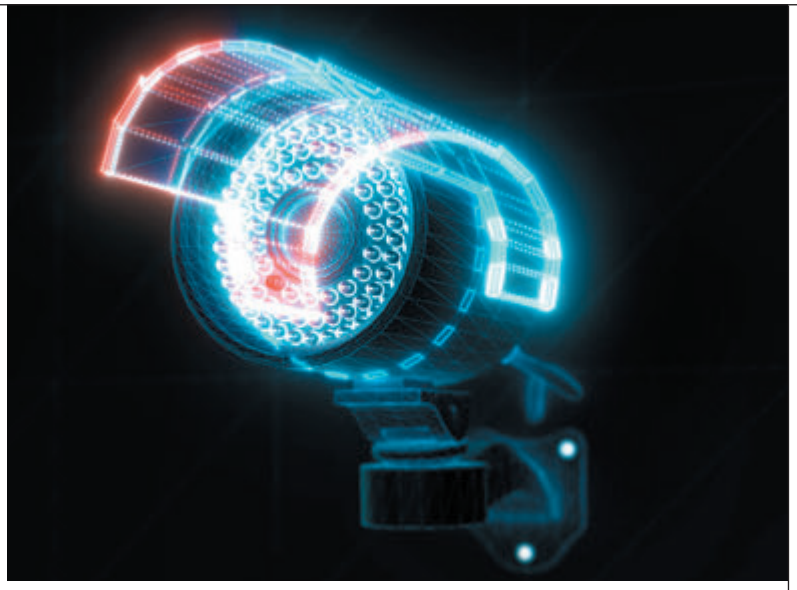
For further information go to www.bloknmesh.com

Above: Water-filled ballast options using tanks made from recycled plastic provide an environmentally friendly alternative to concrete

Right: The Base units on the Defender system are stackable – saving space on haulage

FROM AI TO ESG

Johan Paulsson *explores the six key technology trends that are set to impact the security sector in the coming year*



Technology is pervasive in every aspect of our personal and work lives. Every new technological development and every upgrade brings new benefits, makes the tools we rely on more effective and creates stronger, more efficient services. But as technology's integration into society deepens, awareness of its implications is becoming more heightened.

Ours is an industry making use of increasingly intelligent systems with technology inherently involved in collecting sensitive data. It is also as impacted by geopolitical issues affecting international trade as any other sector. Security innovations will create a smarter, safer world, but in 2023 we will need to evolve to keep pace with these trends – all while moving fast to exploit new technological opportunities.

"From analytics to action" will become a mantra for 2023. AI and machine learning may have aided the development of advanced analytics in recent years, but the focus moving forward will be on exploiting the actionable insights they deliver. The huge increase in data being generated by surveillance cameras and sensors is a key driver for this transition. It is impossible for human operators to interpret the nuances of large data sets and act quickly enough, but analytics and AI functionality can now recommend, prompt, and even start to automatically take real-time actions which support safety, security, and operational efficiency in every key vertical.

Analytics can support new methods of post-incident forensic analysis using, for example, assisted search to automatically find desired video among massive silos of camera data. New techniques will also be used to predict outcomes, using sensors to propose preventative maintenance actions to minimise potential industrial outages before failure occurs.

Advanced analytics can run directly within surveillance cameras on the edge of the network. After-the-fact analysis, though, is a job for on-site servers or the cloud. Building the ultimate data analysis solution demands a hybrid computing architecture – and one which meets a customer's requirements precisely.

There is no perfect off-the-shelf configuration. Each business must assess its specific use case and define the hybrid solution that meets its needs. This process is complicated by localised requirements around data privacy and retention, which can force the use of on-premises storage over the convenience of the cloud, but architecture refinements are an essential part of any 2023 technology strategy. Businesses must maintain the flexibility to create the hybrid architecture best suited to their specific needs – architecture which can change as demand and future trends dictate.

Security hardware can present an opportunity to do more. Cameras themselves are powerful sensors capturing both quality video information and, thanks to advanced analytics, metadata which makes them useful in new and novel ways. Camera metadata can be combined with input from other sensors – monitoring temperature, noise, air and water quality, vibration, weather and more – to create an advanced sensory network and enable data-driven decisions. While we're beginning to see this kind of multi-sensor monitoring appearing in industrial and data centre environments, the eventual use cases are limited only by our imaginations – and platform-agnostic data streams enable bespoke applications for any use.

In the video surveillance sector, ensuring the authenticity and privacy of every data stream as it moves from camera to cloud to server is essential to maintain trust in its value. Cybersecurity is as vital today as it has always been, but 2023 will see a more proactive approach by technology vendors in identifying vulnerabilities, with bug bounty programs becoming even more commonplace to incentivise external parties to take a white hat approach. Customers will also increasingly expect transparency regarding the cybersecurity of security solutions, with a Software Bill of Materials (SBOM) becoming standard in assessing software security and risk management.

The compliance goalposts move regularly, and often with great speed. Each new regulation ratified brings a different aspect of software or hardware into focus. The European Commission's proposed AI Act, for example, aims to assign specific risk categories to uses of AI, and will no doubt be the subject of much debate before it becomes law. But whether in relation to AI, demands surrounding cybersecurity, data privacy, the influence of 'big tech' or tech sovereignty, it's clear that technology companies in the security sector will increasingly need to adhere to more stringent regulations.

KEY TARGETS FOR 2023

This is not a year of great upheaval – it's one of realignment. Our sector's greatest opportunity continues to come from focusing on commercial success in tandem with our responsibility to address critical issues facing the planet and its population. By working together towards a common goal, the combination of human inventiveness, advances in technology, and ethical business practices can be combined to make the world a better place ●

Advanced analytics can run directly within surveillance cameras on the edge of the network

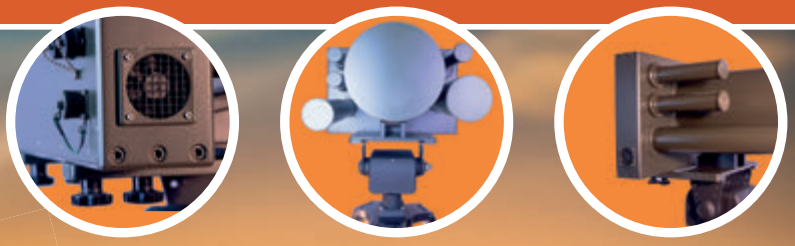
Johan Paulsson is Chief Technology Officer at Axis Communications

Picture credit: Adobe Stock

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

WE ARE ELECTRIC

Ben Chiswick *outlines the importance of combatting barriers to electrification*

The defence industry is impressively dynamic, prepared to swiftly react as needed but an understandable risk aversion leads to slow phasing in of new technologies and implementation of fundamental changes.

The electrification of vehicle fleets is an inevitable change that is already taking hold in various transportation sectors and is now a focal point of discussion both industry and government wide. Though its adoption is not simple, the benefits are clear cut. Understanding the best path forward for where, when and how to electrify fleets despite existing barriers is critical to success. Drive System Design (DSD) has a comprehensive understanding of this industry shift and can help defence industry players define a timeline and next steps according to the vehicle's mission profile, electrification technologies available and the operational challenges and benefits it brings.

One of the key drivers for the adoption of electrification is to improve the efficiency of vehicles and reduce the fleet's reliability on fossil fuels. In 2017 the US Army purchased $947-million worth of fuel, and costs have sharply increased since then. The fully burdened cost, which includes the initial purchase price and the cost of transporting it to where it is needed, is significantly higher.

While reducing fuel consumption saves money, it also can improve personnel safety. 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. Even small efficiency improvements would significantly reduce the number of fuel deliveries required and improve troop safety.

Electrified vehicles lead to huge fuel savings

Picture credit: Drive System Designs

On top of operational benefits, electrification also provides significant tactical opportunities. Every vehicle is now expected to do more – be more lethal or offer more protection – resulting in vehicles being equipped with additional surveillance and weapons systems, which require more power. An electrified vehicle would lead to huge fuel savings, since traditional internal combustion engine (ICE) powered vehicles spend a significant time idling to power these systems.

Powering auxiliary systems using an electrified powertrain will also provide opportunities to introduce next-generation weapons and surveillance systems that can use higher voltages. These can be fitted to traditional vehicles, but require support equipment, such as new DC/DC converters, which add weight and take up space. In vehicles with an electrified architecture, operating at higher voltage levels than current platforms, these systems can be integrated more easily.

There are inherent properties of an electric vehicle that offer significant benefits in theatre as well. For example, the EV propulsion systems are quiet and don't emit any exhaust gasses, aiding stealth efforts.

From a 'big picture' perspective, the sustainability value of adopting electrification should not be underestimated. This is why we continue to see environmentally friendly regulations enforced on a global scale.

While the benefits are extensive, there are still many issues at play combatting electrification. Perhaps the biggest barrier, and what will require the most change from an operational perspective, is the current fuel ecosystem. The vehicle infrastructure is set up around fossil-fuelled vehicles and would need to be completely rethought. There is not currently an infrastructure set up to charge a large fleet in remote operations, such as the desert, but getting JP8 to these areas is a well-established supply methodology. In the short term, the answer is to use the fuel that can be easily transported more intelligently using hybrid systems. This provides some of the benefits of electrification while mitigating the risk of step-change technology adoption.

Another common counterpoint to pure electrification is concern around redundancy and failure mechanisms. As ICE is the current accepted technology, the perception is that a traditional vehicle can limp home if it is damaged whereas an electric motor would leave the vehicle stranded. However, a parallel hybrid configuration that yields the benefits of a staged electrification introduction strategy can provide enhanced redundancy compared with conventional powertrains, if executed appropriately.

Another general perception is that there is no space for hybrid systems to be integrated in today's vehicles and making room would result in a compromise in the vehicle's survivability, lethality, mobility or size, weight, power and cost (SWAP-C). However, by taking a whole system approach to design, that can change. For example, when using a range extender engine, combining the power of an ICE and electric motor, peak performance including maximum torque and desired power can be achieved. As a result, a much smaller engine can be utilised, and this creates room to package the electric motor. Likewise, a hybrid vehicle will optimise the use of the energy onboard from both the fossil fuels and battery pack enabling the fuel tank to be reduced creating room for the electrified sub-systems. A good example is Cummins' development of an Advanced Combat Engine (ACE), a modular and scalable diesel engine solution that is capable of hybridisation, through a contract with the US Army.

Engineering consultancies like DSD are using this whole system approach, honed over years electrifying automotive, commercial vehicle and off-highway platforms, combined with specialist simulation tools to design electrified powertrains optimised for this scenario. We fully expect these perceptions will change as the technology becomes more widespread.

An often overlooked limitation to electrification is the thermal constraints of today's technologies. Thermally managing an electrified powertrain is not only important for performance, but critical to durability. The defence industry arguably presents the most challenging and diverse range of vehicle operating cycles and harsh environments that a powertrain engineer would need to design for. Whether it is required to climb the sand dunes in the Namibian desert or sit patiently waiting in the arctic, the range of temperatures the vehicle is subjected to is extreme. The necessity for armour, naturally representing a sealed or impenetrable layer around the vehicle, exacerbates these thermal challenges.

REDUCING FUEL CONSUMPTION SAVES MONEY AND IMPROVES PERSONNEL SAFETY

Commonly available power electronics modules that DC-DC converters and inverters are built upon are generally rated to around 90°C, limited by inherent material properties. Many defence applications would require this to be at least 25 percent higher, to allow incumbent cooling circuits supporting the ICE power-pack to cool electrified sub-systems as well. When this is most often not viable, the difficult reality of separate cooling systems must be faced, along with the additional complexity and potential failure mechanisms that accompany the new systems. Solving these thermal problems is a near-term necessity, with high power electrical distribution and conversion systems already critical in supporting the increasing demands for different voltages and power requirements for a multitude of communication, protection and weapon systems, before electrified propulsion systems can even be considered.

Thermal modelling and simulation early in vehicle architecture development is essential to understand and mitigate the failure modes. Once the weak links are identified, design decisions from high-level cooling architecture changes right down to chip placement to alleviate junction temperature issues, can be taken.

Considering the barriers, moving directly to a purely electric vehicle fleet from what is currently in operation today simply isn't feasible. It would require a quantum leap in vehicle operation, fuelling infrastructure and retraining vast numbers of personnel, posing too much of a risk. Instead, a stepping-stone approach will be taken to progressively integrate electrification into the combat fleet, and this is likely to be guided by vehicle weight classes.

The defence industry is already looking to other sectors to leverage well-understood and proven

technologies to take these first few bold steps. The automotive industry, whose adoption of electrification has been accelerated by legislation, is the current benchmark. This has naturally led to smaller vehicle platforms, such as the Humvee or the JLTV (Joint Light Tactical Vehicle), being good candidates for pure electrified architectures as they are wheeled and in a weight class that makes sense for hybrid architectures.

As vehicle weight classes increase, pure electrification becomes far from viable with current technology. The issue is battery power density; for example, to power a 70 tonne M1 Abrams tank the battery pack would weigh more than 12 tonnes and be around 350 cubic feet in volume – not so different to the overall package size of the existing Abrams powerpack. So pure electrification at this weight, and even at the 45-50 tonne IFV (Infantry Fighting Vehicle) class, is not yet practical, with a significant leap forward in battery technology needed to change this.

VEHICLE AUTONOMY AND ELECTRIFICATION COMPLEMENT EACH OTHER VERY WELL

This horizon line where electrification becomes viable for larger weight classes will be continually changing in years to come, as battery and motor technologies rapidly advance. The matrix of vehicle types, applications, mission profiles and electrification technologies is too vast to rely on manual calculation, so simulation is playing a critical role in accurately pinpointing where this line is and plotting its movement as time and technology progresses.

Autonomy is arguably an even bigger trend in the defence industry than electrification. Its benefits in terms of removing troops from harm's way are clear and armies are already rolling out this technology. The US Army is developing the Optionally Manned Fighting Vehicle (OMFV), enabling Manned Unmanned Teaming (MUMT) whereby a lead vehicle is crewed while the other vehicles follow autonomously. In the lighter weight classes, it is also using Robotic Combat Vehicles (RCV) to carry equipment alongside troops and perform advanced reconnaissance tasks.

Autonomy and electrification complement each other very well and the move to autonomy could help accelerate electrification. For instance, removing personnel from the vehicle significantly shifts the design paradigm that exists between a vehicle's survivability, lethality and mobility. With no personnel on board, the survivability and armour can be compromised, liberating significant volume and weight allowance that can be utilised for battery packs and electrified sub-systems. Additionally, when platforms such as an RCV-L are considered expendable, even greater headroom for battery packs is available, not to mention the simplified thermal management systems that can be introduced in the absence of armour.

Fully maximising the benefits of autonomy requires a completely new vehicle architecture. Seats, steering controls, windows or air vents and even doors are no longer needed and this provides an opportunity to improve the design of the vehicle. So it is the perfect time to also optimise these new architectures for electrification too.

Developing an effective electrified technology deployment strategy isn't easy, but it is becoming increasingly necessary. We will continue to see more advanced electrification and autonomous technologies and infrastructure come to fruition that will provide sustainable and reliable growth for the electrified ecosystem. The trade-offs between mobility, survivability and lethality will continue to be at the forefront of the transition, with autonomy allowing the current trade-offs to be challenged, especially considering the potential for reduced personnel exposure and additional power for new, critical weapons and communication systems. In the short-term, a staged, system-level approach to electrification minimises risk and maximises platform capability. Marching toward hybridisation is the best first step ●

Ben Chiswick is Drive System Design's Director, Engineering Business Development.

In 2017 the US Army purchased $947-million worth of fuel and costs have sharply increased since then

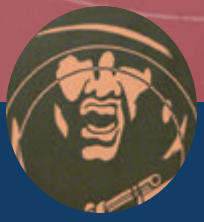
Picture credit: iStock

MCQUEEN TARGETS

LIVE FIREARMS TRAINING TARGETRY

AIM FOR THE BEST.

CIVILAIN TARGETS



MILITARY TARGETS

POLICE TARGETS

THREAT ASSESSMENT

3-D FOAM TARGETS

3-D FOAM ACCESSORIES

Hit the mark every time with

MCQUEEN TARGETS

GALASHIELS, SCOTLAND

targets.ukgal@sykes.com

+44 (0)1896 664269

mcqueentargets.com

INCIDENT BRIEF

Europe

29 December, Heathrow – UK
Border Force officers found traces of uranium on a shipment of scrap metal, which arrived on a flight from Oman.

11 January – UK
Royal Mail was forced to request that customers stop sending parcels and letters to overseas destinations after a cyber incident caused: "severe service disruption" to international exports. No one has yet claimed responsibility.

11 January, Paris – France
Six people were injured by a man wielding a knife during rush-hour at the Gare du Nord station. Police arrested the man after they opened fire and wounded him.

14 January, Goodison Park – UK
Everton football club's board of directors were forced to miss the Premier League game against Southampton after being warned of: "a real and credible threat to their safety and security" related to protests by fans.

16 January, Cheshire – UK
A man was arrested on suspicion of a terror offence in relation to the uranium found at Heathrow on suspicion of an offence under section 9 of the Terrorism Act 2006, which covers the making and possession of radioactive devices.

20 January, Leeds – UK
Police ordered a partial evacuation of the Gledhow wing at St James's hospital after a 27-year-old man was arrested on suspicion of a terror offence after being seen with a suspected firearm and a suspicious package.

Americas

6 January, Virginia – USA
A six-year-old pupil deliberately shot their teacher during a lesson. The child was taken into custody and the teacher is in a stable condition. The motive as yet remains unknown.

8 January, Brasília – Brazil
Thousands of far-right extremists and supporters of the ex-president Jair Bolsonaro stormed congress in a failed attempt to overthrow the new week-old government in a breach that was reminiscent of the 6 January invasion of the US Capitol by followers of Donald Trump in 2021.

15 January, Lima – Peru
The government declared a 30-day state of emergency in the capital and three other regions following weeks of protests against President Dina Boluarte that have so far claimed at least 42 lives.

19 January, Lima – Peru
A march demanding the resignation of President Dina Boluarte escalated into running battles between protesters and riot police amid stone-throwing and teargas.

21 January, Los Angeles – USA
Ten people were killed and 10 others hospitalised after a gunman opened fire in a ballroom dance studio during a lunar new year festival. The 72-year-old suspect then shot himself.

24 January, Half Moon Bay – USA
Two fatal shootings took place at a mushroom farm and a trucking firm on the outskirts of this coastal community about 30 miles south of San Francisco. Seven people were killed and the attacker arrested.

Asia

6 December, Nanjing – China
Students at Nanjing Technical University in protested days after people took to the streets in Beijing and Shanghai demanding an end to continuing Covid lockdowns .

9 December, Jamshoro – Pakistan
Improvised explosive devices planted at the foundations of power pylons partially damaged two pylons. The Sindhudesh Revolutionary Army claimed responsibility.

14 December, al-Aqbieh – Lebanon
An Irish peacekeeper was killed and another seriously wounded in a gun attack after a hostile crowd surrounded Irish members of the UN peacekeeping force in the south of the country.

26 December – South Korea
South Korea scrambled warplanes and attack helicopters and fired warning shots after North Korean drones violated its airspace, according to the South Korean military.

27 December – Andaman Sea
About 180 Rohingya refugees are feared to have died after their boat went missing in the Andaman Sea after trying to flee refugee camps in Bangladesh, bound for Malaysia.

11 January, Kabul – Afghanistan
An explosion near the Foreign Ministry in the capital killed five people and wounded several others. The Islamic State in Khorasan Province group is suspected.

23 January, Bolan – Pakistan
A passenger train was derailed by a bomb blast, leaving at least 15 passengers injured. The separatist Baluchistan Liberation Army claimed responsibility for the attack.

23 January, Bannu – Pakistan
A Pakistani soldier died while trying to defuse an IED in a joint operation in the Khyber tribal district.

23 January, Papua – Indonesia
A veteran reporter known for covering rights abuses in Indonesia's militarised region claimed that a bomb exploded outside his residence. No one was hurt.

Africa

8 December, Boala – Burkino Faso
At least 10 people, most of them civilian volunteers supporting the armed forces, were killed in an attack by suspected jihadists.

8 January – South Africa
Police are investigating a plot to poison Eskom ceo André de Ruyter after he drank a coffee suspected to be laced with cyanide. Eskom is one of the main South African power utilities and has been subject to claims of corruption that has led to record levels of power cuts in the country.

12 and 13 January, Arbinda – Burkina Faso
As many as 66 women and children were seized by armed men while they scoured the bush for fruit and leaves outside two villages in the Sahel region's Soum province.

17 January, Yaoundé – Cameroon
Prominent journalist Martinez Zogo, the director of the private radio station Amplitude FM, was kidnapped by unknown assailants after trying to enter a police station to escape his attackers.

20 January, Arbinda – Burkina Faso
The 66 women and children kidnapped by armed assailants in the north of the country on 12 and 13 January were freed after security forces staged a rescue operation. Jihadists are suspected of being responsible.

22 January, Mogadishu – Somalia
Five civilians were killed when al-Shabaab fighter laid siege on the mayor's office and other local government facilities. Six gunmen were killed by the army.

22 January, Galcad – Somalia
Roughly 30 Islamist al Shabaab militants were killed in a US military hit in the centre of Somalia, where the country's military was engaged in fierce combat, according to a statement from the US Africa Command.

23 January, Yaoundé – Cameroon
The mutilated body of journalist Martinez Zogo was found near the capital after he was abducted. Zogo had been talking on air about a case of alleged embezzlement involving a media outlet with government connections.

NEWS

Europe

Abloy UK announces Digital Access Solutions Academy dates

Abloy UK has released new 2023 dates for courses at its Digital Access Solutions Academy, with training available for solutions such as Incedo, SMARTair, Aperio and the ePED Escape Door System. Launched in 2022, the Digital Access Solutions Academy is a purpose-built facility to showcase, work with, install and test Abloy's extensive range of products, with particular focus on new digital solutions and ecosystems. Pip Courcoux, Head of Product, Technical and Digital Transformation at Abloy UK, said: "The way we move and use today's smarter buildings is becoming more fluid, and different people require different access times and entry points. With change comes the need for more agile security systems that keep us safe, while keeping us moving. With this in mind, we recognised a need to create a new area of our Academy for our growing customer base, to focus specifically on our expanding range of digital access solutions. Since its launch last year, the Digital Access Solutions Academy has been incredibly popular, and we anticipate a similar response to this year's courses – so don't delay in booking your free place."

G4S to create new security jobs at Sizewell C nuclear plant

G4S Secure Solutions UK will create almost 100 jobs for those living near Suffolk, close to the Sizewell C nuclear plant. EDF has awarded a £4.3-million interim security contract to G4S and so far, over 50 local residents have applied for positions or are in the process of onboarding. Contract Manager, James Self, explained: "There's going to be plenty of opportunities for those looking to change careers or get on the employment ladder, and they'll be supported by an experienced and friendly team throughout their time with us. The roles we are recruiting for are more than a Security Guard. You'll ensure the safety of our customers, contractors and their staff, their buildings and assets, whilst delivering excellent customer service in a safe and secure environment." The contract for Sizewell C is expected to continue through 2023 and available roles will comprise of vetting employees; managing access to the site in the Access Control team, monitoring surveillance systems, the perimeter of the site and being involved in incident management reporting. G4S is also implementing the Sizewell C Induction Team. Almost 80 percent of these new roles will be filled by workers who do not hold a Security Industry Authority licence, meaning that they will gain a new qualification working for G4S funded by G4S.

Ministers studying plans for UK child-specific terrorism orders

The official adviser on terrorism law has told the UK government that new legal terrorism orders specifically for children should be brought in to tackle the growing numbers being arrested. Ministers are studying plans that would result in children accepting help or facing jail, devised by Jonathan Hall KC, the independent reviewer of terrorism legislation. The move comes as the number of children arrested has increased, mainly for lower-level offences, such as sharing propaganda or downloading material. The rise has been fuelled by growing internet use and an increase in terrorist propaganda available online, with children as young as 13 being arrested. There is a growing belief among counter-terrorism officials that a section of those arrested, while clearly breaking terrorism laws, pose little threat of staging an attack. The proposed new orders would carry legal force and, under them, children aged 17 or under who have been arrested for lower-level terrorism offences can either risk prosecution, imprisonment and a criminal record or accept stringent measures, Hall said.

CybExer Technologies to provide cyber tech to Ukraine

Estonian cybersecurity company CybExer Technologies has announced that its cyber range technology will provide the underlying technology for the cyber lab of the Ukrainian Armed Forces as part of the European Union's support to Ukraine through the European Peace Facility (EPF). The cyber lab has been set up in the framework of the EU's support to Ukraine through the EPF cyber defence component, led by the Estonian e-Governance Academy. The EPF assistance project to support Ukrainian Armed Forces' cyber units started in 2021 to expand the EU's capability to provide security, including military equipment and infrastructure to Ukraine. Aare Reintam, COO of CybExer Technologies, explained: "Investing in training and education is probably the best kind of investment one can make for incident prevention and response. It is great to be able to develop a more comprehensive approach to advanced exercises and training using new cyber defence technologies and scenarios."

Denmark to scrap bank holiday to increase defence spending

Denmark's new left-right coalition government has announced that one of its earliest policy proposals is to scrap a bank holiday in order to divert more money towards defence spending. The government has proposed to remove from the calendar one of Denmark's 11 national holidays – Store Bededag, or Great Prayer Day – claiming that scrapping the holiday will increase economic activity and productivity, helping it to achieve a coalition pledge to reach Nato's target of 2 percent of GDP on defence spending three years ahead of schedule. The move has been criticised by the far left and right, as well as by church and business communities. The New Right party threatened to trigger a referendum, saying the holiday was "associated with important traditions".

NEWS

Americas

Delinea report reveals significant decrease in cyber attacks

US provider of Privileged Access Management (PAM) solutions for seamless security, Delinea, has published its 2022 State of Ransomware Report, which finds that things may be looking up in the fight against ransomware. A survey of 300 US-based IT decision makers, conducted on Delinea's behalf by Censuswide, found that only 25 percent of organisations were victims of ransomware attacks over the past 12 months, a 61 percent decline from the previous year when 64 percent of organisations reported being victims. Furthermore, the number of victimised companies that paid the ransom declined from 82 percent to 68 percent, which could be a sign that warnings and recommendations from the FBI to not pay ransoms are being heeded. Larger companies are much more likely to be victims of ransomware, as 56 percent of companies with 100 or more employees said they were victims of ransomware attacks. Along with these positive results, the survey also raised concerns that a potentially reduced threat could lead to complacency. Budget allocations for ransomware are in decline, as only 68 percent of those surveyed said they are currently allocated budget to protect against ransomware versus 93 percent during the prior year. The number of companies with Incident Response Plans also declined from 94 percent to 71 percent, and only half are taking proactive, proven steps to prevent ransomware attacks such as enforcing password best practices (51 percent) and using Multi-Factor Authentication (50 percent).

US supreme court lets WhatsApp pursue Pegasus lawsuit

The US supreme court has let Meta Platforms Inc's WhatsApp pursue a lawsuit accusing Israel's NSO Group of exploiting a bug in its WhatsApp messaging app to install spy software allowing the surveillance of 1,400 people, including journalists, human rights activists and dissidents. The justices turned away NSO's appeal over a lower court's decision that the lawsuit could move forward. NSO has argued that it is immune to being sued because it was acting as an agent for unidentified foreign governments when it installed the Pegasus spyware. Joe Biden's administration had urged the justices to reject NSO's appeal, noting that the US state department had never before recognised a private entity acting as an agent of a foreign state as being entitled to immunity. Meta, the parent company of both WhatsApp and Facebook, in a statement, welcomed the court's move to turn away NSO's "baseless" appeal, noting: "We firmly believe that their operations violate US law and they must be held to account for their unlawful operations".

TSA intercepted record number of guns at airports in 2022

The US Transportation Security Administration has revealed that in 2022 it intercepted a record number of guns at airport safety checkpoints, and an overwhelming majority of them were loaded. In a statement the TSA revealed that as of 16 December its officers had intercepted 6,301 firearms. Out of those, 88 percent were loaded. The number marks an increase of more than 300 from the 5,972 firearms that were detected in 2021. Since 2010, the number of firearms intercepted by the TSA has steadily increased, with the exception of 2020, because of the coronavirus pandemic.

Hackers stole data from multiple US electric utilities

According to a memo obtained by CNN, hackers stole data belonging to multiple electric utilities in an October ransomware attack on a US government contractor that handles critical infrastructure projects across the country. It's understood that Federal officials have closely monitored the incident for any potential broader impact on the US power sector while private investigators have combed the Dark Web for the stolen data, according to the memo sent this month to power company executives by the North American grid regulator's cyberthreat sharing centre. It's believed that the ransomware attack hit Chicago-based Sargent & Lundy, an engineering firm that has designed more than 900 power stations and thousands of miles of power systems and that holds sensitive data on those projects. The firm also handles nuclear security issues, working with the departments of Defense, Energy and other agencies "to strengthen nuclear deterrence" and keep weapons of mass destruction out of terrorists' hands, according to its website.

Hackers leak email addresses of 200-million Twitter users

Hackers stole the email addresses of more than 200-million Twitter users and posted them on an online hacking forum, a security researcher has revealed. The breach "will unfortunately lead to a lot of hacking, targeted phishing and doxxing", Alon Gal, co-founder of Israeli cybersecurity monitoring firm Hudson Rock, wrote on LinkedIn. He called it "one of the most significant leaks I've seen". Twitter has not commented on the report, which Gal first posted about on social media on 24 December, nor responded to inquiries about the breach since that date. It was not clear what action, if any, Twitter has taken to investigate or remediate the issue. Troy Hunt, creator of the breach notification site Have I Been Pwned, viewed the leaked data and said on Twitter that it seemed "pretty much what it's been described as". There were no clues to the identity or location of the hacker or hackers behind the breach. It may have taken place as early as 2021, which was before Elon Musk took over ownership of the company last year.

NEWS

Asia

Elbit Systems to Supply UAS to the Australian army

Elbit Systems of Australia has been selected to provide the Australian Army with the Skylark I LEX Unmanned Aerial Systems (UAS) equipped with electro optical and automatic dependent surveillance – broadcast (ADS-B) system. With its certified ADS-B system, Elbit Systems of Australia plans to support the Australian Army achieve wider use cases outside of traditional Army UAS employment including integration into more classes of airspace. This will enable Australian Defence Force support to civilian operations for disaster and humanitarian relief. Designed for in-theatre operation by manoeuvring forces, the fully autonomous electric propelled Skylark I-LEX features mission-oriented, intuitive man-machine interface (MMI) and a 40km line of sight communication range, which makes it effective for a variety of missions including reconnaissance and force protection missions. UAS of the Skylark family, including the 18-hours endurance Sklylark 3 Hybrid, have been selected to date by dozens of customers among Israel, Asia, Europe and Latin America.

SecurityHQ expands its operations in the Middle East

Global managed security services provider SecurityHQ has increased its presence in the Middle East with an expansion of its global security operation centre amidst significant growth. SecurityHQ has expanded its offices and operations, situated in Dubai Digital Park. This expansion is one of the company's six global security operation centres located around the globe. With the growth of the team, and the demand of Middle East-based customers in a variety of sectors, including telecommunications, oil and gas, and financial services, it was a natural decision to expand according to Aaron Hambleton, Director Middle East & Africa: "The adversaries that our customers are up against, be it nation state, organised crime groups and everyone in between, are finding ways to diversify and evolve their techniques to either avoid detection or inflict more damage. In response, we have invested heavily in additional technology and talent, with supplementary cyber security capabilities, analysts, offensive security specialists, incident response experts, and upgraded platforms, to ensure that we deliver for our customers based in the Middle East."

Jumeirah Marsa Al Arab resort selects Maxxess eFusion

The newest 'statement resort in Dubai – Jumeirah Marsa Al Arab – from the Jumeirah Group, has announced its intention to use Maxxess eFusion technology to provide feature-rich, enterprise-class access control and enable seamless integration of third-party security, safety and a back and front-of-house systems. The luxury five-star development, opening this year, will include 408 rooms, four super penthouses, a premium yacht club and marina with 128 berths, nine high-end villas and an extensive resort landscaped with infinity pools and beachfront at the heart of Dubai's largest private beach. The surveillance system, comprising over 700 Hanwha Techwin cameras, ensures guest and staff safety, provides a full audit trail of room access and allows services such as room cleaning to be delivered with no disruption to guests.

Australia plans to develop new cyber security strategy

Australia has outlined plans to develop a new cyber security strategy to strengthen the country's critical infrastructure, among other goals, following a spate of high-profile cyber attacks against Australian companies. Speaking at the National Press Club, minister for home affairs and minister for cyber security Clare O'Neil said the strategy will be led by Cyber Security Cooperative Research Centre CEO Rachael Falk, former Telstra CEO Andy Penn and former Chief of Air Force Mel Hupfeld. There will also be an expert panel drawn from around the world, led by former UK National Cyber Security Centre CEO and Oxford University professor Ciaran Martin. According to O'Neil, Australia has been in a "cyber slumber", as evidenced by former prime minister Scott Morrison's decision to abolish the cyber security ministry when he came to office. "With the government's new strategy, we hope Australia can work toward adopting a clear, unified approach to anticipating and overcoming future cyber security challenges," O'Neil concluded.

Ministry denies presence of terrorist groups in Afghanistan

During a press conference held in Kabul, Afghanistan Interior Ministry's spokesperson, Abdul Nafi Takoor, claimed that there is no group in the country that can pose a threat to other countries. "I should tell you about the cultivation of narcotics, that you will not find a single acre of land where poppy is cultivated in the entire geography of Afghanistan," Takoor claimed, before continuing: "Unfortunately, Afghanistan is still leading the world in the cultivation and processing of drugs, and the rise in drug addicts is very serious." According to the Afghanistan ministry's spokesperson, security in the country is better now than in the past, underling that no one will be permitted to cultivate poppies and there is no drug production anywhere in Afghanistan. "Afghanistan's current security situation, which is now ensured, was not like this in the past forty, fifty, or sixty years," Takoor said. The ministry's spokesperson additionally claims that over 1,200 complaints of criminal activity have been received over the course of the previous two months and more than 800 of them have been addressed.

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

NEWS

Africa

3DX-Ray supplies portable X-ray systems to Africa

With its local partner, 3DX-Ray has announced the successful sale of two units of ThreatScan-AS1(ISC) Portable X-Ray system in Africa. The customer is an important unnamed African Explosive Ordnance Disposal Unit, and the system has been supplied for use in counter EOD operations. 3DX-Ray Ltd CEO, Vincent Deery, said: "We are especially pleased about this sale because it is an important landmark in our sales strategy. Whilst we have been supplying our systems to EOD agencies all over the world for many years, this is the first sale of our recently released highest performing fully integrated system into the African market, which is a fast growing and increasingly important market to 3DX-Ray." The ThreatScan-AS1(ISC) is a robust amorphous silicon portable x-ray inspection system that comprises a detector panel with an imaging area of 430 x 347mm, a new high penetration 150kV generator and a laptop along with batteries, chargers, the user-friendly 3DX-RAY ThreatSpect software, wireless communication and transport case. The AS1(ISC) is simple to use and produces extremely high-quality, sub-millimetre resolution images in real time.

Kenya: Meta sued for $1.6-billion for fuelling Ethiopia violence

Amnesty International claims that Meta must reform its business practices to ensure Facebook's algorithms do not amplify hatred and fuel ethnic conflict, following a landmark legal action against the social media company submitted in Kenya's High Court. The legal action claims that Meta promoted speech that led to ethnic violence and killings in Ethiopia by utilising an algorithm to prioritise and recommend hateful and violent content on Facebook. The petitioners seek to stop Facebook's algorithms from recommending such content to Facebook users and compel Meta to create a 200-billion ($1.6 billion USD) victims' fund. Amnesty International has joined six other human rights and legal organisations as interested parties in the case."The spread of dangerous content on Facebook lies at the heart of Meta's pursuit of profit, as its systems are designed to keep people engaged. This legal action is a significant step in holding Meta to account for its harmful business model," said Flavia Mwangovya, Amnesty International's Deputy Regional Director of East Africa, Horn and Great Lakes Region. One of Amnesty's staff members in the region was targeted as a result of posts on the social media platform.

Major Oil Pipeline Project in Africa Entrusted to Senstar

Provider of sensing and information management solutions for the protection of critical infrastructure, Senstar has announced it has been awarded a major oil pipeline project in Africa. The project will reinforce the security of a major pipeline. "Senstar will provide a comprehensive perimeter intrusion detection system with the aim of equipping multiple sites with innovative fibre optic technologies. Together with local partners, we will work on a multi-layered solution that maximises safety and security," said Managing Director of Senstar, Fabien Haubert. "We will also be providing a range of support services to ensure a smooth, ongoing operation." With innovative perimeter intrusion detection systems (including fence sensors, buried sensors and above ground sensors), intelligent video management, video analytics, and access control, Senstar has been safeguarding people, places and property for organisations around the world, with a special focus in utilities, logistics, corrections and energy markets for over 40 years.

PDP abandoned North-East to Boko Haram – APC

The All Progressive Congress (APC) has berated the People's Democratic Party (PDP) over its failure to contain Boko Haram insurgents in the North-East geo-political zone while in power. Speaking at the campaign rally of Bola Ahmed Tinubu, the presidential candidate of the party, the Senior Adviser on strategic planning, Ahmed Lawan, alleged the PDP abandoned vulnerable Nigerians to the mercy of Boko Haram. The Senate President commended President Muhammadu Buhari for technically eradicating insurgency in the sub-region, noting: "Mr. President our father, mentor, the PDP abandoned in the North East to Boko Haram. In 2015 when you were sworn in, you liberated us."

Security Council's lack of African voices is "historical injustice"

The lack of permanent representation for African nations on the UN Security Council is a: "historical injustice" that must be rectified, Mozambique's ambassador to the UN has said. In an interview with The National, Pedro Comissario noted that the world's most powerful international organ is western-centric and called for an overhaul. "[The] Security Council was an institution that was created more than 70 years ago, and it answered the concerns of peace and security, mostly of Europe. But this is no longer the case," he said, speaking as the US ambassador to the UN embarked on a trip to Africa. Africa, the world's second-largest continent after Asia, is "underrepresented", he said, while two of the Security Council's five permanent seats go to European nations – France and Britain. A third goes to Russia, and the remaining two are occupied by the US and China. It is "high time" to address this and Africa should have at least two permanent seats on the Council, something that is especially vital considering African issues account for more than 60 percent of the council's agenda, Mr Comissario said, noting that African states have long called for an overhaul of the Security Council.

DIARY DATES

2023 Conference and Exhibition planner

20-24 February IDEX 2023
Abu Dhabi National Exhibition Centre - ADNEC, Abu Dhabi
Organiser: ADNEC Group
Tel: +971 (0) 2 406 3466
Email: registration@idexuae.ae
idexuae.ae

28 February -1 March Cyber Intelligence Europe 2023
Bern, Switzerland
Organiser: Intelligence-Sec Limited
Tel: +44 (0) 158 234 6706
Email: events@intelligence-sec.com
intelligence-sec.com

15-17 March DSEI Japan 2023
Makuhari Messe Tokyo, Japan
Organiser: Clarion Events
Tel: +44 (0) 207 384 8246
Email: japan@dsei-japan.com
www.intelligence-sec.com

28-31 March ISC West 2023
Las Vegas, Nevada
Organiser: Reed Expos
Tel: +1 203 840 5602
Email: inquiry@isc.reedexpo.com
www.iscwest.com

28-31 March Enforce Tac 2023
Nuremberg, Germany
Organiser: Messe Frankfurt
Tel: +49 9 11 86 06-80 22
Email: enforcetac@nuernbergmesse.de
www.enforcetac.com/en

25-27 April The Security Event 2023
NEC, Birmingham
Organiser: Nineteen Group
Tel: +44 (0)20 8947 9177
Email: info@thesecurityevent.co.uk
www.thesecurityevent.co.uk

3-5 May IMDEX Asia 2023
Changi Exhibition Centre Singapore
Organiser: Experia
Tel: +65 6542 8660
Email: enquiries2023@imdexasia.com
www.imdexasia.com

16-18 May IFSEC 2023
ExCeL London
Organiser: Informa PLC.
Tel: +44 (0) 20 8052 0660
www.ifsecglobal.com

14-17 November Milipol Paris 2023
Paris, France
Organiser: Comexposium
Email: visit@milipol.com
https://en.milipol.com/

THE SECURITY EVENT

25-27 APRIL 2023

NEC BIRMINGHAM UK

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

FIND OUT MORE: WWW.THESECURITYEVENT.CO.UK

Co-located with:

THE HEALTH & SAFETY EVENT

THE FIRE SAFETY EVENT

THE WORKPLACE EVENT

NATIONAL CYBER SECURITY SHOW

Lead Media Partner:

Security Matters

Founding Partners:

ANIXTER

ASSA ABLOY

COMELIT GROUP

Honeywell

TDSi

Texecom

tyco

Videcon

YOUR MOBILITY SPECIALIST FOR ARMOURED VEHICLES

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

TSS International official distributor for:

RODGARD · HUTCHINSON · TSS HEAVY DUTY WHEELS · SEMA WORLD ANTI-TERRORISM SAFETY FEATURES · Téléflow · MOVIT · ProtecTank TSS · B&G electronics · SKYDEX

TSS

TSS INTERNATIONAL BV ZUIDEINDE 30-34, 2991LK BARENDRECHT. THE NETHERLANDS.
PHONE: +31 (0)180-618 922 FAX: +31 (0)180-611 326 EMAIL: SALES@TSSH.COM **WWW.TSSH.COM**

SHOWCASE

Hanwha Techwin Europe unveils AI fisheye camera

Video surveillance specialist Hanwha Techwin has launched the XNF-9013RV, an AI fisheye camera with AI-based object detection and classification, improved image quality features and IK10 vandal resistance. Accurate object detection and classification enables operators to quickly identify people, faces, number plates and vehicle types including cars, trucks, buses and bicycles. This offers more situational awareness and context to an event. Irrelevant motions such as waving trees, moving shadows and animals are ignored, all of which would usually be the cause of false alarms with standard motion-detection technology. The XNF-9013RV comes with WiseStream III, the latest in Hanwha Techwin's AI compression technology. WiseStream III applies a low compression rate to objects and people detected and tracked by AI to maintain the quality of the image, while applying a high compression rate to the rest of the scene This saves on network, storage, energy and power, while improving network bandwidth by up to half in active scenes and 95 percent in idle scenes. This is complemented by extreme WDR that uses Local Contrast Enhancement and Scene Analysis technology to capture ultra-clear images even in environments with strong backlight conditions.

Videx enhances concierge its door entry system

Videx has enhanced its leading door entry system, the VX2300, adding a desk mount concierge unit for small-to-medium-sized installations of the two-wire video system. The CST2310 unit can be used for up to 200 apartments, offering both handset and hands-free speech and a back lit touch control keypad along with a 3.5in LCD display with onscreen information relating to both entrances and apartments, and the stage of a call when in progress. It can also be used to receive or intercept calls from entrances, make and receive calls from apartments and activate outputs, open doors and gates and receive alarm calls from apartments. The CST2310 has three modes of operation. Day mode where all calls from apartments and entrances are intercepted by the concierge. Night mode where calls from entrances can go direct to the apartments unless directed to the concierge and calls from apartments can be received by the concierge. It also has an off mode where calls go directly from entrances to the concierge while the concierge is off duty.

ASSA ABLOY BIM mobile app

ASSA ABLOY Opening Solutions UK & Ireland has launched its new Openings Studio Mobile App, which allows users to manage buildings as a holistic system. Information stored within the app enables buildings to be safely and effectively designed, constructed and operated. Openings Studio is a cloud-based, custom-configuration tool for the creation, visualisation, modification and management of door openings. The BIM application provides access to complete doorset information at all stages from product concept to product care. The installation process and on-site information is also captured, and products are asset tagged (with either a QR code or RFID tag) for ease of access to details and history, allowing comprehensive door-by-door fire and performance inspections to be completed and recorded. The Openings Studio Mobile App is the latest evolution of this software solution, providing a genuine seamless link between design intent during the specification process through to product in service. Users can easily access the information relating to each door via the app, and enable a full and detailed inspection to be carried out.

Burg-Wächter unveils new Sapphire padlock range

Burg-Wächter has launched the Sapphire 111/121 CS padlocks. Sturdy, weather resistant and providing unrelenting strength, they are designed and manufactured to offer convenience and good levels of attack resistance. A durable ABS outer jacket prevents scratches and gives extra protection from the elements as it houses a strong, laminated steel body, while a chrome-plated, hardened steel shackle offers extra protection – giving enhanced security against bolt cutters. The shackle comes double-bolted from the 40mm models upwards, while the 121 C models feature a concealed shackle for additional protection. A brass cylinder also adds resistance against corrosion – making it ideal for outdoor use – while a hardened hinge pin and staple provides unrelenting strength. The 40mm padlock has the option of a long shackle and can come keyed alike, making it handy for properties where multiple users need access to the lock.

Regulus Cyber fully operational counter-UAS system

Regulus Cyber is launching the first fully operational, small-form-factor counter-UAS system using unique GNSS manipulation technology to defeat all UAS threats, including swarms, multi-direction attacks, dark drones, manually piloted drones and 4G/5G drones. The Ring system uses proprietary, combat-proven GNSS manipulation to take control of the drone and deflect, hold or crash it, or force it to land. While jamming requires several RF channels to be jammed to be successful, and can therefore inadvertently affect various other systems in the surrounding area, the GPS-disruption approach can be used to target and neutralise a single threat or unlimited threats simultaneously, using very low-power transmission on a single channel – assuring low collateral damage only on the GNSS channel. The detection capabilities of the field-proven Ring R1 add-on include a detection range of up to 1.5km and fast scanning of the RF spectrum, with minimum dead spots, for coverage that is more scalable and effective. It has a minimal false-alarm rate and provides accurate classification of threat types – for example DJI or Parrot – with threat alerts based on profile matches. The Ring R1 is suitable for operation in multi-threat environments, and non-line of sight, bad weather and low visibility conditions.

GUARD RAIL

Described as a game-changer for the security industry, our IWA-14-rated HVM pedestrian guardrails offer full roadside protection and can withstand a deliberate or accidental impact, unlike regular pedestrian guardrails, which are not designed to protect and so crumple when hit. Perfect for preventing death and injuries outside schools, local government buildings and other locations

- Crash-tested and capable of withstanding the impact with a 2.5 tonne vehicle travelling at 40mph - without significant bending or buckling
- Available as the standard HVM Guardrail, HVM Socketed Guardrail and even our HVM Guardrail Ultra systems
- Uses Securiscape's Smartpost technology in conjunction with fence panels for a flexible security solution
- Manufactured in the heart of the UK from high quality materials and can even be used on road bridges

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

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

securiSCAPE®
protecting people in public places®

FOLLOW US ON:


14-17
NOV. 2023
PARIS NORD VILLEPINTE
MILIPOL
PARIS
Milipol
PARIS
Leading Event for Homeland
Security and Safety
COMEXPOSIUM
www.milipol.com
#Milipol