www.intersec.co.uk

intersec

The Journal of International Security

April 2023

INFORMATION WARFARE

Social and individual resilience, ontological security and counter intelligence

RED ALERT!

The UK public warning system swings into action

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

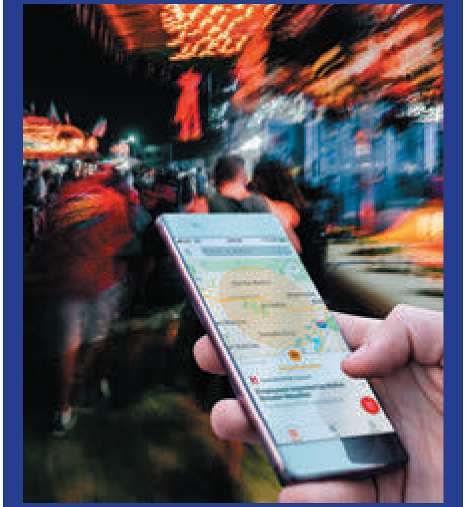
UK +44 1226 712500
Blok 'N' Mesh Global Ltd, 10 Christleton Court, Runcorn, WA7 1ST

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 04
April 2023



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

On 7 July 2005, I – like many Londoners – was starting my early morning commute across the city unaware of the chaos that was unfolding elsewhere. From memory, the first indication I had that something out of the ordinary was going on was the huge crowds of people outside of the tube stations who were forced to have to take the bus as the underground service had been shut down. I remember attempting to call my work to let them know that I was going to be late and was surprised to find that I couldn't get a signal. At the time I was working as a tech journalist and figured that the lack of signal was due to the network being overloaded with everyone trying to do exactly the same as I was, and thought nothing of it. With hindsight, I now realise that the mobile network had been temporarily suspended for everyone but the emergency services so that they could communicate and deal with the unfurling emergency with the minimum of interference.

I remember waiting for a bus for over an hour and even when they did come they were completely full and simply drove past our stop. Exasperated and ignorant to what was causing the delay, word started to spread among my fellow commuters about what was the cause. Someone had heard that a suicide bomber had detonated their device on a bus killing everyone on board, others talked of similar events occurring on trains, one person claimed to have heard that a man with a knife had gone crazy on the platform of a tube station while waiting for a train. Rumours swirled and gathered momentum in a game of Chinese whispers that was sweeping across the entire capital.

In the end, I gave up waiting and decided to walk to my office. Along the way I met other commuters who had heard fragments of what had been the cause of the morning's disruption and by the time I eventually arrived at work some two hours later had managed to piece together a pretty accurate picture of what I had been led to believe had taken place. Of course, it was miles away from the truth and the tragic events that really took place that day.

Looking back on that day I often wonder what could have been done to make the situation better for everyone involved. Data varies, but figures seem to suggest that around 80 percent of UK citizens had mobile phones back then, compared with around 90 percent now. In 2007, a national alert system based on the mobile phone network might not have reached everyone, but you can bet that some of the wilder rumours I heard that day would have been quickly dispelled. In 2023, when it seems that everyone has a phone or is at least in the vicinity of someone else who has one, the mobile network seems like the obvious place to use such a system and sure enough on 23 April the first nation-wide test was carried out. Ironically, I was one of the seven percent of people for whom the alert did not work, although I was with people who did. Obviously, it's still early days and there's hopefully time to iron out any issue with the system before it's required. You can read more about the public emergency alert system in our exclusive feature with Everbridge 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: April 2023

CONTENTS

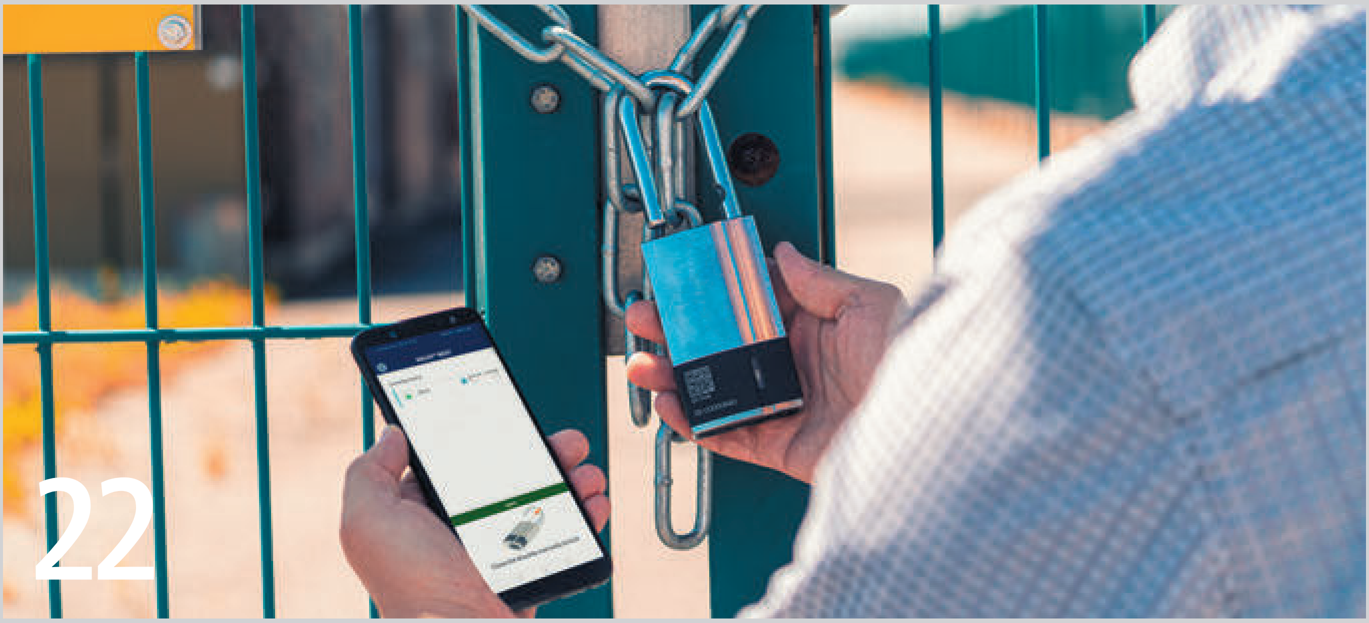
April 2023

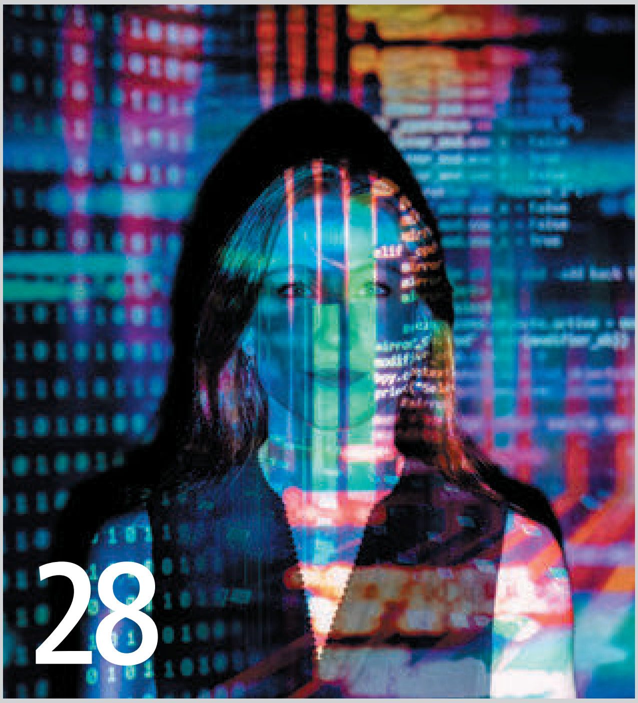
www.intersec.co.uk

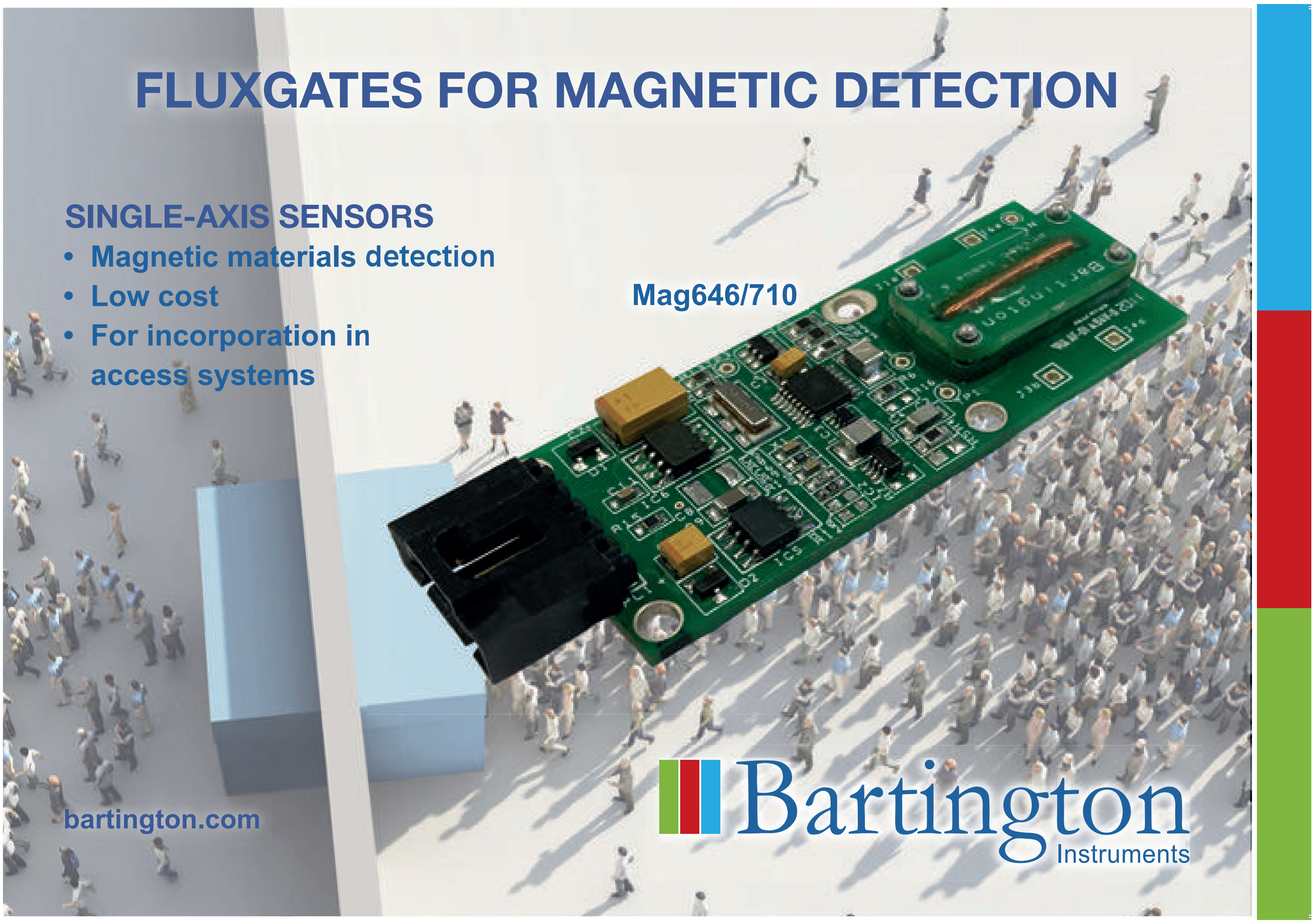
intersec

Features

Regulars







Operations head north

Major General Julian Thompson CB OBE Principal Consultant Editor

President Macron of France is a persistent critic of the North Atlantic Treaty Organisation (NATO). He is dismissive of its achievements implying that it achieves little and should be replaced by a European Defence organisation. One suspects that his anti-NATO stance is caused by a Gallic dislike of American dominance of NATO and a wish to play a more important part personally. These were opinions expressed by Charles de Gaulle with, it must be said, better credentials to consider himself best fitted to head an international defence organisation. Macron's attempts to cosy up to Mr Putin are to no avail. He would do better if he publicly endorsed NATO's efforts to show determination and strength as was demonstrated in March this year in Exercise Joint Viking in North Norway.

The exercise involved more than 20,000 military personnel, about 50 aircraft and around 40 ships training in the unforgiving winter conditions of northern Norway led by the Norwegian Armed Forces who provided the majority of the troops. The rest were contributed by Canada, Finland, France, Germany, the Netherlands, Sweden, the United Kingdom and USA. It attracted the attention of the Russians in the form of Russian Navy Maritime Patrol Aircraft (MPAs) whose snooping activity was monitored by the Norwegian Air Force F-35A Lightning fighters.

Norwegian Lieutenant General Odo, Chief of Norway's Joint Headquarters and overall commander of Joint Viking, said: "the war in Ukraine showed that you cannot take good preparedness for granted". He continued by emphasising that preparedness must be maintained on a regular basis and tested on tough, demanding exercises. The harsh Arctic conditions of North Norway in Winter provide an ideal proving ground for honing fighting ability and resilience.

Included in the overall scheme for Joint Viking was Exercise Joint Warrior a bi-annual exercise that incorporates surface, sub-surface, airborne and land scenarios to provide joint training in a multi-threat environment. Participating nations included the US, UK, Canada, Denmark, France, Germany, the Netherlands, Norway, Spain and Poland. The exercise allowed participating forces as part of NATO to demonstrate that they are among: "the most capable fighting force on earth", in the words of one of the senior participating commanders.

In support of security in the High North, the UK has established a new operations base to support Britain's Royal Marine Commando at the tip of the Arctic spear, the fighting formation that the UK provides when troops able to fight in extreme cold weather conditions are required. The camp is located about 40 miles south of Tromsø, and near the air base of Bardufoss from where the Commando Helicopter Force operates.

Joint Viking involved more than 20,000 military personnel

Picture credit: Crown Copyright

One of the key events during Joint Viking was a parachute descent by Royal Marines of the Surveillance and Reconnaissance Squadron (SRS) from a Dutch C-130 Hercules alongside men of the Royal Netherlands Marine Corps. The target was defended positions behind enemy lines. The Royal Marines bring another set of skills to the battle, a surprise approach by navigating, climbing, or swimming to places and by routes perceived by the enemy as impassable. That is why the SRS undertakes intensive ice climbing training in Norway. This allows the SRS to overcome obstacles such as frozen waterfalls and exploit unpredictable approach routes.

These joint exercises hone readiness capabilities and demonstrate resolve more effectively than any amount of talk can do. As a very senior German officer remarked to the author about a NATO exercise in the North some years ago, when a senior officer from a non-NATO country questioned the wisdom of an exercise so close to the Russian border: "it will show the Russians what will happen to them if they invade NATO territory". That is the sort of language Putin understands.

Picture credit: Getty

RED ALERT!

Lorenzo Marchetti *throws a spotlight on essential citizen safety practices as the new UK public alerting system swings into action*

Threats to public safety can come in many different guises, from extreme weather events such as hurricanes and fires and public health incidents, through to terrorist attacks, civil unrest and more. It is always a challenge for public authorities to anticipate and manage unpredictable events that put citizens at risk. Consider some of the most notorious attacks on British soil in the last six years: the bombing at Manchester Arena in 2017, which killed 23 people and injured 1,017; the Westminster car attack, which ran down pedestrians in 2018; the terrorist attack in a Reading public park that killed three and injured three others in 2020; and the Liverpool Women's Hospital bombing that was thwarted by a taxi driver in 2021.

The police, local and national authorities almost always come under scrutiny for not foreseeing the danger signs, but they are also criticised for mishandling events when they do unfold. In many instances, even when a public safety system is in place, the authorities find it challenging to reach everyone, everywhere and every time. The systems they use may also have limited capability such as not offering multi-channel alerting, and if those systems are aging, they may not be equipped to interact successfully with the latest technology including 5G or satellite communication.

In the European Union, public warning technologies have been considered and evaluated for some years and deployed across various countries. The advantages and disadvantages have been weighed to determine what type of system would be most suitable; but despite the implementations, timeframes under the EU Directive

The platform is fully compliant with data privacy regulations and allows public safety agencies to send an alert to any device without sharing any personal details

(2018/1972, which established that by June 2022 all member states should have adopted public warning systems able to reach end-users during emergencies) already having come and gone – there are many EU nations where no population alerting system is yet in place. In 2020, the Body of European Regulators for Electronic Communications (BEREC) listed in its guidelines both cell-based and application-based solutions as viable public warning systems falling under Article 110 of the Directive.

What has been clearly determined by the impact of natural disasters in Europe, such as the floods in July 2021 that hit Germany, Netherlands and Belgium, is that member states would benefit most from phone-based systems. The quickest method for communicating during an emergency is to use people's mobile phones via cell broadcast, which can reach millions of people in mere seconds with clear guidance and without the need for an app download, registration or mobile operator provider distinction. Cell broadcast enables all mobile devices in an affected area to be instantly alerted by drawing an area on a map. Messages are then received simultaneously on each device within that area.

Another alternative technology option is location-based SMS, which uses the infrastructure of telecom operators to send SMS messages to all connected devices. A combination of both cell broadcast and location-based SMS will reach the maximum number of citizens.

The public emergency alert system in the UK, powered by Everbridge's cell broadcast technology, has only just been introduced. Announced by the Government in March, it has been tested on three of the UK's biggest mobile networks – EE, O2 and Three – which represent the majority of UK mobile subscribers and a population of over 65-million residents plus an additional 35-million annual visitors.

The cell broadcast-based system leverages existing telecom infrastructure, with no opt-in required which means that everyone within a geographic area will be alerted if they are at risk from a public safety or security event. The UK system will also support first responder communications and analyse disaster communication effectiveness for subsequent mitigation activities. The implementation project in the UK was one of the first to closely involve the national security apparatus, which was engaged in setting up and checking the implementation of the security requirements, end-to-end. The platform is fully compliant with data privacy regulations including GDPR and allows public safety agencies to send an alert to any device within a few seconds without sharing any personal details, such as names or phone numbers.

So, let's have a closer look at public alerting technology. It must be rapid, reliable, require no prior action by the people it's trying to protect and not suffer from congestion. Ideally it will be disseminated through a multi-channel approach that can communicate effectively to diverse audiences facing any hazard and across all stages of the emergency. Incidents can also cut across geographic, policy, political, cultural, language and legal boundaries which means alerting systems must do the same. There also needs to be balance in the management of public alerting because while speed of response is vital, decision-makers must consider the full lifecycle of the incident and ensure alerts reach the right people with the right message to elicit the correct response.

Because public alerting systems are technology-based, their development and ongoing effectiveness does have to take into account the awkward topic of obsolescence. The pace of innovation in communications tech is undeniably relentless. 5G and subsequent advances will bring even faster and more ubiquitous digital services and increasingly these will be enhanced through machine learning and artificial intelligence.

DECISION-MAKERS MUST ENSURE ALERTS REACH THE RIGHT PEOPLE WITH THE RIGHT MESSAGE

Which means that an effective system cannot be built on a solution that becomes unusable or outdated in a few years – it must be capable of adapting to developments and changes in the way the public communicates. It is pointless to focus on the application of new technologies to old models. That said, public alerting systems should also be retrospectively functional, for example, users of 3G phones must be able to receive emergency alerts.

There are several best practices that should be considered by national and local authorities for a full-scale public alerting system if it is to meet the requirements of reaching all citizens, leaving no one behind and ensuring a multi-agency response to any incident or event.

COMMUNICATE ACROSS ALL PHASES OF THE INCIDENT

If possible, plan ahead for the most likely incidents that might occur and prepare citizens. When the event happens the public needs to be alerted as quickly and as efficiently as possible. Authorities then need to respond or to communicate through the response phase, ideally in the local language and through two-way communication. This includes to those who can help to let them know what to do. During the recovery phase it's also essential to keep communicating, which can help to mitigate the ongoing impact of the event.

COMMUNICATE WITH ALL STAKEHOLDERS

This means everyone from citizens and visitors to community volunteers, emergency services, support agencies and government departments. All resources available to support an incident should be known and contactable when an incident occurs across multiple channels and with the ability to automatically send messages in the appropriate language to improve the effectiveness of communication to international travellers.

COMMUNICATE WITH THE RIGHT PEOPLE AT THE RIGHT TIME

At each stage of an incident, authorities need to be able to answer the questions: who can help? Who is impacted? Who needs to know? For each category of stakeholder, authorities should know what is the best way to go about contacting them based on the precise nature of the incident and communication that needs to be sent and to seamlessly engage in two-way communication to check on whether they are safe and to receive requests for assistance.

LEVERAGE LOCATION INTELLIGENCE

Where do people live and work most of the time? Where are they now? Can authorities access historic 'snapshots' of where people were six hours ago? By using location intelligence and building situational awareness, emergency services and local authorities can track the location of those that might need help, determine the density of people in an incident area, or how they are moving because of the incident. If a hazard has been unidentified in an area – such as the poison in Salisbury – it will become necessary to alert all individuals who have been in the area over the previous 24 hours using historical location data. Location information can be critical in determining the message to send to the public in any given area or the allocation of emergency services. With geolocation, it's even possible to build models related to population densities at given times or predict the likely location of an individual based on their previous historical behaviour.

> **THE QUICKEST METHOD FOR COMMUNICATING DURING AN EMERGENCY IS PEOPLE'S MOBILE PHONES**

MAXIMISE THE EFFECTIVENESS OF TECHNOLOGY

A combination of cell broadcast and location-based SMS, with situational awareness capabilities, covers all bases. But public alerting technology is always evolving and it's important to consider the role that new and emerging tech will play. 5G offers improved signal strengths, range, material penetration, bandwidth and location date. Machine Learning can analyse huge swathes of data to find patterns and make predictions that would take humans months. AI can be used to help with advanced decision-making and situational awareness for authorities. Soon, we will see the addition of chatbots that are fed information through machine learning so people in danger can get assistance.

The UK, like any other country that is embarking on a new method to keep its people safe, can learn from other countries such as Norway, Sweden, Iceland, the Netherlands, Estonia, Australia and New Zealand when it comes to ensuring its public alerting system is effective. By involving all stakeholders and authorities in its practical deployment it will help to improve engagement and effectiveness and adapt the system based on the unique characteristics of the country, especially as weather-related events, such as wildfires and flooding, are on the rise. Finally, it will be essential to communicate to, and educate the public and visitors so they are more ready to understand how public alerts can help keep them from danger and invest their trust in the system ●

Lorenzo Marchetti is Senior Government and Public Affairs Manager at Everbridge.

> **Location information can be critical in determining the message to send in any given area or the allocation of emergency services**

Picture credit: Getty

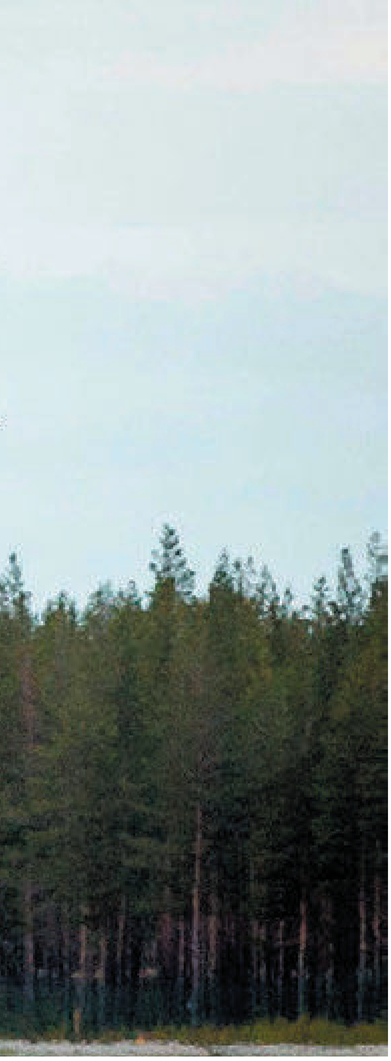
Picture credit: Crown Copyright

CALCULATED RISK?

Barry Scott Zellen *examines, following Turkey and Hungary's consent, the approval by all NATO member states of Finland's NATO accession*

On 30 March, the Turkish parliament ratified Finland's application to join NATO, taking down the final roadblock hindering Finland's much delayed accession into the expanded Atlantic alliance just two days after the Hungarian parliament did the same. Both nations continue to thwart Sweden's accession, however, leaving this last Nordic state outside of NATO for the time being. But unlike Norway, a NATO founding member, and Finland, its newest member, Sweden does not share a land border with Russia at all; therefore, Finland's accession to the alliance is all the more consequential, further encircling Russia by integrating its last non-aligned Nordic neighbour sharing a common frontier, bringing western military power to Finland's 1,340km long border, which combined with Norway's 196km border already fully embedded into NATO's strategic architecture, will soon create what will become a 1,536km fortified frontier to contain any possible future Russian aggression against the Nordic region.

Widely perceived as a diplomatic and strategic setback to Russian strongman Vladimir Putin, who launched his Ukraine invasion over one year ago in part to prevent Kyiv's further drift into the western camp and to forestall it from eventually joining NATO, and – Putin likely hoped – to thus deter other non-NATO states along its perimeter from seeking membership down the road, thus far Russia has not expressed any



The Swedish Air Force takes part in Exercise Arctic Challenge

grave concerns with this northern expansion of NATO. But in the years to come, it is anyone's guess whether Finland's abandonment of its long-embraced policy of neutrality will help or hinder its quest for greater security. For the moment, six of the seven democratic Arctic states are now bound together as military allies, providing a measure of hope that none will experience what Ukraine has gone through during these last 400-plus horrific days of war.

For greater insight into the impact of the NATO accession on Finland, *intersec* spoke with University of Lapland professor of International Relations and acclaimed author, Dr. Julian Reid, based in Rovaniemi – just 415km by air and 583km by road to Russia's northern naval bastion of Murmansk, and the target of Soviet troops during the Battle of Salla in the Winter War between the Soviet Union and Finland, when Moscow initiated its unsuccessful lightning conquest of Finnish Lapland. But just a few years later, during the 1944 Lapland War between Finland and Nazi Germany, the Battle of Rovaniemi resulted in the near-total destruction of the city. With Ukraine now experiencing Russian aggression on comparable scale of destruction as experienced in the Lapland War, and a military stalemate reminiscent of the Winter War when they were outgunned and outmanned Finnish defence forces held off the numerically superior Soviet invasion force, there's little wonder why Finland has so quickly pivoted from its long history of neutrality to full NATO membership. But the repercussions of Russia's loss of one of its longest and most stable neutral buffers along its western frontier as NATO comes ever closer to the Russian heartland remain to be seen, and is the subject of our interview with Dr. Reid.

intersec: How goes the NATO expansion in Finland and how do Laplanders feel about it? Do they find comfort in the military protection from an expansionist Russia or do they worry it may provoke a bear that had been productively cooperating regionally with the Nordic states? Are there second thoughts and regrets on abandoning official neutrality or has neutrality largely disappeared as Finland grew closer to NATO over the years since the Soviet collapse?

Dr. Reid: The overarching sentiment of the Finnish public is indeed one of comfort and assurance that NATO is willing to take Finland as a member. There is confidence that this is the right move, and scant sense that it might provoke Russia or make Finland less secure. The process by which Finland has grown closer to NATO has been gradual, although it is difficult to overstate the importance of the invasion of Ukraine for hastening the shift of its allegiance westwards. It has happened with a sense of urgency, underpinned by fear. Parliament and the policy community have mimicked the public mood, and it is very hard to locate meaningful opposition to NATO membership anywhere here.

But it's not just that there is a lack of opposition which is the problem. There is a real lack of strategic imagination. And that lack has played a major role in determining the ease with which the process has moved forwards. The conversation has been polarised, and parliamentarians as well as policy and media 'experts' have all tended to take the same simplistic pro-NATO stance, with little consideration for the nuances of the problem and virtually no lateral thinking. I would have liked to see Finland develop a more inventive response in terms of policy and strategy, rather than the rush to join NATO. If not just continued neutrality then a stance with more flexibility.

intersec: Does the expansion of NATO make Finland more secure or might it bring new risk?

Dr. Reid: The simplistic assumption is that joining NATO makes Finland automatically more secure, because bigger and more powerful states are then not only allied but contractually obliged to act in the case that Finland were to be attacked in the way Ukraine was. Commentators and policy makers talk endlessly about NATO's Article 5 and the security guarantees it supposedly brings. This is naïve to say the least. Since 2014, NATO has been placing ever greater emphasis on Article 3 and the obligations of member states to practice 'resilience' and 'self-help' in the case of armed attack by another state. In fact Finland has been flaunting itself during the process of application for membership, by talking up its capacities in the area of 'resilience'. If Russia were to attack Finland, you can be sure that it would be the resilience of Finnish society and its armed forces which would be called upon by NATO as a fundamental means of response.

> THERE IS NO SENSE THAT THIS MIGHT PROVOKE RUSSIA OR MAKE FINLAND LESS SECURE

intersec: Has Turkey's continued opposition to Sweden's ascension (unless it renounces it support for the Kurds and extradites selected 'terrorists' and other bad actors to Turkey), and Hungarian resistance to expanding the alliance to include Sweden (in tacit support of Russia) led to any second thoughts in Helsinki?

Dr. Reid: No, not at all. The opposition of Turkey and Hungary has been cast as a minor irritant, and something simply to be dealt with and surpassed, but not in itself a reason to reconsider. Nothing seems to be able to confuse Finland's certainty as to the wisdom of its application to join NATO.

intersec: While Russia has appeared unconcerned in its public statements with the NATO expansion across the Nordic region, could Moscow in fact be more upset than it has let on, and might this lead to increased tension and potential conflict with Russia that might otherwise have been avoided through continued neutrality?

Dr. Reid: For sure. Maybe 'upset' is the wrong word though. I am sure, given their larger views on NATO expansion, that Moscow will be taking it very seriously indeed, and that all its calculations concerning present and future strategic engagements with NATO, and with Finland in particular, will be changed accordingly. This will have every consequence long into the future, practically for as long as anyone can foresee.

intersec: If Russia does feel pressure from the expansion, what might it do – could it use force, or hybrid-warfare methods below the threshold of war, to sow the region with instability and where might it do so? Would Lapland be at risk?

Dr. Reid: They will certainly be looking at other areas of the border with NATO as potential spaces to act and change the dynamics of the conflict with and in Ukraine. It would make common sense to do so. One way or the other they have to engage NATO with a view to weakening it.

> SO FAR RUSSIA HAS NOT EXPRESSED CONCERN ABOUT THE NORTHERN EXPANSION OF NATO

How and where that will happen, we will have to see. But for sure, Finland has offered itself up as a potential battle space, and that includes Lapland too.

intersec: With their land borders now closed to Russian entry, has the Nordic region shut off a much-needed escape hatch for young Russian men avoiding conscription and opponents of the war avoiding persecution – and would allowing refugees to arrive by land provide a helpful escape route for opponents of Putin's war?

Dr. Reid: For sure. The closing of the border and the severing of relations with Russians, including the Russian academic community, looks really narrow sighted for all sorts of reasons.

intersec: Has the war in Ukraine, by consuming fighting men from Russia's remote northern communities as well as military weapons and ammunition hitherto stored in the north near to the Nordic states, paradoxically reduced the military threat Russia poses to the Nordics?

Dr Reid: That would certainly be one way of looking at it. It would be foolish to underestimate the importance of the Arctic to Russia though. Given that its contemporary strategy of cooperation over conflict in the Arctic no longer has the same value, I think we can anticipate a shift towards their using conflict as a means by which to make strategic gains. They have no choice when the other Arctic states are offering them so little to work with otherwise.

intersec: What's your prognosis on the year ahead: will the Ukraine war expand geographically, might Russia implode militarily or experience internal upheaval comparable with the end of WWI when domestic instability rendered its military unable to project power externally? Or, might Russia master the art of protracted warfare, and regain momentum – in Ukraine and beyond. Could Russia turn to its nuclear arsenal to double down on the fight and would this increase the security risk to the Nordic region?

Dr. Reid: I think Russia is invested in its ability to hold out in Ukraine and fight a protracted war against adversaries the morale of which will be worn down over time. How long that might take it is impossible to say. One has to look at this current conflict in context of the realities of US economic and strategic decline, the growth of power of China and the immiseration of Europe. In context of which Russia has every reason to trust in its capacities to outlast the West in Ukraine. ●

Barry Scott Zellen, PhD, is *intersec*'s International Arctic Correspondent

NATO Secretary General Jens Stoltenberg with the President of Finland Sauli Niinistö

Picture credit: NATO

Kestrel TSCM ® Professional Software

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

Signals Intelligence Support System ™

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

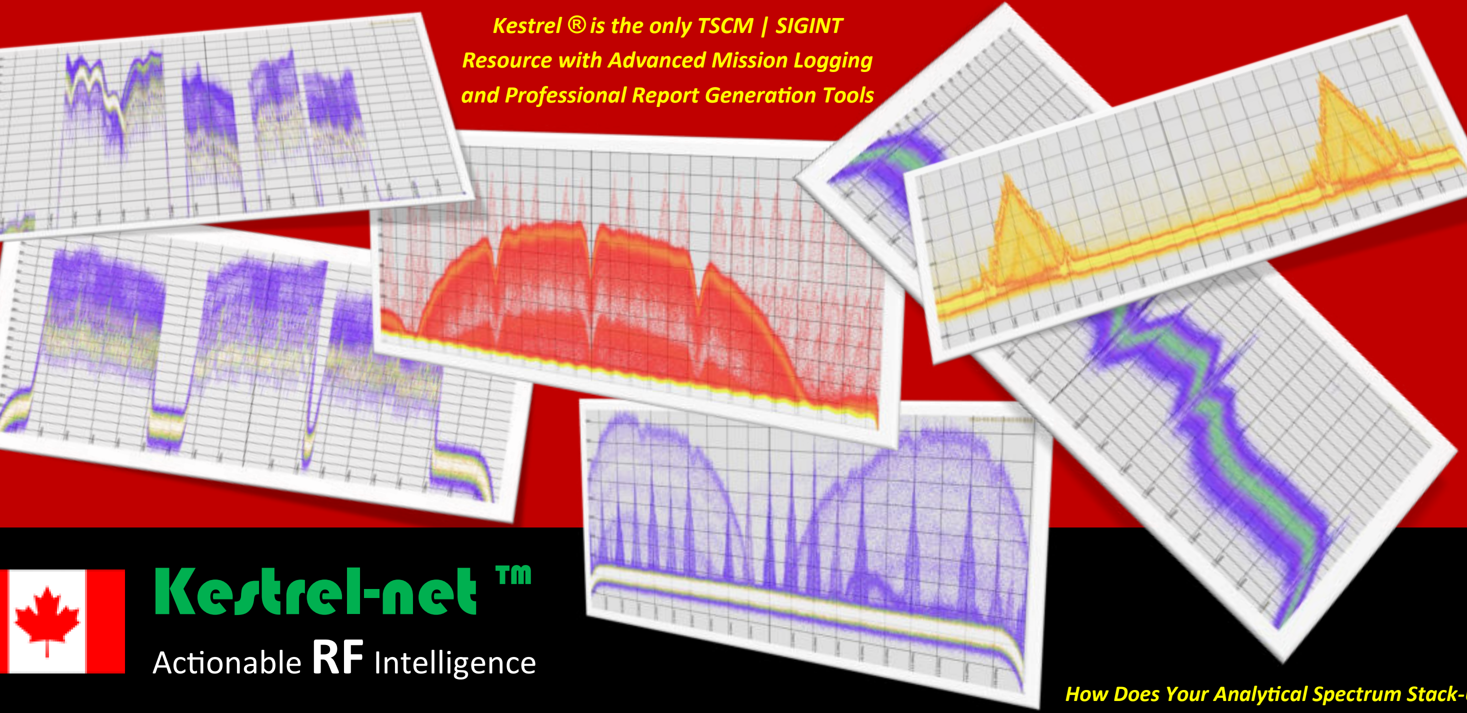
This is Not Just Another TSCM Spectrum Analyzer! | Now You Can Have Tomorrows TSCM | SIGINT Software — Today!

Kestrel TSCM ® Professional Software

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

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

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

INFORMATION WARFARE

Jorge Marinho *addresses various aspects related to influence operations, such as targets, social and individual resilience, ontological security and (counter)intelligence*

This article addresses various aspects related to influence operations, such as targets, social and individual resilience, ontological security and (counter) intelligence. The internet and Artificial Intelligence, as well as a few aspects with regard to training future information/psychological warfare professionals are also highlighted. This work results from the bibliographic research and exclusive interviews with a variety of experts. As part of this piece, it is vital to take into account the concept of influence operations: in general, every activity conducted by states or by any other groups, in both times of peace and wartime, including the gray-zone context, with the aim of influencing a target audience. Specifically, this article is centred on the influence exerted on certain audiences, depending on the messages/narratives conveyed through various channels, such as traditional and social media. According to several authors, often the terms information operation and information warfare are used indiscriminately, that is, as synonyms. There is a variety of terms that can generate confusion: psychological operations, influence operations and information warfare. In all this, there is a common goal that this article focuses

In the case of a conflict between nations, information/influence warfare can be used, by one of the parties, to disrupt the regular functioning of the other

on: influencing (Information Operations/ Psychological Warfare).

For US military operations, intelligence and information operations are crucial components, with information comprising the essence of both communities. There has to be a high degree of coordination between those backing intelligence support and whoever plans and executes operations in the information environment. Among various aspects, intelligence services can provide details regarding targets of information operations.

In the words of Jahara Matisek, the Information Operations Division at US NORTHCOM seeks to cooperate with the intelligence community, when it comes to defending the American homeland against opponents' campaigns and promoting American values in the Western Hemisphere. This National Security Affairs department professor at the US Naval War College adds that, in relation to US intelligence agencies and military units involved in information/psychological warfare, there could be some sharing of the best practices and ways of identifying adversarial actions.

The targets of influence operations could include large swathes of the population of one or several countries, groups of people or an individual. From Jahara Matisek's standpoint, this latter case could end up being part of the next major conflict, given that, in reality, few Western citizens are ready to face well-structured adversarial operations that could go by way of direct messages (DMs) of various social media. James Farwell states that, currently, within the sphere of influence operations, individual targets are important.

According to Jennifer Counter, if an influence operation comprises a narrow goal, the target can be a small group or a single person. This expert points out that, for the sake of efficacy and efficiency, it is vital to have a good understanding of the key public. Counter considers that, in this age of social media and microtargeting, it is easier than ever to address key messages to a target audience comprising a small number of people.

Selecting foreign individual targets and channels for precisely sending them the messages constitutes relevant aspects of influence warfare. Matisek stresses that Artificial Intelligence enables gathering data found in the public sphere on an individual and, based on this, sending him/her messages that have been created specifically for them. This way, according to Matisek, as part of psychological warfare, a different reality can be socially and digitally constructed, in the infosphere of the individual target with which he/she coexists.

James Farwell, Jahara Matisek and Christopher Paul all point out that there is increased intensity and breadth of information/psychological operations, when these are automated, namely with the use of socialbots. This, according to Matisek, can be dangerous, when looked at as entailing a relatively low cost and with hardly any risks, given that there are no precedents for this type of actions on the international system, as to drawing red lines; thus, the likelihood of a conventional military response is low, at least up to the present moment.

Also in the sphere of the internet, Farwell believes that, without generalising, troll farms/factories can be effective, when strongly affecting certain sites and through clever social media. In the opinion of Christopher Paul, troll farms play a relevant role, as part of foreign malign influence, thus allowing a government or group to take advantage of individuals' power to manage the contents of a much larger number of people and accounts that are fake.

Petros Petrikkos states that, in the case of a conflict between nations, information/influence warfare can be used, by one of the parties, to disrupt the regular functioning of the other State and of society in general, thereby calling ontological security into question. For this to happen, when dealing with a systematic process, Petrikkos feels that information resources and time are needed. They explain that, first off, information is gathered on the target country, to identify and subsequently exploit its vulnerabilities. According to Petrikkos, a target, with its functioning disrupted and with no resilience, becomes insecure and more permeable to influences, with regard to its identity.

IN THIS AGE OF SOCIAL MEDIA IT IS EASY TO ADDRESS KEY MESSAGES TO A TARGET AUDIENCE

Jennifer Counter feels that the narratives that guide who we are and the position we take up within a group are very powerful, to the extent that identity is an essential part of the individuals and the society we live in. This is why, she points out, that influence operations can be very dangerous when they seek to gradually weaken aspects that serve as the basis of society – such as shared histories, values and norms. From an offensive standpoint, Counter believes that casting doubt on foundational ideas can somehow serve to create divisions between citizens and their State, between people of different groups in society (in religious and ethnic terms, for instance) and among family members or a circle of friends. According to Counter, part of warfare includes determining target audiences and the messages that gradually destroy societal narratives, thus contributing to, for example, undermining an adversarial government's credibility.

Various experts, including Christopher Paul, Jahara Matisek, James Farwell and Jennifer Counter, acknowledge that, on the international stage, influence operations geared to certain countries already dealing with some social, political and economic problems, possibly combined with involvement from certain local leaders, can contribute toward triggering or heightening uprisings.

From Jahara Matisek's perspective, a specific country's social resilience constitutes a hindrance in relation to threats of psychological warfare. This officer feels that, currently, any society should invest in digital literacy, critical thinking and civic education. With regard to this, Matisek points to Sweden and Finland as two countries that are exemplary in addressing psychological warfare, strengthening their societies, in order to triumph over malign actors seeking to cause divisions through disinformation and misinformation. He explains that, with similarities, the models of the two countries mentioned, respectively Total Defence and Comprehensive Security, present an overview regarding security and national defence, to the extent the elements of the public and private sectors are aware of the role they need to play in a crisis situation. This professor advocates that every citizen's involvement in national defence allows for both individual and collective strengthening that will serve to withstand adversarial influence activities, among other aspects.

Christopher Paul underlines that more effective counterpropaganda strategies should consider every stage of propaganda. Several researchers conclude that, in order for malign or subversive information to be effective, it must successfully go by way of the stages of production, distribution/redistribution and consumption. This is why, with a far-reaching perspective, the fight against said types of information shall concern every stage, not just in consumption, as is the case with fostering resilience, even if such is somehow positive .

TARGETS OF INFLUENCE OPERATIONS CAN INCLUDE ONE OR SEVERAL COUNTRIES

In relation to the activities conducted by counterintelligence services to prevent influence/psychological operations in their countries, Jennifer Counter maintains that, first of all, we need to understand that influence operations and campaigns comprise an end goal. According to Counter, an overview may be lacking, when too much attention is often paid to certain specific contents, such as a tweet or a given account on a social media. This expert states that rarely are content batches compiled in order to grasp the message and be aware of the targeted key public, subsequently reversing the process so as to understand the actor and his/her goal.

According to Jahara Matisek, even though few governments and military organisations publicly disclose offensive or defensive operations, in the sphere of influence/psychological warfare, States generally apply some resources in identifying potential adversarial influence attacks. This type of counterintelligence activities, according to Matisek, goes by way of analysing trends, attempts to put an end to inflammatory information and collecting foreign IP addresses, for instance.

Jennifer Counter maintains that influence operations are more art than science. Among the multiple subjects that comprise training a future information/psychological warfare professional, she stresses political science, behavioural science, psychology, history, geography, anthropology, languages, social movements and measurement approaches (pooling, surveys and focus groups). James Farwell considers that a future information/psychological warfare professional should have talent and study hard, most notably cyber operations. As part of this, Jahara Matisek feels that a cyber professional, within the context of sociopolitical-information warfare, should be dynamic enough to understand a diversity of cultural, social, political and historical trends. Matisek adds that, from his standpoint, said professional should have characteristics that include a free spirit and an ability to come up with out-of-the-box solutions ●

Jorge Marinho has a PhD in Communication Sciences and BA in International Journalism. His main fields of expertise include: influence/information, psychological warfare; international communication, international relations and strategic communication.

Information is gathered on a target country to identify and subsequently exploit its vulnerabilities

OBEY
$1,000,000 QUESTION
ARE WE BETRAYING THE PLANET?
studies warn of damaging effects of global warming
RIGHT WING DENIES SCIENCE OF CLIMATE CHANGE... also claims Earth is flat, abstinence is the best birth control, and humans are the product of intelligent design

NEW TTK TACTICAL TSCM KIT

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

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*

MESA® hand-held Spectrum Analyzer

ANDRE® Broadband Detector

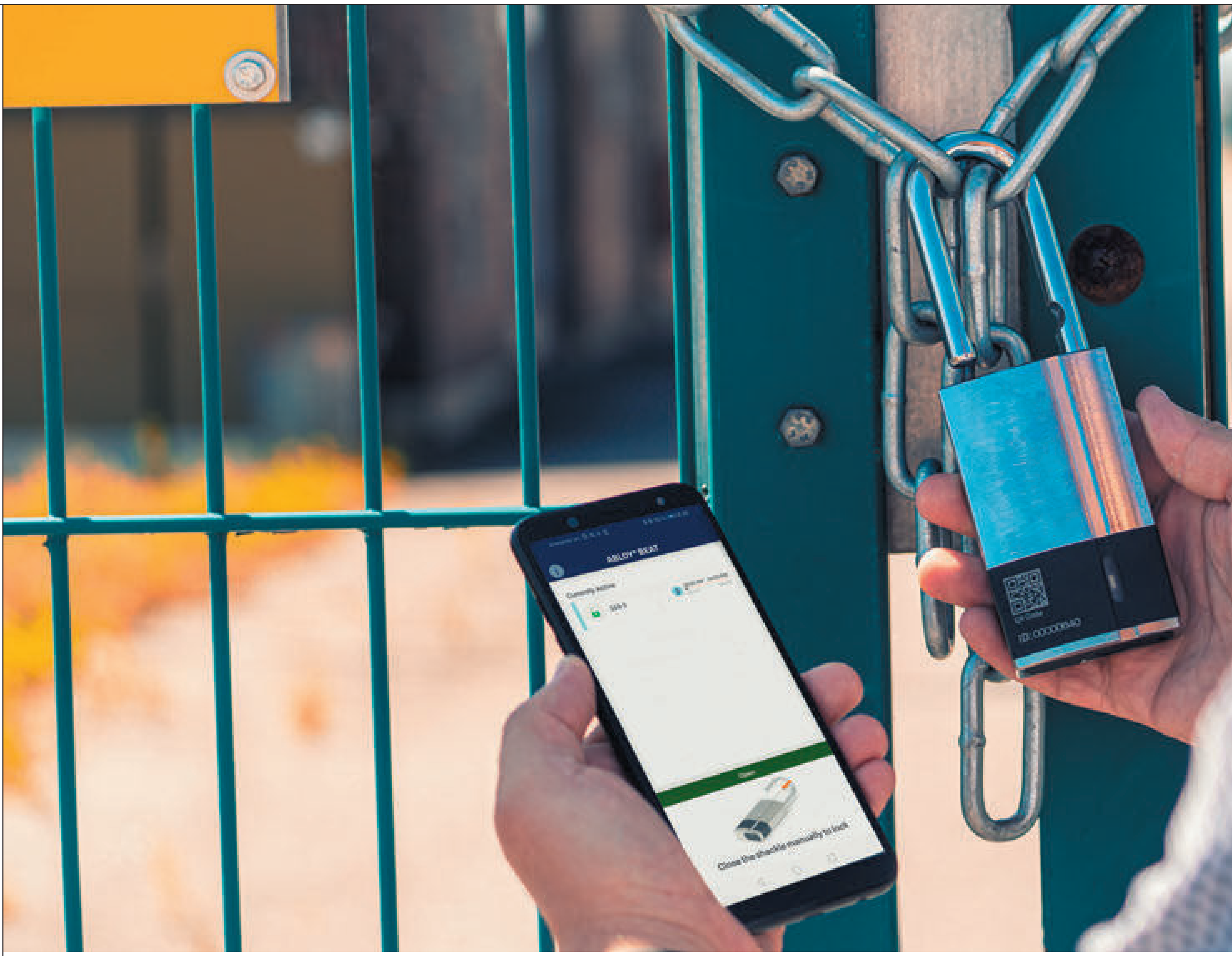
ORION® 2.4 HX
Non-Linear Junction Detector

CMA-100 Countermeasures Amplifier

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

REI®

www.reiusa.net



Picture credit: ASSA ABLOY

EMBRACING CHANGE

The importance of Access Control for Security

Through its thirty-plus-year history, the access control industry has quietly plodded along, out of the spotlight of change and transformation, doing what it has always been asked to: keep bad people out and lock and unlock. Overall, it has delivered on that task. To many in the industry, that is just how we have wanted it. But over the past three years, that has all changed. And it has changed in a big way. Before getting into those changes, let us define what we are talking about and discuss how we got here.

What is access control? Simply put, access control allows the right people to enter a space while, at the same time, keeping the wrong ones out. As an industry that is traditionally slow to adopt macro trends, it is starting to lean into digitalisation, transforming its solutions to keep up with modern-day needs. Security is fundamental to ensuring feelings of comfort and safety in occupants at work and home – so why not invest in the newest technology? This piece will explore the development of the industry and consider the importance of embracing change.

Let's go back to the beginning. While the key (pun intended) aspects are based on the same guiding principle – keeping the bad individuals out – access control has evolved to become more of a future-focused concept. In the Seventies, the industry was based solely

Access control is essential, not only for the workplace but for everyday life

on this former, more straightforward principle. An access control system could prove its worth by keeping occupants of the building from coming to external harm.

Naturally, this requirement is still needed today, but the systems implemented at the time failed to reflect other contemporary requirements – hence, the industry needs to evolve. This evolution is reflected in the industry currently adopting cloud and mobile computing, using APIs and a software-centric approach to business models and technical aptitude. With modern solutions involved, today's access control solutions deliver safety and security, conveniences, operational efficiency and even revenue generation. These concepts should exist together to create the best possible outcomes for professional and personal use.

While the industry's evolution has taken decades, historical events tend to speed up such occurrences; change is only possible with external factors. This is true of access control, as the COVID-19 pandemic highlighted important considerations that had yet to be given weight in the past. To control the spread of infection, those in charge of corporate spaces were forced to introduce seamless, contactless security systems and emphasise occupant health by keeping unwanted visitors out of the space. As a result, the industry was forced to step up with a different story and solution set to meet expectations and demand.

But what did this rushed evolution look like? From 2020 onwards, serious discussions on mobile and cloud architectures, electronic visitor management systems and even biometrics in access control increased, reflecting changing global safety requirements as individuals returned to the workspace. In its Physical Access Control System report, Fact.MR emphasised that the increased demand for biometrics was a large part of the Physical Access Control System industry's 13 percent growth in 2021. In practice, individuals have likely seen such change in their daily lives without picking up on its significance.

THE MORE SECURE AN INDIVIDUAL FEELS IN THE SPACE, THE MORE LIKELY THEY ARE TO BE HAPPY

With research portals now predicting an ever-increasing investment in space over the next decade, we must consider how it will affect individuals professionally. First up – corporate leaders and commercial landlords, who should be in no doubt that security investment is for the long term. By embracing the newest security solutions, these parties can prove dedication to the well-being of their employees and occupants (respectively). It may sound like common sense that the more secure an individual feels in the space, the more likely they are to be happy – however, such factors can go amiss when prioritising more overt workplace benefits. Therefore, business leaders who take it upon themselves to recognise the link, and embrace modern access control systems, will improve the mood of their workers and benefit from increased talent recruitment and retention.

Moreover, the pandemic's impact on the security industry was far from isolated. Not only did those looking into security have to keep health benefits at the front of their minds, but they also had to consider how people did their jobs – remote and hybrid working becoming the norm. Forbes has recently commented on the bosses attempting to reverse this culture shift, failing to recognise their impact on their employees who would instead work from home. With so many people afraid of losing their jobs in 2023's global economic climate, it is pivotal to business success that leaders find ways to make their employees feel supported, encouraging enthusiasm and attendance. Security is one of the best, underrated ways to demonstrate such a commitment to employees and reap the rewards. In summary, access control systems are fundamental to beating corporate competition as the world recovers from a global pandemic, demonstrating your dedication to your employees practically.

For workplaces that hold in-person meetings, the pandemic also brought to light another issue – handling visitor management. We went from visitor management systems only doing precisely that, managing visitors, to everyone being a visitor. With the change in how we manage the facilities and how we handle the people coming and going, a need for data and processes arose, reflected across leisure facilities,

▶

workplaces, and healthcare buildings. The right access control solution has become the one that collects and analyses such data, including digital visualisation, to ensure that only authorised visitors are allowed to enter.

With stakeholders, occupants and visitors to consider, how do you know you're choosing the right solution? Ask yourself the following question: does my chosen solution prioritise the user? Ultimately, if your access control system fails in its user-friendly credentials, it will fail to bring the value you expect from your investment. On the other hand, if you choose a solution that is easy to use, occupants will see clear benefits from its functionality.

COVID-19 HIGHLIGHTED IMPORTANT AREAS THAT HAD YET TO BE GIVEN WEIGHT IN THE PAST

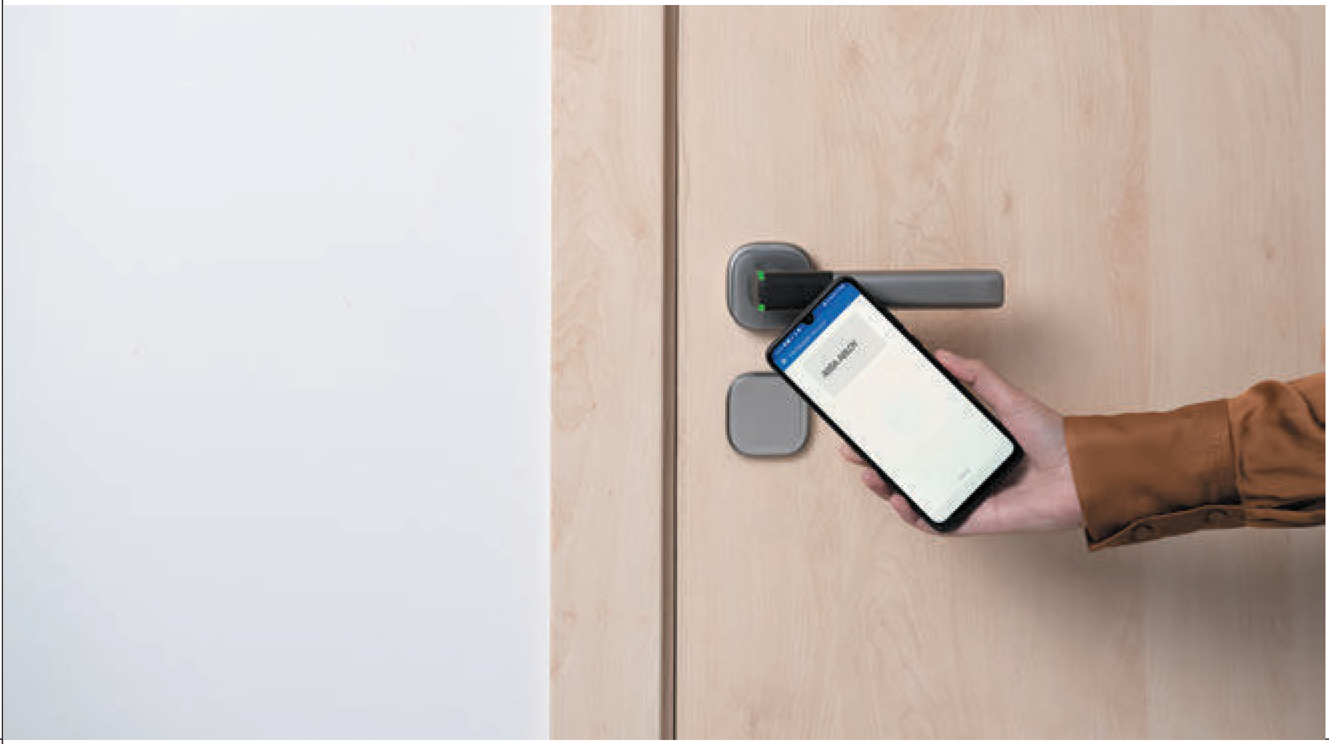
While there are plenty of benefits from embracing access control systems in the workplace, how would it help to include them in the home? As previously mentioned, security and feeling safe are fundamental to happiness and paramount in the place where people spend the most time. In a world where stress is expected and caused by numerous external factors, individuals are likely to do all they can to minimise the stress levels in their homes. Therefore, access control becomes essential, not only for the workplace but for everyday life. We can combat future mental and physical health issues with improved mood and reduced stress about security. But where to start?

As access control becomes an increasingly hot topic, household names like Amazon and Google are making it easier than ever to find your home's most up-to-date security systems. Earlier this year, Google Nest, in its partnership with ADT, unveiled its newest invention, the 'ADT Self Setup' security system. Not only does it attempt to make improving your home security more accessible by letting you set it up yourself, but it also uses the latest technology to connect all elements, including the camera on the Nest, to a 'Smart Home Hub command centre'. This reflects the importance of user-centricity, which is fundamental to a successful access control solution. Of course, such big tech players' involvement in the space doesn't render smaller companies obsolete. However, it demonstrates the increasing competition in the industry, reflecting growth in importance.

Another critical piece of useful access control technology for the home is the smart lock. Since its inception, the industry for home security products has seen a move from hardware to software. In the past, this move has failed to garner the expected enthusiasm – partly due to adaptation issues. The corporations offering additions to the locks already on doors have shown significant momentum – in no small part due to their user-friendly nature. However, their importance for residential homes should not be bypassed. Smart locks enable the collaboration of technology and security at a lesser price. This is especially true as more corporations come out with smart locks, battling to sell the most affordable and best.

Post-pandemic, office safety will be emphasised, with user-friendly models beating the competition. At home, corporations that make adaptation easy for customers will be the ones to succeed. With Big Tech poking into the discussion and increased investment in the space, access control is building significant momentum – for example, M&G Investment Management Ltd has just acquired over 99,000 shares in Napco Security Technologies. With such growth unlikely to slow down anytime soon, the industry is integral to the future of security, both at home and at work.

If this article has left you confident about the world of access control (good!) but unsure where to find the best solution fit for you, now is the time to sign up for the Access Control Executive Brief – the industry's only objective analysis of goings-on. ●



Today's access control solutions deliver safety and security, conveniences, operational efficiency and sometimes even revenue generation

Picture credit: ASSA ABLOY

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

ELECTRONIC COUNTERMEASURES

IPS EQUIPMENT & SWEEP TEAM SERVICES

NEW REI MESA MOBILITY
ENHANCED SPECTRUM ANALYZER

NEW ANDRE DELUXE 12GHZ
WITH ULTRASONIC PROBE

VIDEO POLE CAMERA
2.0 INSPECTION TOOL

EDD-24T NON LINEAR
JUNCTION DETECTOR (HANDHELD)

TSCM TRAINING
COURSES &
CERTIFICATION
UK/US/GLOBAL

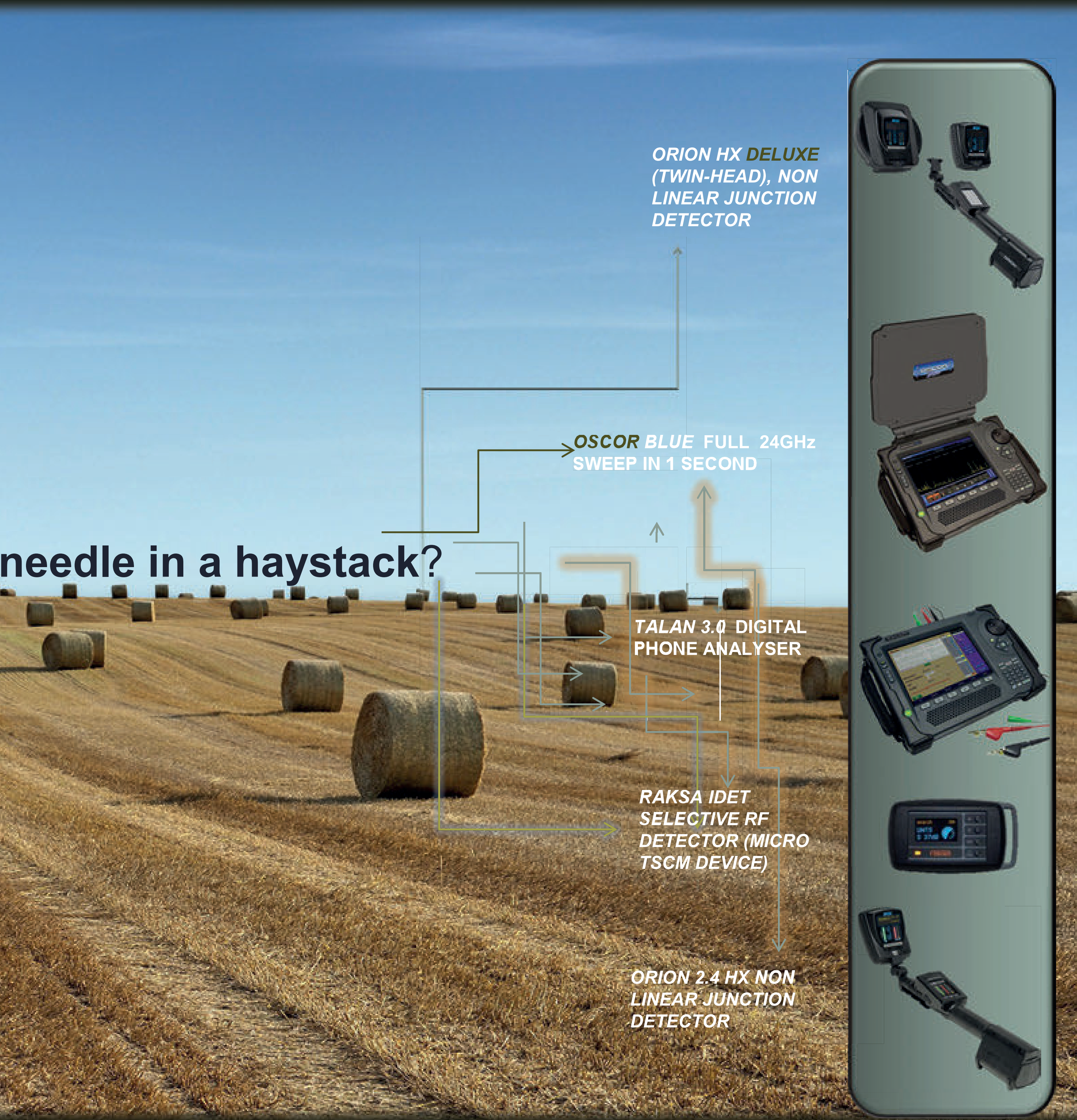
Looking for a

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**

REDRESSING THE BALANCE

intersec *invites a selection of women involved in cyber security to explain how the industry is evolving*

International Women's Day always prompts introspection about the role of women in society, how things have changed, and what more needs to be done to further equality. This is especially true in cybersecurity, where women are still underrepresented. Research from industry analyst Forrester estimates that just 24 percent of the global cyber workforce are female today. So, how has the role of women in security shifted?

Daniela Da Cruz, VP Engineering at Checkmarx, comments: "While we see that progress has been made in recent years, with many organisations actively trying to address gender diversity, the current representation of women in the cybersecurity industry is still relatively low.

"This is consistent with what we also observe in other tech industries, and I think different factors contribute to this: under representation, a lack of role models and gender bias. However, increasing efforts are being made to encourage women to pursue careers in cybersecurity."

While women are still a minority in IT security, there are still many in the field helping to reverse the trend.

Soma Sinha, Senior Manager Business Application, Engineering at Barracuda, comments: "I was fortunate that my parents sent me to study computer science. I joined the tech industry in 2004 and have seen many female leaders who have inspired me. Each of them emphasised the same thing: focus on your priorities, take pride in and enjoy and celebrate every phase of your life. I believe that

There is still a tendency for women to have to prove their worth before being accepted at the same level as a man

diversity brings different perspectives and enables every individual to prepare and perform better.

Stephanie Reiter, Chief Financial Officer at Delinea, shares a similarly positive outlook, commenting: "As a female CFO, I feel fortunate to have had several role models who showed how women can be senior leaders within an organisation. At Delinea, I'm proud to sponsor our first employee resource group, Women @ Delinea, where our mission is to promote positive roles of women in technology. We are building an inclusive community and welcome all of our team to engage with us on this mission.

"As a company, Delinea is committed to our core values including respect, ownership and being spirited in everything we do. We strive to create an environment where everyone feels those values every day, in every interaction with customers and colleagues, and in every experience they have at Delinea."

While equality appears to be improving, most women working in the field today have faced challenges by being the only female in the room. More often than not, negative bias seems to be unconscious rather than malicious.

Brenda Robb, CMO at Blackfog, notes: "I've spent much of my career in male-dominated industries and companies. In one instance I was the only female in the EMEA team for the first few years. When I sat down to write this, I initially wrote that I didn't recall any significant instances of inequality or discrimination, but on reflection there have been a couple that come to mind. Perhaps petty, but I do recall being asked to step out of a customer event in Rome to buy a gift for a C-Level's wife, a task I politely declined! I also recollect a management meeting many years ago where myself and only one other woman were present. Despite being senior to several men in the room, my female colleague was tasked with chasing up the coffee when it didn't arrive on time."

"Fortunately, I have always felt comfortable when it comes to pushing back, but I understand this is more difficult for some women who have no doubt had experiences worse than mine. My thoughts are that the issue of inequality may be felt less in marketing than in other areas of business. I first got into technology via PR, followed by events and later marketing, all three probably more dominated by women typically. I've been fortunate to be able to progress within the technology industry and at BlackFrog I am part of the leadership team and on the board of directors. Good companies are built by good people, regardless of gender, an ethos we follow at BlackFog."

Similarly, Christine Bejerasco, CISO at WithSecure, explains: "I [have faced] some hurdles throughout my career as a woman in a typically male-dominated industry. In the earlier stages of my career, I encountered negative bias as a woman working in the technology field.

"There was one notable experience, where I was hired with a lower salary than my male counterpart, despite working in the same role and having similar backgrounds and experience levels. At the time, I chalked it up to my experience level and didn't act on it, but today I'd definitely raise it as an issue. Happily, in this case, my salary was adjusted to match my male counterpart once my managers saw my skills in action.

She continues: "Nevertheless, it's not always the same case for every woman in the security industry. I still believe that women in tech face numerous challenges, especially when it comes to particular niche areas like cybersecurity. There is still a tendency for women to have to prove their worth before being accepted at the same level as a man. In my experience at least, it's often unconscious bias – the men are usually well-meaning and don't intentionally set out to discriminate and keep women out of the field."

Mor Bikovsky, Global Head of Business Development at Claroty, who entered the cyber field through seven years in the technology department of the Israel Defence Force (IDF), adds: "I've always worked in very male-dominated environments and have become used to being the only woman (and the youngest person) in the room. However, as a woman, you can achieve anything. At Claroty, for example, I've been awarded Employee of the Year by the CEO three years in a row.

WOMEN IN TECH FACE NUMEROUS CHALLENGES, ESPECIALLY WHEN IT COMES TO CYBERSECURITY

"For me it's important to simply ignore the biases, be professional and focus on solving the business challenge at hand – ultimately, just show up and do my job! As soon as people recognise my expertise, skills and knowledge, I quickly earn their trust. The key is to not let the initial judgments and biases hold you back from demonstrating your capabilities and proving your value right off the bat."

With women still representing less than a quarter of security professionals, and many still facing bias in their roles, the consensus is that more needs to be done in the years ahead.

"While there have been improvements in work culture and inclusivity, there's still progress to be made in terms of greater female representation in leadership positions and support for women entering the industry," adds Christine at WithSecure.

Devona Chia, Marketing Director APAC at Hackuity, elaborates: "We're now well into 2023, and certainly, the tide is turning for women around the world. We have more female Prime Ministers, Presidents, Directors, etc. than ever before. I have more female peers and colleagues that I work with who are rising to excellent positions of leadership. This is mainly down to a higher level of gender awareness within the industry, as well as STEM subjects becoming a core part of education for the youngest generations. Though that's not to say we still don't have a long way to go, I would say this is a common theme among the gender gap on the whole, as equally men are now entering traditionally 'female-only' roles such as childcare and education.

"To overcome inequality in the workplace you need to be a voice for change. Stand up to the opposition, whether female or male, nobody should be put down, especially your own team. Perhaps the hardest part is recognising this, but the more that talk about it, the more they'll be aware of what they say. Some people don't realise they are being hurtful or stereotyping."

There is a strong sense that women already in the cyber industry, as well as IT and technology in general, have the biggest role to play in further equality. Most agree women who have risen to senior roles can create a positive environment for others entering the field.

Mor at Claroty explains: "The most important advice I can share with other women in tech is to learn from and help others. At Claroty, I've become a mentor to

▶

women across multiple departments, including Product, Research & Development and Technical Support – giving them advice on career progression and promotions, shifts between roles and dilemmas in a male-dominated work environment. I've even got to the point where I give advice to men who are double my age with twice as much experience!"

Sheila Hara, Director, Product Management, Application Delivery at Barracuda, believes support should also focus on helping young girls gravitate towards technical fields. She observes: "To encourage more women into technology, we need to cultivate curiosity in little ones, so they are not afraid of technology when they are older. Talk science at home and run experiments (that do not destroy your home, for the most part). Cultivate courage – let girls jump off structures, swing on the monkey bars and bruise their knees so they feel brave and strong.

MOST WOMEN HAVE FACED THE CHALLENGE OF BEING THE ONLY FEMALE IN THE ROOM

"With women outnumbered in many technology workplaces, training and mentorship programmes that focus on the needs of diverse employees can create support and recognition of career goals and potential. We can all play a part in speaking for other women when they are not in the room. Let women know how important their contributions are to the company's success. Showcase their work and achievements and demonstrate to the entire organisation that women are valued. Keep the faith and trust the journey! Be kind to yourself and give yourself permission to excel."

Daniela at Checkmarx highlights three major steps that security leaders should be taking to promote diversity:

"Partnering with educational institutions to offer scholarships and internships is a great way to promote the security industry and create a diverse talent pipeline. By doing so, you can help students gain practical experience and exposure to the security industry, which can be invaluable in terms of building their knowledge and skillsets. Myself, as a teacher at university for Computer Science students, constantly promote these initiatives and the fact that I'm a woman in a leadership position might influence other women to understand it's possible to follow a similar path.

"Secondly, provide opportunities for professional development: we can help promote diversity by providing opportunities for professional development, including training, mentorship and coaching. This can help women build their skills and advance their careers in the security industry.

"And finally, create an inclusive culture. We, as leaders, should promote an inclusive culture where all employees feel valued and heard. This means recognising and addressing biases that may exist in the workplace and creating an environment where all employees feel comfortable sharing their ideas and perspectives."

Hacktivity's Devona adds that women also need to believe in themselves and their abilities. She comments: "My biggest piece of advice to women starting in tech: Believe in yourself. You are no less worthy than your male counterparts. Don't fall into an 'imposter syndrome' mentality. Believe in your worth, your experience, and the value of what you bring to the table.

"It's difficult when the door is shut on you. But don't stop there. Find a mentor that can help you. Especially at the start of your career, guidance is essential to shaping your growth! And network. Network, network, network. You never know when contacts will come to good use."

She concludes: "It's time to change the face of cyber. We've come a long way as females, but there's still a long way to go. Only one out of 365 days is International Women's Day, one too many. The aim is for that day to no longer be necessary. Ever" ●

Daniela Da Cruz is VP Engineering at Checkmarx. **Soma Sinha** is Senior Manager Business Application, Engineering at Barracuda. **Stephanie Reiter** is Chief Financial Officer at Delinea. **Brenda Robb** is CMO at Blackfog. **Christine Bejerasco** is CISO at WithSecure. **Mor Bikovsky** is Global Head of Business Development at Claroty. **Devona Chia** is Marketing Director APAC at Hackuity and **Sheila Hara** is Director, Product Management, Application Delivery at Barracuda.

Diversity brings different perspectives and enables every individual to prepare and perform better

TSCM & SECURITY SOLUTIONS

Delivered globally by the world's largest TSCM company

TSCM solutions

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

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

Security solutions

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

About QCC

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

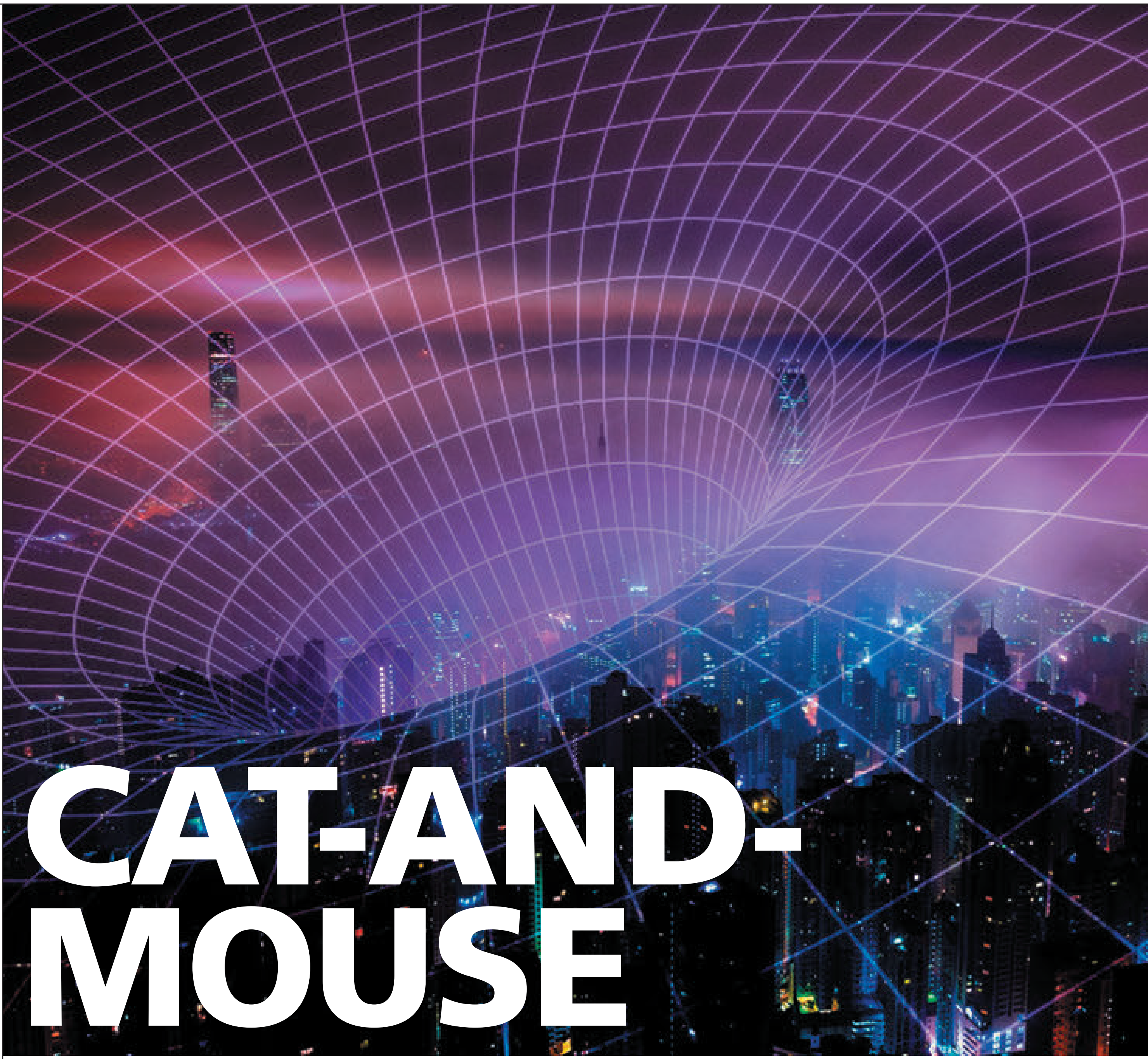
We are serious about what we do, and adopt a partnership approach to directly reduce our clients risk exposure.

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

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

ISO 9001 CERTIFIED
ISO 27001 CERTIFIED
ISO 45001 CERTIFIED
ISO 14001 CERTIFIED
ISO 17025

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



CAT-AND-MOUSE

Rani Osnat discusses *10 of the cloud security trends that organisations are likely to face in the continually evolving cyber security landscape*

As anyone involved with cyber security knows, it is a constant game of high stakes cat-and-mouse. Every year new attacks emerge, while new security solutions are created, and old security fixes are upgraded. Threat actors constantly append new methods to the old ones, using them as part of their ever-growing toolbox. With this in mind, below are some of the top trends organisations should expect to see over the next 12 months and beyond, in terms of new attack vectors in cloud native environments.

An increase in attacks that bypass agentless security solutions. Many organisations have been adopting agentless security models that utilise volume scanning to identify vulnerabilities and misconfigurations. Some have been using these solutions to detect threats in runtime as well. But agentless solutions don't detect certain attacks such as memory-resident malware. Threat actors are already using such evasion techniques in more than half of attacks, and are highly likely to continue this trend and append new techniques that bypass agentless solutions to their arsenal. Vendors will need to adopt supporting agent solutions in order to detect and block these runtime attacks going forward.

New severe vulnerabilities will be weaponised even faster. Recently, there's been an increase in the number of severe zero-day vulnerabilities. Some have been conducted through Remote Code Execution (RCE), including log4shell, Confluence, Zimbra and Zabbix among others. Over the past year, large botnets

As threats to the software supply chain escalate, CISOs will be compelled to develop and deploy better strategies

(such as Kinsing, Mirai, Dreambus, etc.) were able to quickly append these new vulnerabilities on top of their existing infrastructure, effectively both decreasing the time it takes to weaponise new zero days and increasing the reach of these new attacks. This trend is expected to not only continue, but even increase in the coming months. Consequently, vendors will face the challenge of rapidly updating threat intelligence feeds and solutions accordingly.

Attackers shift left – a new generation of attacks. Attackers often invest significant time and resources to detect new vulnerabilities in applications and the infrastructure on which it runs. Meanwhile, security practitioners utilise a range of solutions in various locations throughout their development lifecycle to detect and mitigate vulnerabilities including source code management security solutions, container image scanning, CI/CD security tools and runtime controls. Simultaneously, threat actors are now aggressively innovating and adopting new or emerging technologies themselves. It's expected that these threat actors will adopt similar approaches to improve and even optimise their campaigns. Attackers will begin to leverage offensive security tools such as code scanning to detect security issues in a victim's code and development infrastructure, especially if they're developing open-source software.

More creative attempts to bypass eBPF-based solutions. Over the past couple of years, there's been discussions about the advantages of eBPF-based technology for runtime protection, leading to wider adoption of agent-based solution technology. We've seen methods that seek to bypass eBPF technology and believe threat actors will continue to look for more creative ways to circumvent these solutions and avoid detection. Strong up-to-date security research that analyses campaigns will soon be able to detect threats, update the agents and block such bypass attempts.

A darker side of BPF. With the expanding adoption of eBPF technology, there's been exponential growth in the use of BPF and eBPF malware in the wild. In particular, state-sponsored threat actors have been using this technology to bypass security solutions and avoid detection. In fact, several new eBPF based rootkits have emerged on GitHub as proofs of concept. Expect to see an increase in such publications over the coming months. As eBPF-based technology is further adopted, it can also help to detect these elusive threats. Additionally, threat actors will likely use these open-source proof of concept tools to launch attacks in the wild, requiring advanced security solutions that have the capability to detect them.

The skills gap will widen further. With most organisations now leveraging cloud native architectures for the bulk of their digital transformation initiatives, the lack of knowledgeable staff to support the growing number of production applications running on these platforms is widening. Although more and more operations and security resources are being trained (or cross-trained) in Kubernetes, CI/CD pipeline automation and Infrastructure as Code (IaC), it simply isn't keeping up.

As a result, in order to bring production ready resources on board faster, both time-to-hire and overall compensation to fill these positions is expected to increase by more than 15 percent in the next 12 months.

Providers of professional services will emerge as winners. One way organisations are likely to address the growing skills gap is by relying more on partner-delivered services. Procurement models are shifting, with many customers buying technology solutions directly through cloud providers. This is also an opportunity for resellers and distribution partners to get creative in the ways they bring value to customers.

THIS MARKET DEMANDS THAT WE STAY AHEAD OF ATTACKERS AND ANY NEW TECHNOLOGIES ADOPTED

Timing will align with the growing appetite from customers for managed solutions and those partners who have built strategic relationships with vendors to provide advisory and professional services will win market share. This will shake up the traditional channel model for security products, leading to greater consolidation and fewer partners doubling down on individual vendors. That said, following in the footsteps of firms like Fishtech and The Herjavec Group, it wouldn't be a surprise to see additional M&A events in this space in the coming months.

Consolidation of tools for multi-cloud and cross-business use cases. Another way to address the skills gap is by maximising productivity of existing resources. As organisations move from separate pockets of cloud native development within their various business units to an environment where the architecture team is defining cross-company tooling, the point solutions across different cloud stacks and dev teams will rationalise.

With economic constraints increasing over the next 12-18 months, there will be even more pressure for CISOs to quantify the value of their toolsets and increase ROI on their security spend. Moving forward we can expect to see a shift in demand towards solutions that offer a broad set of cloud native security capabilities – particularly those that can be embedded into developer workflows – and a greater focus on measuring and reporting on the value they provide. With companies typically managing more than 75 tools, organisations will reduce the number of separate products in use for cloud native application protection by more than 20 percent this year on average, putting pressure on smaller point product providers.

Extending DevOps with GitOps. Another current hot trend in cloud native deployments is taking DevOps principles and applying them to infrastructure with the primary approach being GitOps. If this isn't already gaining traction within your organisation's teams, it most certainly will be at some point soon. GitOps use cases will span beyond continuous delivery (eg ArgoCD) to infrastructure, with the main tool being Crossplane. GitOps is making changes to any resource more observable through version control and thus, more secure.

We'll see more cloud native projects implementing GitOps tools such as Crossplane and ArgoCD, going from proof-of-concept use cases to large scale adoption across end-user companies. With GitOps becoming more mainstream, more resources are going to be defined as code in a structured way, allowing for higher scan coverage with security scanners.

SBOM will move front and centre. Shifting further left in the supply chain, the attention of nearly every CISO will be on the Software Bill of Materials, or SBOM, this year. New tools, languages, and frameworks that support rapid development at scale are being targeted by malicious actors who understand the catastrophic impact that attacks on the software supply chain can have. As threats to the software supply chain escalate, and with government regulations in the form of executive orders (EO 14028) mandating proper action to be taken, CISOs will be compelled to develop and deploy better strategies to secure this area of significant weakness. Going forward, expect to see fewer sophisticated attacks like SolarWinds and more attacks like those targeting Log4J, Spring4Shell, and OpenSSL which are widely used across code and production. These attacks will have a much larger potential blast radius, allowing hackers to impact (and potentially penetrate) many more organisations.

ATTACKERS WILL USE SECURITY TOOLS SUCH AS CODE SCANNING TO DETECT SECURITY ISSUES

To demonstrate the level of commitment to the executive order, it is highly likely that several companies found to be out of compliance with the order will find themselves facing fines or lose business with the government. While simply generating SBOMs is already becoming easily accessible today, the processes and tools around handling, signing and managing SBOMs, as well as applications of SBOMs in different use cases, will become more sophisticated and prevalent.

With so much change in the world of cloud native security, the old saying: "May you live in interesting times" comes to mind. This market demands that we stay ahead of the attackers, the technologies being adopted and the cultural/organisational changes that come along with these changes.

While many of the key predictions above are troubling, the good news is that leading cybersecurity companies are not only monitoring growing trends, but they are constantly developing sophisticated new technology and tactics to help organisations everywhere stay one step ahead in the ongoing game of high stakes cat-and-mouse. Whether you're a senior executive, security researcher, engineer or practitioner, taking these forecasts into account will help you to formulate, procure and implement a cyber security programme that helps protect your employees, customers and stakeholders as effectively as possible throughout 2023 and beyond ●

Rani Osnat is SVP Strategy at Aqua Security

One way organisations are likely to address the growing skills gap is by relying more on partner-delivered services

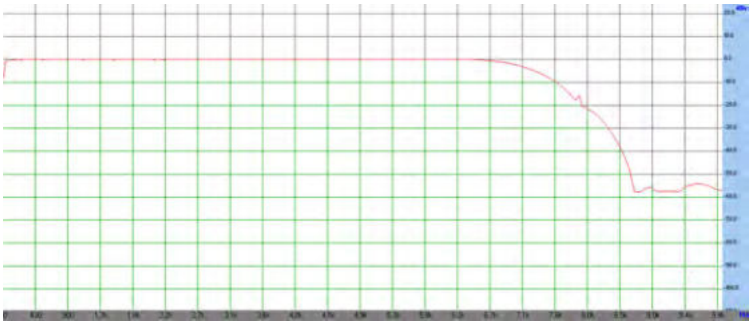
MGT SST-33

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).

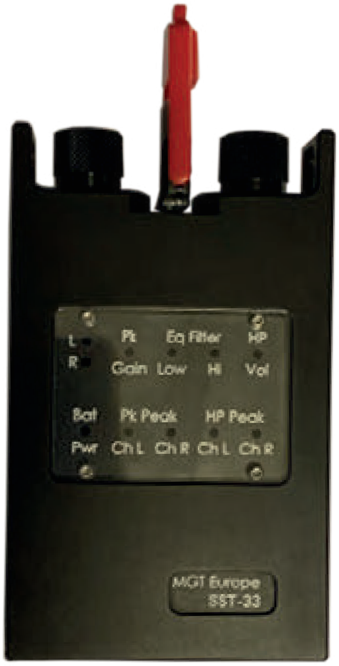
An incredible five-band equalisation technology gives you a crystal-clear audio experience.

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

Picture credit: Carolinebn8

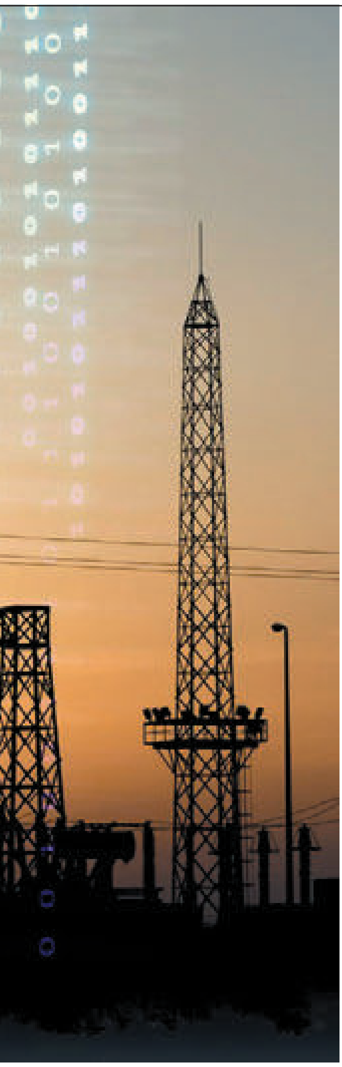
PROTECT YOUR WEAK SPOTS

Paul Baird *provides essential advice on the best way to link your operational and IT security together*

IT security is big business. Gartner predicts that spending on information security products and services will grow by 11.3 percent in 2023, reaching more than $188.3-billion globally. But while the approaches around IT devices, cloud computing services and IT networks have grown massively, there is an area that is lagging behind significantly – operational technology that companies use to run their physical infrastructure.

Operational Technology, or OT, includes all the IT systems used to manage areas like manufacturing systems, production lines and industrial processes. NIST defines OT as: "any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information". Typical applications include Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS).

In the past, OT networks were kept secure by running them on separate networks that were not connected to other systems, otherwise known as air gapping. However, this approach is no longer possible or desirable. Companies want data from their OT systems to make decisions in real time, rather than waiting on data exports or reports that are out of date as soon as they are compiled. This requires implementing systems using the Purdue Reference Model, where ICS systems and their programmable logic controllers (PLCs) run at level 1 and 2, then enterprise applications run separately at level 5 through a demilitarised



Industroyer was designed to affect ICS systems used in electrical substations and used as part of the conflict in Ukraine

zone, or DMZ. Each level should have security measures like firewalls between them to stop unauthorised traffic.

Having access to data faster helps businesses run more efficiently and trade more effectively, which is essential in today's modern global and interconnected economy. However, this means more connectivity is needed, and the air gapping model is not possible. According to the Dragos 2022 ICS/OT Cybersecurity Year In Review report, about half – 53 percent – of all ICS and OT systems now have external network connections. However, this opens up these systems to potential attack without the correct cyber security governance in place, which traditional IT networks have been following for years .

Because these systems were not connected to external or public networks, security could be overlooked when it would affect business operations. While modern IT systems developed to cope with real-time security issues and huge volumes of attacks, OT security approaches are less likely to have kept pace. According to Dragos, 80 percent of companies have little to no insight into their OT networks.

This is the basic requirement for all effective security planning – after all, you can't secure what you don't know about. While companies should be aware of everything attached to their OT networks, there is a difference between what you think you have in place and what actually is connected. On the IT side, common metrics used include tracking the percentage of assets that are managed versus unmanaged, and how up to date the software is on those assets. While 100 percent accuracy is the goal, 97 percent accuracy is seen as 'good'. Maintaining this level of accuracy as devices move in and out of the network or require patches is where the hard work takes place.

For OT assets, this level of accuracy should be the goal too. For very large assets, like physical plant machinery, you may think it is impossible to miss whether they are on or off the OT network. However, these systems will have multiple interconnected components. A lot of this OT equipment will also be directly connected to IT assets so that staff can interact or carry out management tasks too.

Checking which assets are connected can throw up some surprises, from the assets that you did not consider, that were connected without your knowledge or that had been left in place rather than decommissioned. Without that insight in the first place, you leave yourself open to potential attacks over time. Lacking this OT asset overview makes it impossible for you to truly say that you have a full picture of what is in place, how protected those assets are, and how you are prepared to keep security effective over time.

In order to improve OT security, you will have to bring your processes up to speed around areas like asset management, patching, network segmentation and threat intelligence analysis. These processes have developed quickly in the world of IT based on the volume and variety of attacks taking place.

There are more threats to OT systems than ever before. For example, security researchers have discovered approaches to move within OT networks and take advantage of issues in their implementations of networks that are equivalent to Purdue's Layer 1. ICS systems are targeted with specific malware to damage components. A good example of this is Industroyer, which was designed to affect ICS systems used in electrical substations and used as part of the conflict in Ukraine.

The malware landscape has evolved with new malware like INCONTROLLER aimed at ICS systems more generally through their programmable logic controllers and with a fully fledged framework for accessing devices, download and upload files, and exploit specific vulnerabilities in those devices. These customised malware developments point to more effort being put into attacks on OT networks, and work through misusing common standards like CODESYS to carry out functions as well as attacking existing security issues in order to work.

To prevent these kinds of attacks from succeeding, there are multiple steps to take. Implementing better access-control and authorisation mechanisms can help reduce the ability for bad actors to get onto the network in the first place, while restricting access can prevent mis-use of industry standards like CODESYS. Alongside this, teams need to improve their intrusion detection and analysis capabilities for their OT networks just as they have done for IT networks and cloud deployments. Adding real-time asset detection to the OT network like its IT counterpart will allow for more asset control so no unauthorised assets are left unattended.

GARTNER PREDICTS INFORMATION SECURITY PRODUCT SPENDING WILL GROW BY 11.3% IN 2023

To help in these processes, the Cybersecurity and Infrastructure Security Agency (CISA) has developed a Working Group on ICS to develop more best practices and share information on developments. Standards are improving as well – under the aegis of the International Electrotechnical Commission and the International Society for Automation, the IEC/ISA 62443 series of standards provides guidance on security best practices for OT environments. Specific standards have been developed for patch management in OT environments as well.

Alongside the wider industry development work taking place around standards, there are also changes that you can make internally. Consolidating IT and OT security management under one team can help. Today, many OT and IT teams within companies don't work together on a regular basis causing a lack of understanding on both sides – for example, the IT team would be hard-pressed to tell what is installed on the OT network and vice versa. This has to evolve so that security processes on the OT side can improve and teams can deliver that consistent approach to managing risk effectively. This can ensure that areas like patching get addressed across both IT and OT assets in the same way.

As an example, patching is one of the best approaches to preventing security issues. Applying patches quickly stops attackers from entering networks or gaining a foothold on devices which can then be leveraged to get into high value assets elsewhere. It ties into the overall picture that you can have of your overall IT and OT networks, and the various software packages and operating systems that exist across your estate. However, this is often where the problems come in for those companies running OT systems.

For companies that have to operate 24/7, simply finding the time to implement patches and updates is hard, if not impossible. If you have to take systems down to apply updates, this directly affects revenue for the period when updates are deployed, and there is a risk factor in bringing those systems back online successfully

▶

too. These risks can lead to patches being put off for later, relying on mitigating factors like air gapping to prevent attacks. However, with more OT systems getting connected, this is no longer as reliable as it once was. These OT assets represent high-value targets for attackers, whether these groups are motivated by financial gain or by nation state goals.

CUSTOMISED MALWARE DEVELOPMENTS POINT TO MORE EFFORT INTO OT NETWORK ATTACKS

In these circumstances, the role for security is not just about understanding best practices and applying them consistently. It involves educating the rest of the business – and particularly the leadership team – around how important a strong security programme across both IT and OT is. While many boards at companies now recognise the importance of security, they will have to understand the issues that might come up around stopping production systems to apply updates and the risks that arise if these activities don't take place. Would they rather have a controlled outage for a system update or an uncontrolled outage from a bad actor accessing internal systems?

Boards and business leaders are always told that their primary responsibility is to their shareholders. This normally gets translated into looking at revenue, so any activity that might affect the business in that regard will be discounted or overlooked. However, both boards and executive leadership teams are now more understanding of IT and security risks that can affect their companies around operations. Gartner has predicted that 50 percent of C-level executives will have performance requirements related to risk built into their employment contracts by 2026. This means that management teams have to consider the long-term impact from their decisions and how to deliver resilient and sustainable success over time, rather than just looking at the financial performance for that quarter.

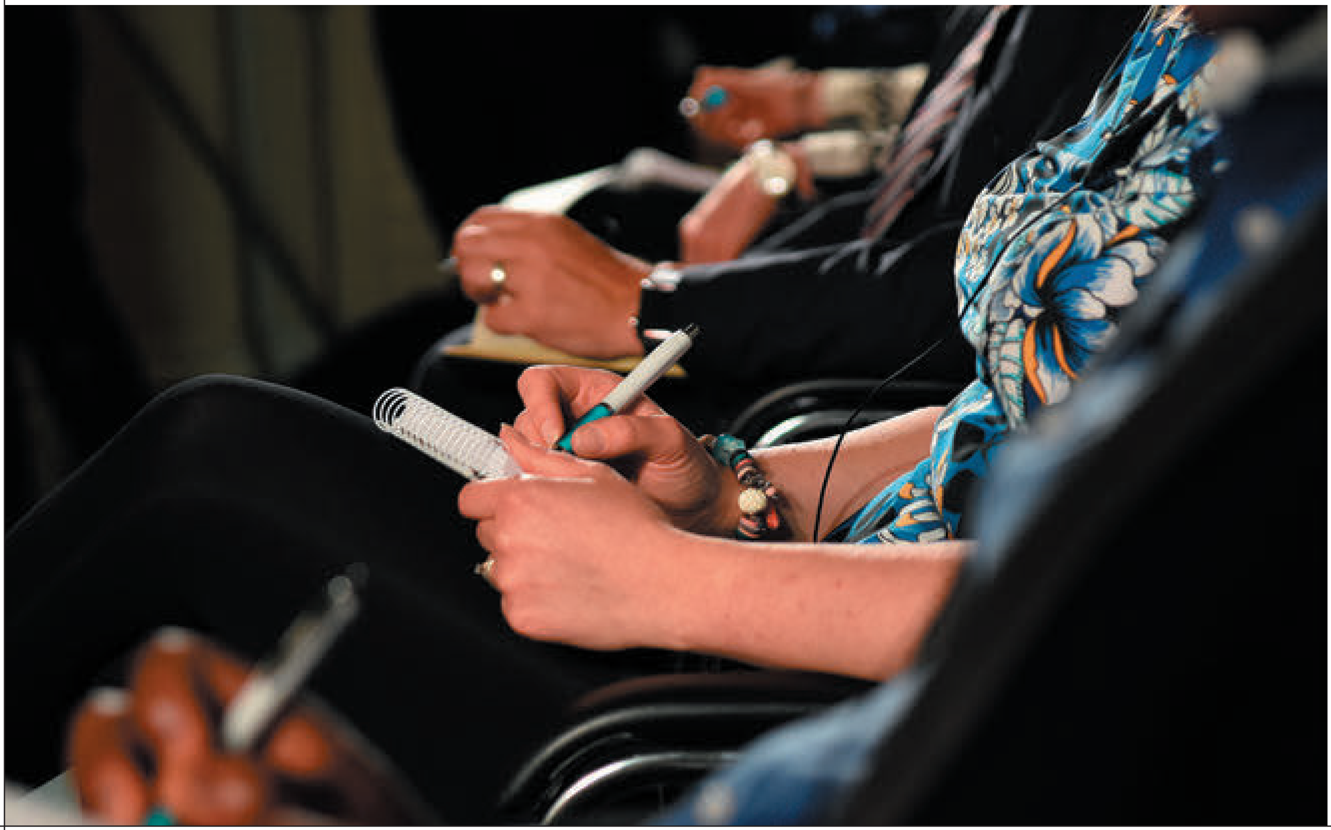
With more skin in the game for these teams, any initiatives that can protect against attack will get more consideration. To succeed here, you can develop metrics to help your board and leadership team understand the level of risk that the business faces alongside the impact from taking time out to carry out updates. This information will help executives measure short-term effects against the potential losses from attacks. There are plenty of examples of the impact of poor security for businesses and organisations that rely on their ICS and OT systems, from Colonial Pipeline and water treatment plants in 2021 through to attacks on companies in the automotive manufacturing, renewable energy sector, electronics manufacturing and oil and gas industries during 2022.

This can be used to provide real-world insight and context on the costs involved in attacks, compared with any losses in productivity. With this data, you can support your approach to maintaining and prioritising security issues and win backing for any planned downtime that is needed. Alternatively, you can make the business aware of what steps are needed and any mitigation measures and costs that are required to maintain services as they are.

In order to make security work more effectively across IT and OT and to protect your most sensitive assets, you have to structure your approach to processes like applying updates and make them part of that wider approach to managing risk. While there are new threats developing that specifically target ICS and OT systems, you can apply some of the best practices developed for IT security to prevent them from affecting your business operations. By building more understanding of risk for the business, you can also get the support you need to ensure that security is managed effectively ●

Paul Baird is a highly experienced and accomplished IT and cybersecurity professional with over 25 years of industry experience. He is the Chief Technical Security Officer for Qualys.

The role for security is not just about understanding best practices and applying them consistently, it also involves educating the rest of the business



Picture credit: Chuck Patch

INCIDENT BRIEF

Europe

9 April, Sheffield – UK
A murder investigation was launched after a man in his twenties was shot dead in a housing estate south of the city.

10 April, off the coast of Syracuse and Calabria – Italy
The Italian coastguard had to carry out two rescue operations involving fishing boats with a total of 1,200 passengers on board, as migrants attempting to cross the Mediterranean from north Africa surged over the weekend.

11 April, Derry –Northern Ireland
A small crowd threw petrol bombs and other missiles at a police Land Rover during a parade by dissident republicans in the Creggan area of the city on the eve of US President Joe Biden's visit to the country.

12 April, Italy and France
Hyundai disclosed a data breach impacting Italian and French car owners and those who booked a test drive, warning that hackers gained access to personal data.

15 April, Aintree – UK
More than 100 animal rights protesters were arrested after some invaded the Grand National course and forced the start of the horse race to be delayed by 15 minutes.

17 April, Sheffield – UK
The World Snooker Championship was disrupted by protesters after a Just Stop Oil activist climbed onto a snooker table and poured a packet of orange powder paint over it, forcing the match to be suspended.

Americas

5 April, Santa Catarina – Brazil
Four children were killed and at least five others injured after a 25-year-old man armed with a small axe attacked a pre-school in the southern state. The assailant later turned himself in.

5 April, Dulles – USA
A Youtube prankster was shot and wounded by a man at a mall in the Washington suburb after playing a joke on him.

10 April, Kentucky – USA
A Louisville bank employee armed with a rifle opened fire at his workplace, killing five people while livestreaming the attack on Instagram. Police killed the shooter in an exchange of gunfire.

12 April, Montreal – Canada
The Port of Halifax was hit with a denial of service cyberattack that shut down its public website but did not compromise internal data or interrupt operations.

14 April, Massachusetts – USA
The FBI arrested 21-year-old air national guardsman Jack Teixeira after he was suspected of being responsible for the leak of US classified defence documents revealing military secrets.

15 April, Dadeville – USA
Four people were killed and 28 injured in a shooting that erupted during a birthday party held inside a dance studio in the small Alabama town.

17 April, New York – USA
The FBI arrested two men accused of running a covert station for China's police force and using it as a base to track Chinese dissidents living in the US.

Asia

10 April, Jericho – Israel

Israeli troops fatally shot a 15-year-old Palestinian boy and wounded two others during an arrest operation in a West Bank refugee camp in the occupied territories.

13 April, Hokkaido – Japan

The launch of a North Korean ballistic missile caused confusion in Japan after a government-run alert system warned residents the projectile could fall on or close to the northern island.

15 April, Saikazaki – Japan

Japanese prime minister Fumio Kishida was safely evacuated after being targeted by an explosive device while visiting the port. A 24-year-old man was arrested at the scene.

16 April, Papua province – Indonesia

Separatist gunmen attacked Indonesian troops who were deployed to rescue a New Zealand pilot taken hostage by the rebels, leaving six dead and about 30 missing.

16 April, Hama – Syria

Suspected Islamic State fighters killed 26 people (16 civilians and at least 10 pro-regime fighters) foraging for truffles in an attack in the desert to the east of Hama.

16 April, Deir ez-Zor – Syria

Suspected IS jihadists carrying automatic rifles and riding on motorbikes killed four shepherds and stole sheep before fleeing.

16 April, Prayagraj – India

A former MP and his brother were killed in a dramatic shooting broadcast live on TV when three men fired more than 20 rounds of bullets at them from close range as they took questions from reporters outside a hospital in the northern Uttar Pradesh state.

17 April, Sultan Kudarat province – Philippines

A homemade bomb ripped through a bus in the south of the country, injuring at least eight people.

18 April, Diyala – Iraq

An Iraqi soldier and his wife were killed after a number of suspected Islamic State members attacked his house.

Africa

6 April, Kourakou and Tondobi – Burkina Faso

Forty four civilians were killed by "armed terrorist groups" in the two villages near the Niger border. Jihadists linked to al-Qaida and Islamic State were understood to be responsible.

12 April, Tunisia

At least 25 people died after a boat carrying migrants from sub-Saharan Africa towards Europe sank off the coast.

14 April, Douentza – Mali

A UN peacekeeper was seriously injured when his vehicle hit a mine placed by jihadists.

16 April, Zangon Kataf district – Nigeria

Gunmen killed 33 people in an attack on a farming village in the north-west of the country, opening fire on residents and torching homes as people tried to flee.

18 April, Amba – Mali

Two UN peacekeepers were wounded by a mine explosion near the village 75km west of Douentza.

18 April, Nara – Mali

The chief of staff of the country's military-dominated transition was among four people killed in an ambush near the Mauritanian border.

19 April, Sanaa – Yemen

At least 78 people died in the capital after a stampede was caused by Houthis shooting up into the air to try to control the crowds. A round hit an electrical wire, which caused it to explode – triggering panic on the ground.

20 April, across Africa

A campaign by China-linked hackers Daggerfly came to light, targeting telecommunication services providers across Africa. The attack began as far back as November 2022.

20 April, Kano – Nigeria

The Department of State Services intercepted guns concealed in a sack of yams reportedly on transit for a planned attack on one of the northern states. Two suspects were arrested.

NEWS

Europe

Visa delays as UK crime records office hit by cyber attack

The process of securing an overseas visa was thrown into chaos after the UK's criminal records office was hit with a two-month cyber security "incident" between 17 January and 21 March. ACRO, the national policing body which manages criminal record information and the exchange of records with other countries, was victim to a cyber security attack which affected it for two months. The agency warned while it had no conclusive proof of a data breach, there is the possibility that data sent to it by customers such as: "identification information and any criminal conviction data" was affected. The website's downtime has seen a significant backlog to get police certificates crucial for obtaining visas, meaning the applications have to be processed manually by email. An ACRO spokesperson revealed: "We take data security very seriously and as soon as we were made aware of this incident we took the customer portal offline. At this time we have no conclusive evidence that personal data has been affected by the cyber security incident." Applications for International Child Protection Certificates (ICPCs), used for UK nationals intending to work with children overseas, are also affected. The Information Commissioner's Office, which is the UK's data watchdog, said it was aware and that it was: "making enquiries".

Threefold increase in Med crossings this year says EU

Three times as many people sought to reach the EU across the Mediterranean in the first three months of 2023 compared with a year before, the bloc's border agency has said, as the UN's migration arm decried the deadliest first quarter since 2017. Overall, the EU agency, Frontex, reported 54,000 irregular crossings into the bloc via all routes in the first quarter of the year, up a fifth from 2022. "The central Mediterranean route accounts for more than half of all irregular border crossings into the EU," Frontex said, adding that nearly 28,000 people had arrived that way between the start of the year and the end of March – three times as many as in the same period in 2022. "Organised crime groups took advantage of better weather and political volatility in some countries of departure to try to smuggle as many migrants as possible across the central Mediterranean from Tunisia and Libya."

Labour glitch puts millions of UK voters' data at risk

The voting intentions of millions of Britons in local authority wards across the UK could have been at risk of misuse as a result of a glitch in the Labour party's main phone-banking system, according to *The Guardian* newspaper. Experts had warned that the sensitive data could potentially have been harvested via an automated programme and used for targeted election interference by campaign groups or even hostile states. More than half a million Labour party members have access to the Dialogue system, used by activists to make calls to the public for a variety of reasons, including to ascertain how they are planning to vote. However, the glitch meant that they could also access sensitive information including postcodes, which – when combined with voting intentions – would potentially have allowed them to generate a list of millions of people across Britain. The paper alerted Labour, which is believed to regularly monitor the programme to make sure it is not misused, to the potential breach, and the Dialogue system was taken down for 48 hours.

Greece purchases Spike missiles in €370-million deal

The Israeli Ministry of Defense has announced that the Hellenic Ministry of National Defence is acquiring Rafael's Spike missiles in an agreement valued at approximately €370-million. Director General of the Israel Ministry of Defense, Maj. Gen. (Res.) Eyal Zamir and the Greek Director of the General Directorate for Defence Investments and Armaments, Vice Admiral (rtd) Aristeidis Alexopulos signed a GTG agreement for the export of naval, air and land-based SPIKE missiles manufactured by Rafael Advanced Defense Systems Ltd. Minister Gallant explained: "This project joins a series of agreements between the State of Israel and the Hellenic Republic, and further emphasises the strong partnership between our countries and our defence establishments, as well as our mutual commitment to ensuring regional stability.

UK carries out first nationwide test of emergency alert system

At 3pm on Sunday 23 April, the UK carried out its first nationwide test of the emergency alert service. The test saw messages along with an alert and vibration appearing on mobile phones across the country, which automatically stopped after 10 seconds. The test has been in production for three years and is designed so that notifications can be sent to specific areas or across the UK. Pilots have previously taken place in East Suffolk and Reading. Following the tests, the government said it would be used in: "life-threatening emergencies", including extreme weather events like the wildfires and flooding seen last year, before adding that it is unlikely to be used during an active terror attack as the attackers would then receive a notification as well, but decisions would be taken when and as needed. Cabinet Office minister Oliver Dowden said the alert could one day: "be the sound that saves your life". Similar services are already being used in other countries including the US, Canada, the Netherlands, Greece and Japan.

NEWS

Americas

UN criticises Washington for eavesdropping

The United Nations has raised concerns with the United States over reports that it eavesdropped on the private conversations of the UN secretary general, António Guterres, and other senior officials. The criticism arose after leaked Pentagon files appeared to show Washington was closely monitoring conversations between the secretary general and his aides. *The Washington Post* reported in mid-April that the documents included embarrassing allegations that Guterres had expressed frustration with the Ukrainian president, Volodymyr Zelenskiy, and: “outrage” when his plans to visit a war-torn region of Ethiopia were rebuffed. The documents viewed by the *Post* suggest that Guterres was: “really pissed off” after an appearance with Zelenskiy in March. During the visit, Guterres was reportedly surprised Ukrainian officials photographed him at a public presentation of medals to uniformed soldiers and later shared the images in a way that suggested Guterres had congratulated Ukrainian military personnel. A spokesperson for Guterres said that he was: “not surprised” that he was allegedly spied on by the US. “Unfortunately, for various reasons, it allows such private conversations to be distorted and made public”.

Genetec helps Brazilian airport enhance security

Genetec has announced that its flagship unified security platform, Security Center, has been chosen by Brazil’s Hercílio Luz International Airport in Florianópolis to manage its physical security infrastructure and provide operational insights. The Genetec platform currently manages over 500 cameras and 210 doors to administrative and critical areas of the terminal, such as boarding, arrivals and customs. Because Genetec Security Center is based on an open platform, it can integrate a variety of operational systems and sophisticated analytics tools such as the ability to identify and track unaccompanied luggage and generate alerts so that appropriate security measures can be taken. Using the Security Center Plan Manager tool, the airport’s security teams can easily visualise and manage their security environments through an intuitive interface that displays the location of events and devices on geographical maps and floor plans. Cameras, doors, automatic license plate recognition units, intercoms, and other security devices can all be operated from the same interface.

Mexican cartel may be classified foreign terrorist organisation

US Secretary of State Antony Blinken stated at a March hearing that the department is considering designating the Gulf Cartel, responsible for the kidnapping and killing of four US citizens, as a foreign terrorist organisation (FTO). Once designated an FTO, anyone knowingly providing material support to the organisation within United States’ jurisdiction can face fines and imprisonment, according to the Department of Justice’s website. The proposed designation has also been getting support because of the DEA seizing more than 50 million fentanyl-laced pills and over 10,000 pounds of fentanyl powder, most of which came through the southern border. However, the designation could negatively impact US-Mexico relations with its sanctions, making it harder for the Mexican government and law enforcement agencies to cooperate with US forces. Although Blinken has stated that his department is considering the route, an official plan has yet to be announced.

Hurras al-Din leader specially designated global terrorist

The US Department of State has designated Sami Mahmud Mohammed al Uraydi as a Specially Designated Global Terrorist for his leadership role in Hurras al-Din, the armed insurgent group affiliated with al-Qaeda and fighting in the Syrian civil war. In addition, the Department’s Rewards for Justice is offering up to $5-million for information on the identification or location of al-Uraydi. All property and interests in property of al-Uraydi that are subject to US jurisdiction will be blocked and all US persons are prohibited from engaging in any transactions with him. The Department stated that any US or foreign citizens that engage in transactions with this individual may be exposed to sanctions risk, including under secondary sanctions authorities.

US Republicans push for asylum restrictions

In mid-April Republicans jump-started work on an immigration and border enforcement package that would remake immigration law to make it more difficult to apply for asylum and easier for the federal government to stop migrants from entering the US It combines proposals from a number of conservative hardliners into a single bill. The Republican legislative package aims to revive a number of policies either enacted or proposed under former President Trump that restricted asylum rules. They point out that illegal border crossings have increased under President Joe Biden and cast the current situation at the border as overrun and dangerous for both migrants seeking safety and border communities. Democrats on the House Judiciary panel swatted the bill as an extremist proposal that had no chance in the Democratic-held Senate. It has also been criticised by moderate Republicans who would be crucial to it passing the House, where Republicans have a slim 222-213 majority. “Republicans have chosen a narrow path that imposes extreme pain and hardship on the most vulnerable people while doing nothing to actually solve the problem,” said Rep. Jerry Nadler, the top Democrat on the House Judiciary Committee.

NEWS

Asia

New Zealand warning about aggressive foreign interference

New Zealand's intelligence bosses have warned of: "increasingly aggressive activity" in the country by people they believe are spies for foreign states. The country's annual report by the Security Intelligence Service (SIS) said unnamed states are making: "enduring and persistent" efforts to collect intelligence against the government, target those with access to sensitive information and interfere in all spheres of the country's public life. Agents from one foreign government have cultivated: "a range of relationships of significant concern", the report said. Though it did not name the countries accused, it's understood that New Zealand's strategic importance in the Pacific, as well as growing global awareness of its politics, has attracted the ire of authoritarian leaders such as China's Xi Jinping and Russia's Vladimir Putin. "Countries aggressively interfere in a liberal democracy because they're extremely insecure, very fragile authoritarian regimes," said Robert Patman, a professor at the University of Otago who specialises in international relations. The country's burgeoning influence has increased its strategic importance in the Pacific, he added. New Zealand has long been seen as a moderate voice in the contest for Pacific influence between China – its largest trading partner – and the US and Australia, its partners in the Five Eyes intelligence-sharing group of nations.

Bangladesh improves ranking in Global Terrorism Index

Bangladesh has become the second most improved country in terms of terrorism impact in South Asia as it has jumped down two places to 43rd of 163 countries, according to the latest edition of the Global Terrorism Index (GTI). Bangladesh received a score of 3.827 on the GTI index. The calculation of the score takes into account the deaths, incidents, hostages and injuries caused by terrorism weighted over a five-year period. Among other South Asian countries, Pakistan received a score of 8.16, India 7.173 while Nepal got 4.134. The South Asia region is home to two of the ten countries with the worst GTI scores; Afghanistan and Pakistan. Of the seven countries in the region, only Bhutan has a GTI score of zero, meaning that is has not recorded a terrorist attack in the past five years. Although Afghanistan improved in 2022, it remains the most terrorism-impacted country in 2022. Afghanistan recorded a 58 percent decline in deaths due to a drop in terrorism, from 1,499 to 633. The GTI report is produced by the Institute for Economics & Peace using data from Terrorism Tracker among other sources.

Japan's PM gives G7 security pledge after pipe bomb attack

Japan's prime minister, Fumio Kishida, has vowed to ensure the safety of politicians and officials attending this year's G7 meetings, days after he escaped unharmed after being targeted in a pipe bomb attack in mid-April. The attack provided an uncomfortable reminder of last summer's assassination of Shinzo Abe, and called into question security arrangements for senior politicians and other dignitaries. Japan's environment minister, Akihiro Nishimura, who hosted the G7 climate, energy and environment meeting in the northern city of Sapporo in mid-April, said security was noticeably tight. "My security has become even heavier this morning," he told reporters at his hotel. "It's so tight I think it is going to be difficult to go out into the city."

Iranian police to use cameras to identify "violators of hijab law"

Police in Iran have unveiled plans to use smart technology in public places to identify and penalise women who violate the country's strict Islamic dress code. A statement said police would: "take action to identify norm-breaking people by using tools and smart cameras in public places and thoroughfares". Police will then send "the proof and warning messages to the violators of the hijab law" to "inform them about the legal consequences of repeating this crime". The number of women in Iran defying the compulsory dress code has increased since a wave of protests after the death in custody of Mahsa Amini, for allegedly flouting it.

Jacinda Ardern to tackle online extremism in new role

Former New Zealand prime minister Jacinda Ardern has revealed that she will take on a new role working alongside international governments and social media companies to target extremism and terrorist content online. Prime minister Chris Hipkins announced in early April that he had appointed Ardern as special envoy for the Christchurch Call, a newly created position. The Christchurch Call was created by Ardern in the wake of the 15 March 2019 mosque shootings, which was livestreamed and broadcast on a number of social media platforms. "I … still feel a duty at a personal level to the community who are affected by this tragedy," Ardern said in an interview. "I knew that I would have the time to do it. And I certainly have the passion for it," she said. The Christchurch Call project calls on signatory nations to adopt and enforce laws that ban objectionable material, and set guidelines on how traditional media can report acts of terrorism without amplifying them. In her first substantial media appearances since stepping down as prime minister, Ardern said that she believed her resignation could lower the temperature in New Zealand's political discourse after deep divisions emerged around vaccination, the country's Covid response and her as a figure.

3DX-RAY

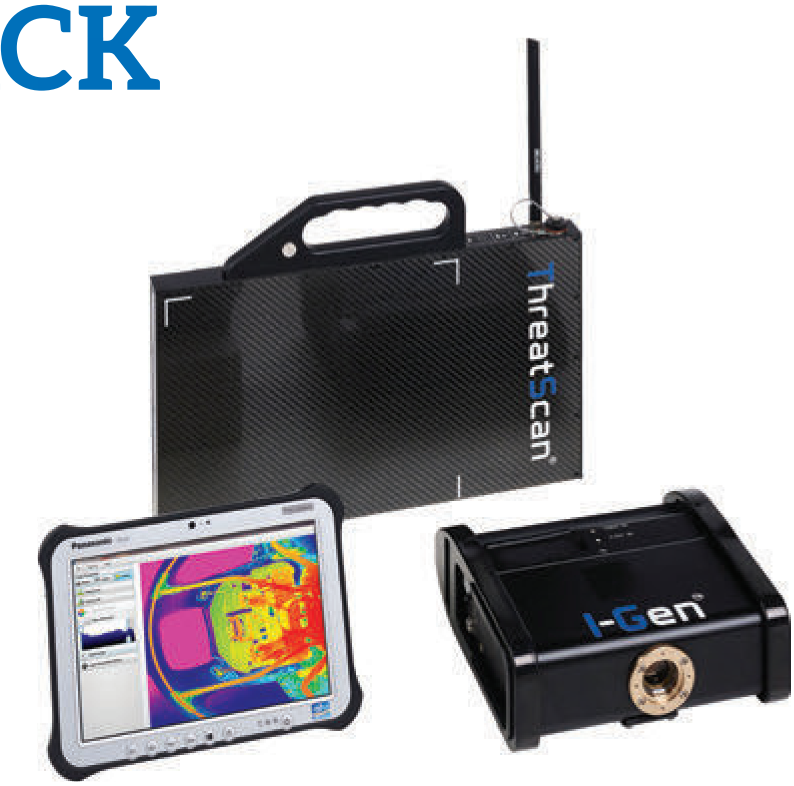
INSIGHT WHERE IT MATTERS

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^{TM}, 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

55,000 Nigerian Christians killed in the last 14 years

Islamic militants in Nigeria have killed almost 55,000 Christians in the last 14 years, according to a new report. Since the Boko Haram insurgency began in 2009, a total of 52,250 Christians have been murdered in the West African country, the report called Martyred Christians in Nigeria claims. It goes on to add that more than 1,000 Christians have already been murdered in Nigeria this year alone. A total of 30,000 killings have taken place under the rule of President Muhammadu Buhari, who has been often criticised for not doing enough to combat the growing insecurity in the country. Islamists have also murdered 34,000 moderate Muslims and burned 18,000 churches and 2,200 Christian schools. The report was published by the International Society for Civil Liberties and Rule of Law (Intersociety), a Nigerian-based research and investigative rights group, which has been monitoring and investigating domestic religious persecution since 2010. Researchers also recorded the kidnappings of at least 707 Christians, with more than 200 carried out in the Northern Nigerian Niger State.

China denies funding terrorists to access Nigerian minerals

The Chinese government has denied funding terrorist groups in parts of Nigeria to secure access to mineral reserves. A report in *The Times* newspaper, claimed that through bribes and illegal transactions: "Beijing could be indirectly funding terror in Africa's largest economy". The report alleged that some Chinese nationals who have worked informally as miners in Zamfara serve as runners for militant groups in the state and other parts of the north-west zone. Reacting in a statement in mid-April, the Chinese embassy in Nigeria said the report was based on: "unproven information", adding that the allegations: "were totally irresponsible and unethical". The embassy said China remains committed to addressing development and security-related issues in Nigeria: "The Chinese government, as well as the Chinese Embassy in Nigeria, have always encouraged and urged the Chinese companies and nationals to abide by the laws and regulations of Nigeria, and to implement the local rules and guidance on labour, environment, health and safety, *etc*, and would continue their efforts in this regard," the statement reads. The Chinese embassy added that it rejects "any intention or action that would smear our cooperation".

Gun battles erupt in Ethiopia as PM axes security force

Gun battles and mass protests have engulfed parts of Amhara, Ethiopia's second-biggest region, after a move to centralise the regional security forces of the country's 11 states. The federal government announced the policy in early April, in pursuit of building: "a strong centralised army". People from several towns in Amhara responded with protests, while some units of the region's security forces refused to disarm and clashed with the federal military. Two aid workers employed by Catholic Relief Services (CRS) were shot and killed while driving near the town of Kobo, while a US embassy alert reported: "serious exchanges of gunfire, involving heavy weapons" in "several areas of the region", including the towns of Woldia and Sekota. Shooting was also heard in Debre Birhan, Dessie, Debre Tabor and the regional capital, Bahir Dar, in recent days. Elsewhere, protesters burned tyres and blocked roads as banks and shops closed. The Amhara regional government has responded by imposing a curfew and blocking mobile internet services in some areas.

US to assist with fight back against jihadist attacks

The United States is preparing long-term assistance for Côte d'Ivoire, Benin and Togo following increased jihadist violence from the Sahel to coastal regions of West Africa. US officials stated that Western support was crucial to prevent the progression in the Sahel countries of mercenaries from the Russian private security company Wagner, deployed in particular in Mali. US State Department officials believe that the West African coastal areas could only be overrun by violence if there is an overflow from the north into the Sahelian strip. "Obviously we want to help governments that are more interested in a holistic approach and good governance to deal with problems in the north (of their territory), where resources are more limited," said Gregory LoGerfo, a senior department official in charge of the fight against terrorism.

South African companies face cybersecurity risks

A mere 19 percent of organisations in South Africa have the "mature" level of readiness needed to be resilient against today's modern cybersecurity risks, according to Cisco's first-ever Cybersecurity Readiness Index. The report highlights where businesses are doing well and where cybersecurity readiness gaps will widen if global business and security leaders don't take action. Other findings stated that 52 percent of companies fall into the Beginner (8 percent) or Formative (44 percent) stages. While organisations in South Africa are faring better than the global average (15 percent of companies in the Mature stage), the number is still very low given the risks. This readiness gap is telling, not least because 65 percent of respondents said they expect a cybersecurity incident to disrupt their business in the next 12 to 24 months. The cost of being unprepared can be substantial as 57 percent of respondents said they had a cybersecurity incident in the last 12 months, and 17 percent of those affected said it cost them at least $500,000.

DIARY DATES

2023 Conference and Exhibition planner

26-27 July India Homeland Security Expo 2023

New Delhi, India
Organiser: Nexgen Exhibition
Tel: +91-11-4153699info@
homelandsecurityexpo.in
www.homelandsecurityexpo.in

11-13 September GSX 2023

Dallas, Texas
Organiser: ASIS International Tel: +1 703.519.6200
Email: asis@asisonline.org
www.gsx.org

12-15 September DSEI 2023

Excel, London
Organiser: Clarion Defence. Tel: + 44 (0)330 912 1213
Email: enquiries@dsei.co.uk
www.dsei.co.uk

19-20 September International Security Expo 2023

Olympia, London
Organiser: Nineteen.Group Tel: +44 (0)20 8947 9177
Email: info@internationalsecurityexpo.com
www.internationalsecurityexpo.com

26-27 September DSEI 2023

Excel, London
Organiser: Clarion Defence. Tel: + 44 (0)330 912 1213
Email: enquiries@dsei.co.uk
www.dsei.co.uk

14-17 November Milipol Paris 2023

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

15-17 November Sicurezza 2023

Milan, Italy
Organiser: Fiera Milano S.p.A. Tel: +39 02 4997.7238
https://www.sicurezza.it

16-18 January Intersec 2024

Dubai, UAE
Organiser: Messe Frankfurt Exhibition
Tel: +971 4 3894 500
Email: intersec@uae.messefrankfurt.com
www.intersecexpo.com

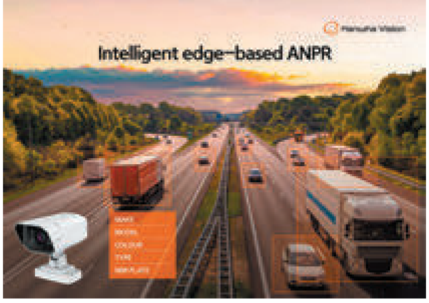
19-21 November MAST Australia 2024

Adelaide, Australia
Organiser: MAST. Tel: +44 7411 732978
Email:admin@mastconfex.org.
mastconfex.com

NEW TECHNOLOGY SHOWCASE

Hanwha Vision AI powered high-speed camera

Hanwha Vision has launched its TNO-7180RLP high-speed ANPR camera with 3-mega-pixel Global Shutter technology to detect number plates on vehicles moving at up to 200km/h (125mph) across two lanes of traffic. The camera features Hanwha's newly launched ROAD AI solution, which uses AI video analytics to identify the type, make, model and colour of detected vehicles, across 70 different automotive brands, 600 models and 10 colours. It comes with global shutter, to give greater accuracy and clarity of captured number plate images and a high frame rate of up to 60fps. Footage can be accessed through Wisenet WAVE, Wisenet SSM and other industry-leading video management software including Milestone and Genetec. The camera can also identify number plates and vehicle make/models. To get the best view of number plates, the TNO-7180RLP camera web viewer can provide suggestions to operators on camera set-up including the optimum vertical, roll, and horizontal angle. It also comes with adaptive IR with three separate IR illuminators (short/wide, medium/mid and long/tele). It illuminates up to 50M with a motorised varifocal lens and up to 18x optical zoom.



RT Unveils DOVE 10 Aerostat System for civilian market

RT LTA Systems Ltd. has unveiled DOVE 10, its new aerostat system for the civilian market. Leveraging the company's extensive experience, the new system was designed and built for civilian missions, based on the needs and capabilities of the civilian operator. The new system will be offered to potential civilian clients at a more cost-effective price. The system will incorporate cameras with relevant features based on customer's needs, and will be connected to a mobile launcher that was designed according to the European transportation regulation for the wide range of civilian security missions. Delivering affordable, high-quality information gathering and accurate target allocation, the DOVE 10 system provides 360° observation coverage and full digital recording of mission video and data. The system, which can carry any type of payload up to 6kg, enables continuous day and night operations up to 600 feet for up to 72 hours, with a wind limit of 30 knots.

Sectra mobile phone receives NATO SECRET approval

The NATO Military Committee has approved the latest version of the mobile encryption solution Sectra Tiger/S 7401 LTE from Sectra. This approval, which applies to the classification level NATO SECRET, certifies that Sectra Tiger/S securely supports NATO officials in the exchange of classified information. Sectra Tiger/S is a quantum-resilient mobile phone, allowing the user to share sensitive information up to and including the classification level NATO SECRET through encrypted speech, messaging and data transfer. The latest version includes support for all fixed and mobile 4G networks as well as improved robustness and sound quality. The new features provide improved availability, while also enhancing the user experience and potential use cases. Sectra Tiger/S is used by a large number of user organisations across many EU and NATO countries. Quantum computers will have the capability to perform certain types of calculations much more efficiently than today's computers.

Tracerco unveils personal electronic dosimeter range

Tracerco has announced the launch of its range of next-generation personal electronic dosimeters that will provide clients with a patented detection technology to enhance radiological safety performance. The PED2 range of dosimeters enable clients to effectively monitor, measure and manage radiation exposure. Providing a grab-and-go radiation dosimetry solution, Tracerco's unique PED2 technology will enable its clients to manage radiological safety performance in the most challenging of environments. Boasting numerous key technology features, PED2 offers: ruggedised hardware with a large, colour display so vital information is clear in all scenarios; simple, one-button operation with intuitive menus, imagery and event triggered instructions; reliable dose and dose rate measurement at both high and low levels; and is available in both intrinsically safe – certified for use in flammable atmospheres – and standard versions. The Tracerco PED2 is underpinned by a powerful, cloud-based dosimetry management software platform – DoseVision2 – enabling effective dose record keeping for compliance. This allows simple device configuration and management and provides flexibility to meet both individual and organisational needs.

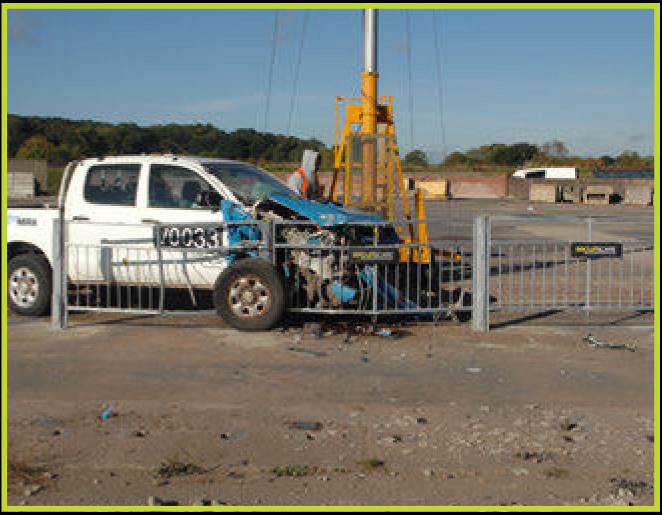
Crowdguard adds ARX Stopper! to its HVM range

Crowdguard has added the ARX Stopper! to the company's extensive range of hostile vehicle mitigation solutions, following a new partnership with ARX Security. The move adds to the range of temporary, semi-permanent and permanent HVM systems and perimeter protection solutions offered by Crowdguard as part of the company's 'plan, provide, protect' approach to event security and crowd safety management. As the events industry prepares for the introduction of Martyn's Law, the new addition to the Crowdguard range means that the company can offer even more flexibility in specifying appropriate and proportionate protection against vehicle-as-a-weapon attacks, aligned to identified threat, vulnerability and risk factors, along with operational requirements and budgets. Designed to stop vehicles and prevent them from progressing into safe zones or secure areas, ARX Stopper! can secure an average road width within 10 minutes, offering high levels of pedestrian permeability. Providing both a physical and visual security deterrent to protect against vehicle-as-a-weapon attacks and unauthorised vehicular access, the ARX Stopper! is effective at protecting events and publicly accessible solutions.

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

FOLLOW US ON:

securiSCAPE®
protecting people in public places®