www.intersec.co.uk

intersec

The Journal of International Security

April 2022

LOGISTICS AND SUPPORT

How enterprise asset management holds the key to success

Opening doors

Mobile credentials revolutionise access control

POLMIL®

ON-GROUND RELOCATABLE SECURITY FENCING

POLMIL® CPNI ASSESSED

POLMIL® PAS 68 RATED
(Test Reports on Request)

POLMIL® MOB ATTACK TESTED

POLMIL® TESTED AND PROVEN

POLMIL® HOT DIPPED GALVANISED FOR COASTAL ENVIRONMENTS

POLMIL® WITH WATER BALLAST

POLMIL® IS A DIVISION OF BLOK N MESH UK LIMITED

THE QUEEN'S AWARDS FOR ENTERPRISE: 2016

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

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

Tel: UK +44 (0) 151 545 3050

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

Tel: FR +33 (0) 3.20.02.00.28

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

Tel: Qatar +974 6652 1197

www.polmilfence.com

intersec
Volume 32 Issue 4
April 2022

Cover photograph: US Dept Defense

Editor
Jacob Charles

Principal Consultant Editor
Maj. Gen.
Julian Thompson CB OBE

Design & Production
jellymediauk.com

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

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

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

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

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

EDITORIAL COMMENT

For British Prime Minister Boris Johnson the indignities keep piling up. The last month alone has seen the ongoing shame surrounding Partygate as he was handed fines by the Metropolitan police (with more expected in the near future) for breaking his own laws during lockdown, while simultaneously pushing the frankly bizarre policy of sending immigrants captured from boats attempting to cross the channel to Rwanda. But rather than get bogged down in the financial and moral implications of dumping British problems in Africa, I'd instead like to concentrate on the Prime Minister's flimsy grasp of basic cyber security protocols after it came to light as we prepare to go to press that the United Arab Emirates has been accused of hacking into Downing Street mobile phones.

Like so many world leaders, it would appear that Johnson has fallen foul of Pegasus, the sophisticated software made by Israeli company the NSO Group that covertly takes control of a person's mobile phone. Using Pegasus, it's not only possible to access and remove any data on said handset, but also to turn it into a remote listening device. However, for this to be possible the software requires the phone number of the target. "But surely such delicate information is closely guarded by those at Number 10 in the know?" I hear you cry… Well, actually not. It turns out that Boris Johnson was forced to changed his mobile phone last spring after his number was published on a thinktank press release and then left online… for 15 years.

For its part, the NSO Group claims that such allegations are: "Wrong and misleading" and the company has denied any involvement in the incident, noting: "For technological, contractual and legal reasons, the described allegations are impossible and have no relation to NSO's products". The fact that the group is understood to have rewritten its software to prevent Pegasus from being allowed to target UK numbers in August 2020 provides further cause for concern.

The security breach came to light after a group of technology researchers based at Toronto University calling themselves Citizen Lab uncovered evidence of: "multiple suspected instances of Pegasus spyware infections" within official UK networks including Downing Street and the Foreign Office. The researcher utilised a series of digital forensic techniques developed over a number of years to conclude that the attack on Downing Street was: "associated with a Pegasus operator we link to the UAE", and took place on 7 July 2020. Quite why the UAE decided it wanted to target Downing Street on that day remains unclear, however what we do know is that the day before the British government announced a range of economic sanctions targeting 20 Saudi nationals accused of being involved in the murder of the journalist Jamal Khashoggi, plus individuals from Russia, Myanmar and North Korea. Coincidence, you decide...

The Foreign Office routinely refuses to pass comment on any such security incidents, but Citizen Lab alerted officials from the National Cyber Security Centre, which is understood to have tested several phones but was unable to locate which one was compromised.

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 2022

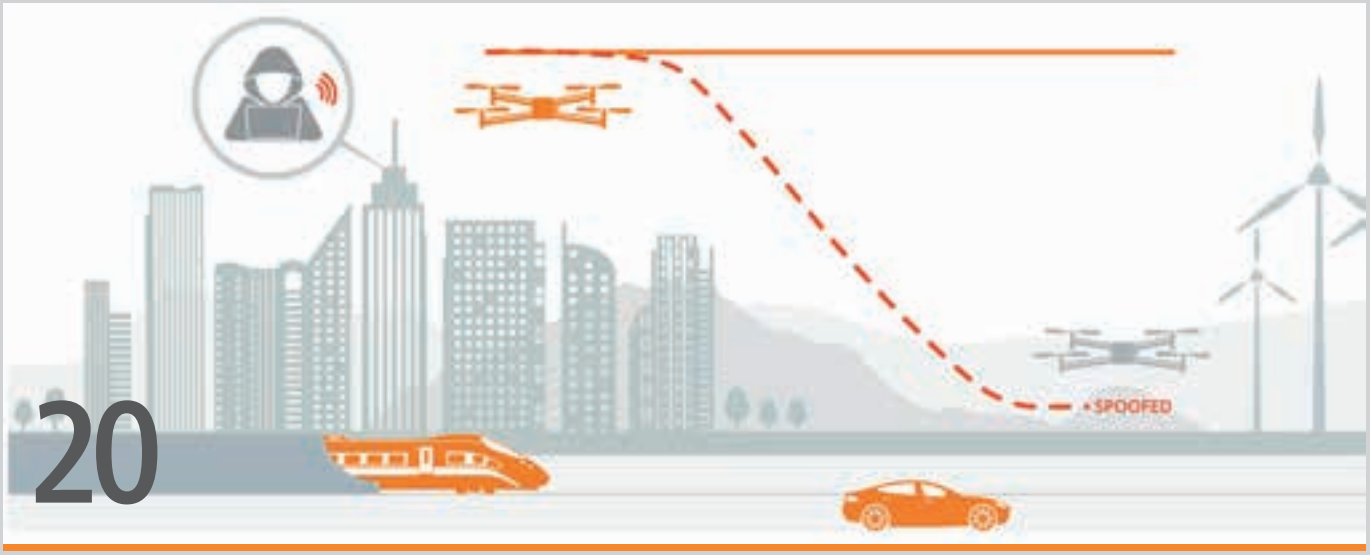
CONTENTS

April 2022 www.intersec.co.uk

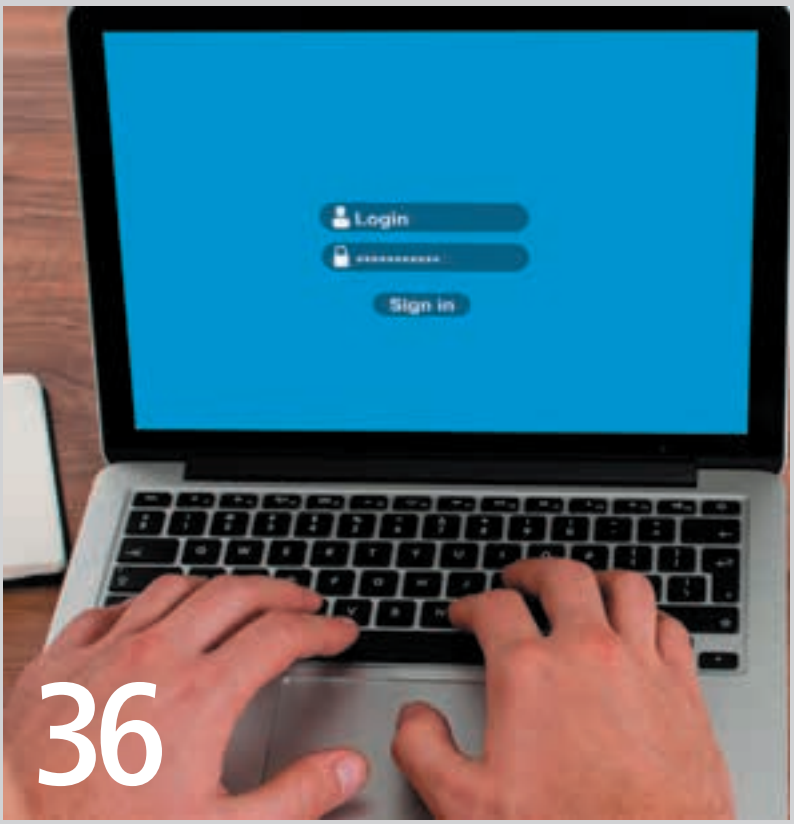
intersec

Features

Regulars


SPOOFED


COVID-19
VACCINATION
CERTIFICATE
VACCINATED


Login
Sign in

FRONTIER PITTS

PROTECTING YOUR WORLD

FRONTIER PITTS

WWW.FRONTIERPITTS.COM

+44 (0)1293 422800

IWA14 & LPS1175 HVM Terra Bifolding Gates

LPCB

Terra Bifold Gate
Certified to LPS1175: Issue 8 B3
Cert no C1059d/02
Certified to IWA14-1:2013
Rating V:7200[N2A]/48/90/0.2
Cert no C1059e-01

The First IWA14 certification by LPCB in the Red Book Live

& the full range of Security Rated Gates

IFSEC INTERNATIONAL | 17-19 MAY 2022 ExCeL LONDON

WE'RE EXHIBITING

AT THE #1 REUNION EVENT FOR THE GLOBAL SECURITY INDUSTRY

SEE US ON STAND IF5845

What price success for Putin?

Major General Julian Thompson CB OBE Principal Consultant Editor

As the tide of Russian success in Ukraine appears to be ebbing, for the moment at least, it is time to take stock. By the end of February 2022, it became clear that Russian losses have been heavy. The damage and loss figures compared with Russian losses in Afghanistan tell the story. After four days of fighting in Ukraine, the rate of Russian personnel losses was over 300 times that of Russian personnel losses in Afghanistan. Similarly, all types of aircraft have been lost by the Russians at a vastly greater rate than in Afghanistan. The most telling losses have been in tanks. In Afghanistan the Russians lost 147 tanks in nine years and nine months. After a mere four days fighting in Ukraine, Russian tank losses totalled 191. The Russians have lost armoured personnel carriers (APCs) six times faster than they did in Afghanistan.

The disparity in Russian losses between Afghanistan and Ukraine might be explained by the fact that the campaign in the former was counterinsurgency (COIN), whereas in Ukraine conventional war is being conducted with the full panoply of all types of equipment and weaponry. But surely the Russians have always been proficient at all-out, brutal, fighting deploying all arms in successive waves of head-on assaults supported by massive fire power, using a combination of armoured infantry and tanks in overwhelming numbers? Afghanistan was regarded by the Russian military as an aberration, an unwelcome one-off. When it ended one could imagine Russian senior officers saying thankfully: "Now we can get back to proper soldiering". There were many reports of the army undergoing radical reforms to restore its 'edge' and ethos after the Afghan campaign ended in such damning humiliation.

It would appear that the reforms have not gone far enough and were misdirected; for example, not increasing the ratio of regulars to conscripts. This has had an effect on training standards and hence morale. The morale of the Russian infantry is reported as being low. There have been cases of some infantry units surrendering when they discovered that they were expected to fight in Ukraine. Some units at staging areas have mutinied. Using conscripts to fight in a war of aggression as opposed to a war of national survival is potentially a source of trouble both politically and among the population – especially the mothers of the conscripts.

Possibly the biggest mistake made by Putin was starting the war apparently totally unaware of what he was demanding his army take on. He under estimated the ability of the Ukrainian army and over rated that of his own. The Russian army of today is not the Red army of the latter years of the Second World War. Furthermore, the Russian staffs seem to have failed to meet one of the most important rules when planning any warlike operation: getting the basics right, for example achieving the right ratio of troops to tasks and ensuring that the logistic system is in good order. The latter includes matters such as working out how much fuel is required and how it will be supplied including ensuring that there are enough fuel carriers, or bowsers to call them by their military name. These need to be mobile enough on bad, or even non-existent, roads to go forward to the 'customers' (the fighting units) to save them driving back and forth consuming fuel to top up fuel tanks. An additional drain on fuel is reported to be caused by Russian soldiers in stalled convoys keeping warm by running the engines – an indication of bad discipline and poor training.

Soviet forces lost 147 tanks in nine years and nine months in Afghanistan, while in just four days fighting in Ukraine they have lost 191

It is becoming apparent that the initial force deployed will be insufficient to conquer Ukraine, or even secure the initial objectives including Kyiv. This the Russians have conceded, leading to the question: what are they going to do about it? They have employed about 75 percent of their best troops getting this far. It would take years to raise, train and equip a new army. In the meanwhile, the job of holding the ring will fall to the existing conscript force while the Ukrainians, fighting in their own country and familiar with the terrain gain in confidence and expertise. If the war drags on, morale among soldiers and folks back home alike will deteriorate.

In this event, the big question that has hung over this war from the outset is: will the increasingly unstable Putin lose patience and use weapons of mass destruction (WMD), biological, chemical and nuclear? This behoves the West to think very hard and act extremely carefully to ensure that we do not provide him with an excuse to employ any of his large stock of WMD. Those members of the public who have demanded in the media for more action, for example NATO enforcing a no-fly zone over Ukraine, are either stupid or unaware (possibly both) that this would involve shooting down Russian aircraft and Ukrainian ones, and constitute an act of war. This would risk starting World War Three: no one would benefit, including the victim: the Ukraine.

Picture credit: US Dept. Defense

READY FOR ANYTHING

Matt Medley *reveals why 2022 is set to become the year of the Integrated Data Environment – providing the digital thread to underpin defence logistics and support*

While the utilisation of software by militaries to manage IT infrastructure and mission-critical weapons systems has been quickly advancing, analysis, data collection and execution is yet to make the same technological leap forward. The advancement of this critical data backbone is essential now and will form the basis of three key developments for defence support and logistics in 2022. It will take three forms: advanced servitisation of equipment support, the digitisation of the modern shipyard and further growth of unmanned systems on the battlefield.

There has been a lot of recent movement with military operators and their support providers modernising both supply chains and logistical processes, especially over the pandemic. The result has been the development and maturity of a lot of technologies such as augmented and virtual reality, artificial intelligence, AI, digital twins and 3D printing.

Yet processing the data gleaned from these new technologies is far from optimised. This trend is

Over 100 military organisations now have some form of drone capability

highlighted in a recent report by the US Government Accountability Office, which evidences the fact that the Department of Defense's own data collection and IT development has not kept up with developments in critical weapons systems used by the US military. The requirement is there and there are three key developments that will underpin the development of military logistics and support throughout 2022.

For equipment procurement and support, in recent years, the military has ascended the so-called 'transformational staircase' out of the scenario of simply buying and maintaining its own assets and equipment. The risk and availability linked with supporting an asset through its military lifecycle has increasingly involved industry assistance from OEMs or military in-service support providers. Now, performance-based logistics (PBL) is the widely accepted model for the procurement and support of military equipment. PBL strategies work effectively when applied to a specific asset or components, but these service-based agreements can even be taken a step further – what is deemed at IFS as "Total Asset Readiness" in relation to force-wide asset mobilisation and visibility.

This move towards a service-based approach for military asset support is underlined by recent research from Boston Consulting Group (BCG), which examined the cross-industry shifts towards delivering outcomes and pinpointed servitisation as: "the focus of creating and capturing value shifts from one-time sales to long-term partnerships". It's therefore no surprise that BCG report sees the defence sector prioritising the adoption of enterprise asset management (EAM) solutions in the next three years.

My prediction is for the next evolution of asset support to be focused on installing a constant and transparent framework across the entirety of a military force, connecting the military operator, OEM and in-service support providers. All separate reporting mechanisms and software systems can be consolidated within a single, all-encompassing solution, giving commanders planning operations a real-time image of each asset at their immediate disposal – tracking asset readiness within the context of the mission they need to complete.

You can see this already in progress with the US Navy's Naval Operational Business Logistics Enterprise (NOBLE) project. The programme will eliminate over 700 database/application servers and consolidate over 23 currently isolated application systems – ultimately aiming to improve asset readiness both on a shore and material basis. As part of a support agreement for the NOBLE project, Lockheed Martin and IFS will deliver an intelligent maintenance solution that will help power digital transformation of multiple legacy systems into a single, fully modernised and responsive logistics information system. The solution will support planning and executing maintenance, repair and overhaul of more than 3,000 Navy assets including aircraft, ships and land-based equipment.

My next prediction involves the digitisation of shipyards across the globe in the maritime and naval sectors. Much like the US Navy, shipbuilders, maintenance providers and other military operators are beginning to realise the value of digitising operations. ResearchAndMarkets data sees the digital shipbuilding sector poised for explosive growth – from $591.63 million in 2019 $2.7 billion by 2027, growing at a CAGR of 21.1 percent. This will be fuelled by rising adoption of digital twins in the shipbuilding industry and increasing use of new manufacturing technologies.

The largest geography for this growth is expected to be the Asia-Pacific as Indian and Chinese maritime presences are set to increase, however, the US too shall see high growth. This will culminate in a host of new vessels following the Navy's vision to create a 500-ship navy to protect America's global influence and interests. As such increased orders are being made, including Gerald R Ford carriers, a new block of Virginia fast-attack submarines, frigates, destroyers and the replacement to the Ohio ballistic missile submarine to continue the American at sea deterrent. Many of which, due to complexity and modular construction techniques will help boost US digital shipyard investment and growth. There are also parallels in the UK, in 2017 the UK Royal Navy announced project NELSON, specifically designed to deliver digital transformation across the service. Project NELSON highlighted the onset of the digital information revolution, its use in global marine warfare and how harnessing emerging commercial technologies would increase the Royal Navy's military capabilities.

INVESTING IN A VERSATILE DATA-DRIVEN BACKBONE FOR LAND, SEA AND AIR IS VITAL FOR SUCCESS

As such, digital oversight of maritime and naval assets begins not at sea, but right at the beginning of a ship's lifecycle – in the design process and at the manufacturing plant. This means shipbuilders themselves will have to prioritise digital advancements in the coming years. Take IFS customer, Australia's largest defence prime contractor, submarine and warship builder ASC, that recently announced a company-wide digital transformation programme. This will set the ground for the ASC digital shipyard transition – facilitating more streamlined processes, enhanced integration between systems and the expanded use of real-time data to drive optimised decision-making across the organisation. The ASC digital transformation programme will strengthen its enterprise resource planning system and introduce advanced technologies to enable its workforce and optimise its capabilities to support the sovereign sustainment of the Royal Australian Navy's Collins Class submarine fleet, now and into the future.

Any successful naval or maritime digital transformation programme means putting in place a full Integrated Data Environment (IDE) to ensure these barriers to executing a digital transformation project are removed, requiring close collaboration from military organisations, industry players and software providers.

But in order to build a naval or maritime digital transformation programme, most organisations need a digital overhaul. They need an enterprise-breadth system that can do more than simply manage essential MRO or supply chain processes and optimise scarce resources and assets in isolation. They require a software system that's agile enough to act on the increasing

data volume and complexity to deliver quantifiable operational benefits.

We're looking further forward in my final prediction, into the world of unmanned systems and drones – which are increasing in use across land, air and sea. There is a high degree of R&D investment planned in the unmanned systems sector going forward, drones in particular are increasingly being used in military operations. In fact, according to the Drone Databook, an in-depth survey of the military drone capabilities around the globe, over 100 military organisations now have some form of drone capability – and a rising number now have combat experience using unmanned systems. The proliferation of military drones will only grow with an expected rise in spending of $11.1 billion in 2020 to $14.3 billion by 2029.

DIGITAL OVERSIGHT OF NAVAL ASSETS BEGINS NOT AT SEA, BUT AT THE START OF A SHIP'S LIFECYCLE

In addition to removing human soldiers from harm, unmanned systems also bring about certain operational advantages. For instance, being unencumbered by life support systems (breathing apparatus, ejection seats) means 'uncrewed' aircraft can carry larger payloads with sensors for improved intelligence and reconnaissance or carry more fuel, which allows for longer trips.

The key near-term area of focus I see with the inevitable growth of unmanned systems space is the sustainment of these military assets. As this is something military organisations are still scoping out, consider these thoughts from Australian Defence Force Captain, Stephen Wardrop: "One of the key questions that must be answered is how the Army should structure maintenance support for UAS (Unmanned Aerial Systems) into the future. UAS maintenance is much more widely scoped than just the Air Vehicle (AV) – it encompasses the Ground Control Station, launch and recovery equipment including automatic take-off/landing systems, and all communications equipment involved in controlling the receiving data from the AV and its payload(s) during flight."

DIGITAL BACKBONE

The key to drone sustainment and support is very similar to the all-encompassing ecosystem I've outlined in my first two predictions, with critical importance being placed on having an end-to-end system to link all data sources and stakeholders. This means unmanned system design, manufacturing, supply chain and aftermarket services need a digital backbone capable to support sustainment now and into the future.

As military equipment and support becomes more technologically advanced, an ever-increasing data gap will continue to grow and need to be prioritised across the entire defence value chain to make sure it does not hinder and effect future military operations or deployments. Investing in a versatile and futureproofed data-driven backbone for land, sea and air is the key to future military logistical success for OEMs, in-service providers and operators alike ●

Matt Medley is Industry Director, Defence Manufacturing, IFS. In his current position Matt ensures IFS solutions meet the demanding needs of defence service and support organisations, defence manufacturers and defence operators and helps bring these solutions to market.

There is a high degree of R&D investment planned in the unmanned systems sector going forward

Picture credit: US Dept. Defense

THE QUEEN'S AWARDS FOR ENTERPRISE: INNOVATION 2020

eskan™

OFFER!

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

Increasing security. Reducing risk.

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

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

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

Picture credit: Marshalls Landscape Protection

THE FUTURE OF HVM

Roger Knight *examines the importance of getting the balance between protection and aesthetics right*

Unfortunately, it is a reality that Hostile Vehicle Mitigation (HVM) systems are required to protect the public against both accidental and intentional vehicle collisions. However, this does not need to be at the expense of the aesthetics of the public realm. Utilising modern street furniture solutions can enable urban planners to create visually appealing public landscapes while also delivering high levels of protection. Today, striking a balance between both aesthetics and protection is crucial for a number of reasons.

Globally, there has been a number of recent high-profile terror attacks involving the use of a vehicle as a weapon, with several occurring in the UK. During a four-month span in 2017, there were three vehicular attacks, which took place at London Bridge, Finsbury Park Mosque and Westminster Abbey. In each scenario, a vehicle was driven at high speeds into areas that were busy with pedestrians. Tragically, these attacks resulted in a number of innocent lives lost, with many more suffering severe injuries.

While HVM solutions are crucial for protecting against intentional attacks, accidental collisions also pose a threat

Owners and operators of publicly accessible spaces will soon be legally required to have protective HVM solutions in place

to the public. In the UK, between 2005 and 2015, there were 548 reported incidents in which pedestrians were killed in accidental vehicular collisions, while standing on pavements or verges. There were a number of reasons listed for why the drivers lost control of their vehicles, including dangerous driving, momentary lapses in concentration, inexperience and medical episodes.

The incorporation of HVM solutions into public spaces is key to keeping pedestrians safer and bringing these figures down. There is currently no legislative requirement for businesses and other organisations that operate in publicly accessible spaces to protect people from intentional or accidental vehicle collisions, however, that is soon to change.

Although it didn't involve a vehicle, the 2017 Manchester Arena terrorist attack – in which 22 people lost their lives and hundreds more were injured – has resulted in new legislation set to be introduced later this year. The 'Protect Duty' will establish a new obligation for venue owners and those responsible for public spaces to have the necessary measures in place to protect the public from potential threats. These requirements include: seeking counter-terrorism advice and undertaking appropriate training; carrying out a vulnerability assessment of their location or venue; and developing and implementing an effective plan to mitigate the risks and vulnerabilities identified. As such, owners and operators of publicly accessible spaces will soon be legally required to have the necessary protective HVM solutions in place.

While traditional HVM solutions are effective in the protection that they offer, their 'heavy-duty' appearance can often have a negative impact on visual aesthetics. This is particularly important to consider due to the high-street decline experienced in the UK in recent years. Overly fortified spaces can feel oppressive, using only bollards, barriers and fences to provide protection is a possible contributor to the UK's high street decline, more likely to put people off rather than encouraging them to visit public spaces.

In a document published by High Street Task Force, it was found that footfall in England has fallen year on year for the last decade, with a decline of 5 percent witnessed in just the last five years. Research conducted by Local Data Company identified that during the period of January 2016 and June 2021, the UK saw a net decline of 5,251 chain stores, with high streets suffering far more than retail parks.

Of course, this issue has been further exacerbated by the impact of the COVID-19 pandemic. Three separate lockdowns forced non-essential shops to close their doors overnight, with many unable to reopen. Additionally, the emergence and success of homeworking throughout the pandemic has seen many businesses continue with this system, resulting in far less footfall. Despite initiatives, such as the Government's 'levelling-up' agenda, being set up to combat this, the UK's retail recovery looks to be uncertain.

However, town centres that offer a greater number of amenities, as well as provide green spaces, are much more likely to encourage greater footfall and dwell time. Thankfully there is now a solution for urban planners, so that they can deliver protection, function and aesthetic design into the public realm.

The difficulty then for many urban planners, is delivering adequate protection while having minimal visual impact. For years, the focus has rightly been on protective qualities rather than visual appeal. Traditional HVM systems, such as bollards, fences, gates and walls, have been the favoured measures implemented to shield public spaces, including shopping centres, town plazas and sports stadia, from vehicular threats. Not only do these systems detract from the aesthetics of the spaces in which they reside, as easily recognisable protective systems, they can also evoke a sense of danger among pedestrians. For these reasons, traditional HVM products are not conducive to creating a welcoming environment, something desperately needed for high street recovery.

However, recent advancements in technology, design and manufacture have led to a rapid progression in protective street furniture solutions, with an extensive range of products now available for urban planners to consider. These street furniture solutions offer equal protection as their traditional counterparts, as well as several other advantages.

URBAN PLANNERS CAN NOW DELIVER PROTECTION, FUNCTION AND AESTHETIC DESIGN

The key benefit that crash-tested protective street furniture holds above traditional HVM systems, is the secondary functionality it offers in addition to its protective properties. This functionality can take many shapes, but ultimately enhances the public realm.

Amenities are a necessity in the public realm and help to make public spaces more visitor friendly. In essence, amenities provide a specific purpose that make public spaces easier to navigate and more accessible. Litter bins and bike rails are staples within public spaces. The former help with maintaining the appearance of the public realm while the latter encourage green travel and offer somewhere safe for those cycling to store their bikes.

By enabling visitors to identify where they are, or where they need to go, signage is possibly the most vital amenity to have within the public realm. As either directional signposts or maps of an area, signage can assist visitors in finding other amenities, such as transport links or public toilets.

Street lighting is fundamental to public spaces. The presence of adequate lighting has repeatedly been proven to contribute towards a feeling of safety when moving through a space at night. Additionally, environments that possess strong lighting report far less crime and antisocial behaviour than those environments that don't.

As previously discussed, the difficulties facing high street retailers and leisure facilities are ever increasing. Understanding these struggles, encouraging more footfall is a key ambition for urban planners. Fortunately, there are protective street furniture solutions that can assist in this endeavour.

The inclusion of tables and seating within public environments is vital for a number of reasons. Acting as a meeting point for friends, a rest stop (particularly important to the elderly and those with mobility restrictions), or just a place to enjoy lunch, are just

some of their uses. When positioned and coordinated appropriately, these products make public spaces more inviting and naturally encourage visitors to socialise and spend more time occupying the space in which they are situated, something desperately needed by business owners.

THE 'HEAVY-DUTY' LOOK OF HVM SOLUTIONS CAN HAVE A NEGATIVE IMPACT ON VISUAL AESTHETICS

There is also an extensive variety of protective street furniture products that can assist with enhancing the visual appeal of public spaces. The importance of greenery within the public realm, such as trees, plants and flowers, is sometimes overlooked. Small-scale greening additions can deliver health, social and environmental benefits, helping to create a more relaxed and inviting space. Planting trees, bushes, *etc*. directly into the ground can create a great amount of disruption and is not always a feasible option for urban planners. However, protective planters and shrubbery boxes provide a straightforward solution for introducing green elements into the public realm.

Introducing protective art, such as sculpture, into the public realm is another means for urban planners to visually enhance an environment. It is well accepted that public art contributes to community identity and improves the experience had by visitors. As such, using artwork to deliver protection against vehicular threats is a perfect way to keep pedestrians from harm without them knowing. Thanks to new innovations, all of the aforementioned products are available with protective properties, allowing urban planners to offer purpose and protection in one go.

It is sometimes assumed that, because protective street furniture solutions have been advanced in a relatively short period of time, that the range of designs and products available isn't that varied. This is absolutely not the case, with a vast number of materials – including metals and stone – that offer an exceptional amount of design freedom for urban planners to work with.

With such a wide choice of street furniture products available on the market, there is likely a solution to suit any given location – whether modern or historic. The aim for urban planners should be to blend-in street furniture seamlessly with its surroundings. This is particularly important for heritage sites, in order to maintain the integrity of the historic space while providing adequate protection.

While the need for HVM products is still as pertinent as ever, the demand to deliver adequate protection through less obvious means is growing. Protective street furniture solutions not only provide the same levels of security as their traditional counterparts, but also offer urban planners a range of additional functionality that benefit pedestrians, the public realm and the businesses that reside there. Street furniture makes it achievable to strike that all-important balance between protection, aesthetics and function ●

Roger Knight is Head of Product Development and Engineering for Marshalls Landscape Protection with 18 years' industry experience. Roger is also a board member of PSSA (Perimeter Security Solutions Association).

The difficulty for urban planners is delivering adequate protection with minimal visual impact

Picture credit: Marshalls Landscape Protection

NEW TTK TACTICAL TSCM KIT

Compact, Portable, Tactical

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

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

**Kit contents may vary*

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

lbs/kg

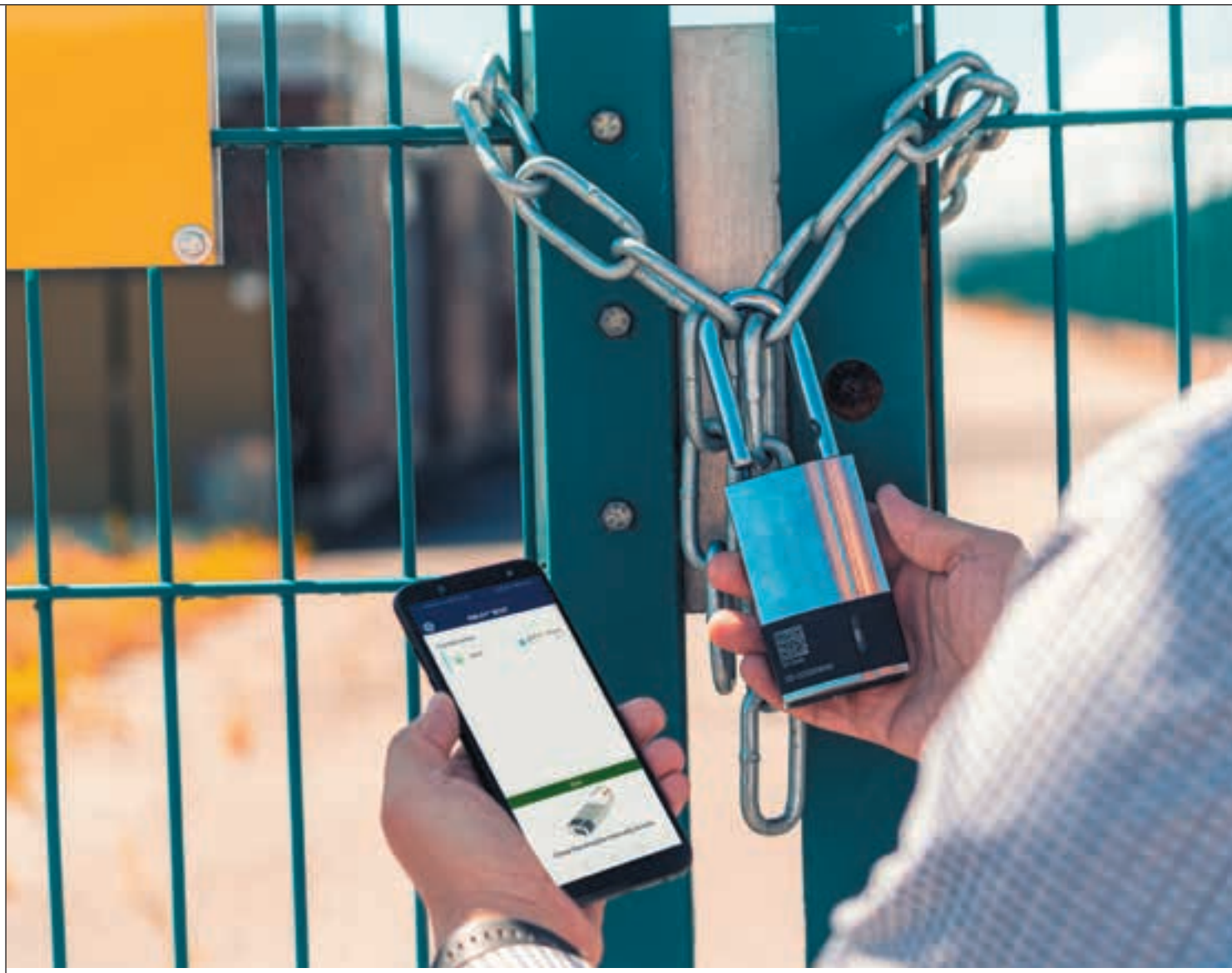
The TTK weighs approximately 25lbs/11.3kg - for easy transport.

MESA® hand-held Spectrum Analyzer

ANDRE® Broadband Detector

ORION® 2.4 HX
Non-Linear Junction Detector

CMA-100 Countermeasures Amplifier



Picture credit: ABLOY

OPENING DOORS

Steve Wintle *reports on mobile credentials and how they are revolutionising access control for a digital world*

The world is adopting new technologies at an astounding rate, and as a society we are becoming more reliant on digital devices. When it comes to managing access control, mobile credentials are similarly gaining popularity across a wide range of industries and applications.

A mobile credential is a digital access key that sits on a smart device such as a mobile phone. This replaces a traditional credential such as a key, fob or card. A mobile credential allows you to authenticate with your smartphone and use it as your key to gain access to a building, room or location.

Forecaster IHS Markit predicts over 120-million mobile credentials will be downloaded in 2023 – an enormous increase in contrast to the 4.1-million downloads recorded back in 2018. Furthermore, research finds that over two-thirds of organisations will have adopted mobile access control to some extent within the last two years.

Here, we explore some of the reasons for this increased demand for mobile credentials, including the need for flexibility and convenience, an easy way to manage access rights with instant delivery and increased security and sustainability. We also consider some of the barriers to implementation of mobile credentials and recommend which type of applications are most likely to have the most success.

The global mobile workforce – a group of employees not bound by a central physical location but connected by various types of mobile technology – is expected to reach 1.87-billion workers by 2022, and this new way of working brings a requirement for adaptable and flexible access control.

Mobile credentials offer a way to enable access permission changes in real time for contractors travelling between remote sites

Mobile credentials offer convenience as there is no need for a separate RFID credential when you open secure doors and openings with a device you already carry. They are also flexible, as facility managers can amend, issue or cancel credentials from anywhere and building users always have their access rights up to date. Plus, as mobile credentials are updated wirelessly and remotely, it reduces face-to-face contact for both staff and visitors as they do not need to collect a card or fob. This improves efficiency too, as employees waste less time collecting or amending access credentials in person and visitors get instant temporary access as and when they require it.

Passwords are no longer enough in the cyber world as they can be shared, stolen and copied – just like some keys. The only way to overcome this issue is to verify the identity of each individual that is attempting to gain access.

Identity verification has become standard practise in society, for example in the realm of online shopping. Consumers are familiar with having to enter a verification code when using a shopping app to confirm their identity, and this offers peace of mind that their details are secure.

Mobile credentials utilise on-device passwords and biometrics such as fingerprint, voice and facial recognition, to keep unauthorised people from accessing the key stored on the smartphone. They are also seen as a more secure way to manage access because people are less likely to lose a mobile phone in comparison with a key card or fob. In fact, 17.3 percent of people lose at least one card or fob annually, compromising security and creating a cost for the organisation to replace.

If a key or fob goes missing, it can easily be used by anyone that discovers it. In direct contrast, if a smartphone is mislaid, the level of security on the device makes it incredibly difficult for anyone to access it, let alone get far enough to utilise the credential that's stored on it. Also, people are more likely to notice if they have lost a mobile than if they misplace a key or fob. This means the organisation can be promptly alerted to the missing smartphone, so they can revoke access instantly using the credential's management software.

When using traditional credentials such as a key, card or fob, there is a time and efficiency cost in distribution, whether that is via delivery or handing them out physically. By using mobile credentials, organisations can reduce these costs and increase operational efficiency, making them an attractive option from a sustainability perspective.

It's a more efficient system, and employees and contractors waste less time collecting or amending access credentials in person and visitors get instant temporary access when they need it. Eliminating the need for key cards and fobs – and the constant replacement of lost cards and fobs – additionally reduces plastic usage.

For organisations with contractors travelling between disparate and remote sites mobile credentials offer a way to enable access permission changes in real time. This not only reduces CO2 emissions from wasted trips and going back and forth to collect and return keys, but improves operational efficiencies, saving time and money while improving management and tracking of who accessed what and when.

With all these advantages, it's easy to forget there is still a management requirement for a mobile key. Mobile credentials can be convenient and flexible, and in some cases practical for external applications, but it's not the credential that's providing the actual security. The credential provides confirmation that the holder can access a site or open a lock – and that's where practicality issues come into question.

The credential is seen as the answer to no physical keys, which has been a challenge for most businesses to manage. The reality is, a mobile credential still needs to be managed and this seems to be a factor that's not clearly understood. Without question, integration of mobile technologies with Permit To Work ticketing and individuals' training and competencies management systems can make the management of controlling access easier and at the same time enforce compliance. Automation will allow the process to happen routinely, providing a seamless and efficient operation and enabling the exceptions to be scrutinised. But beyond the credential, little thought is often applied to what it could operate.

A CREDENTIAL CARRIED OR SENT TO A MOBILE PHONE IS IDEAL FOR SHARED SITE ACCESS

Mobile credentials require a lock that has an inbuilt reader, a power source and something to operate it – turn the lock – a function traditionally performed by a key. At present, a large thumb turn is usually provided on the outside, acting as the reader and a means of operating the lock.

This design leaves the lock vulnerable for a vandal or organised criminal to attack and disable, causing disruption and potential easy access for the perpetrator. This in turn also causes an issue for the authorised engineer or contractor that needs to gain access.

If it's a high security door, how do you protect the thumb turn with a high security shroud against hammer or drilling attacks simulated by the LPS standards? In this instance, a key is actually a far more practical means of securing and controlling access to critical assets.

Among other concerns raised by integrators around the implementation of mobile credentials for access control, phone battery life is listed as a potential issue. A phone with no power left means no access can be granted by the user, which can impact a business in terms of lost working hours. Plus, in areas where there is no internet signal, the credentials on the smartphone can not be updated if access needs granting on arrival. This is where unpowered fobs or cards, or a physical key are seen as a more reliable source of credential.

Keyless solutions aren't perfect for every application, and keys are still a very practical solution especially for legacy estates with traditional

locking mechanisms. The practicality of keyless solutions working in dirty harsh remote conditions is completely different from warm dry office applications. In addition, there will be certain environments where mobile phone usage is simply not permitted – nuclear sites, for example – making mobile credentials an unsuitable solution.

Although there can be barriers to success with mobile credentials, there are instances where the technology can thrive and come into its own. A credential carried or sent to a mobile phone is ideal for shared site access, for example.

IF A KEY GOES MISSING, IT CAN EASILY BE USED BY WHOEVER FINDS IT – A LOCKED PHONE CAN'T

This is ideal for the ad hoc visitor needing to access once, rather than on a regular basis. Abloy Beat is a prime example of this, offering the ability to use a phone to open and lock a padlock. The padlock is physically secure, and access is managed via an app controlled by the same piece of mapping software as Protec2 Cliq.

With this in mind, CIPE Manager from Abloy UK brings together a keyless solution, an electromechanical key solution and a mechanical key solution that can secure all applications with easy management – with all three elements working together. It is tailored to give a comprehensive situational overview and increase operational efficiency in critical infrastructure access management. The solution allows organisations to manage all their keys, locks and access rights from any location, with a user-friendly, cloud-based management system.

CIPE Manager connects with every locking solution in Abloy's digital portfolio, including the Beat keyless Bluetooth padlock, the electromechanical Protec2 Cliq system, as well as Abloy's high-security mechanical master key systems. Beat combines three main components: a digital key, a mobile application and a heavy-duty Bluetooth padlock, all managed with the visual CIPE Manager user interface.

Alternatively, ASSA Abloy's Incedo Business Mobile Keys are a new type of credential that offers secure mobile access, simplified management and user convenience and efficiency.

Incedo Business provides a user-friendly interface for managing your access control platform. You have a choice of system management options – Lite or Cloud – to administer Incedo-enabled hardware in a way that best suits your business' needs.

It's clear to see why mobile credentials are gaining in popularity and while there is certainly a place for this kind of technology, there still remains a requirement for alternative solutions in certain environments. Ultimately, the key is still a very practical credential and shouldn't be written off as a less robust access solution just yet.

By choosing a solution such as CIPE Manager, organisations can get the best of both worlds and adapt their credentials for different applications in relation to their requirements. This offers the ability to have a mix of physical keys, cylinders and padlocks, as well as digital technology using mobile credentials where it is most appropriate, all integrated into one platform for convenient, controlled and secure access management ●

Steve Wintle is Head of Critical Infrastructure at Abloy UK

Mobile credentials use on-device passwords and biometrics such as fingerprint, voice and facial recognition to keep unauthorised people from accessing the key stored on the smartphone

Picture credit: ABLOY

Kestrel TSCM ® Professional Software

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

Signals Intelligence Support System ™

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

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

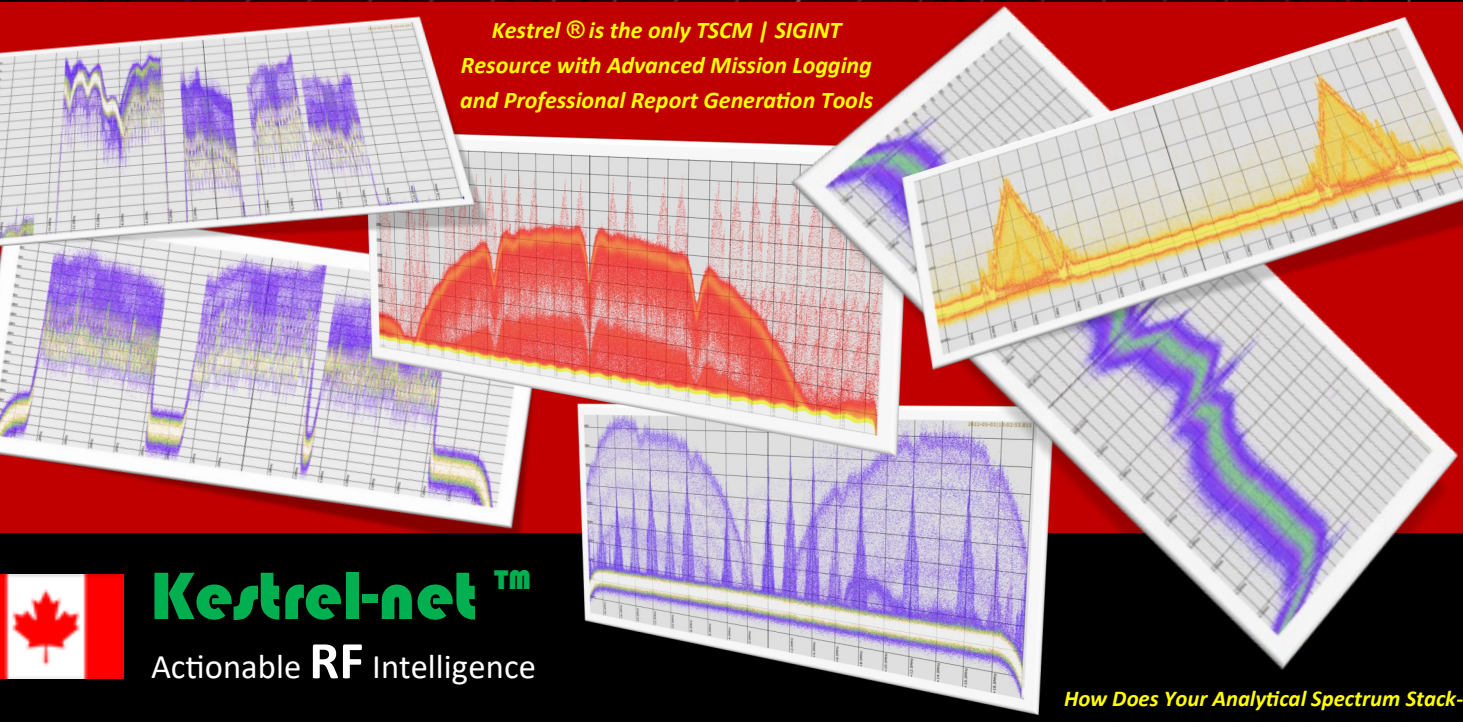
Kestrel TSCM ® Professional Software

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

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

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

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



Kestrel-net ™

Actionable **RF** Intelligence

How Does Your Analytical Spectrum Stack-

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

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

JAMMING AND SPOOFING

Maria Simsky *explains why secure GPS receivers are crucial for GNSS/INS systems*

With the growth of automation and robotisation in many industries, from agriculture and delivery drones to self-driving cars, the demand for accurate and affordable navigation is on the rise. When selecting a GPS/GNSS (Global positioning system/ Global Navigation Satellite System) receiver it is crucial to understand vulnerabilities of these sensors and the effect they could have on the navigation system. For robots and autonomous devices availability is key to ensuring continuous and reliable service. Safety also needs to be considered for robots and drones operating close to people. GNSS jamming or spoofing needs to be detected and flagged immediately so that other sensors can take over.

Most autonomous navigation technologies include an Inertial Navigation System (INS), which consists of a GNSS receiver and an Inertial Measurement Unit (IMU) sensor. While the GNSS receiver provides absolute positioning in terms of geographic global coordinates, the IMU measures heading, pitch and roll angles, which give orientation information of a moving system.

Spoofing is a real threat to GNSS-based INS systems, which is mitigated most effectively by incorporating security mechanisms into all system sub-components. However, since spoofing takes place on the level of the GNSS signal, a number of sophisticated methods can be employed within the receiver to detect and mitigate spoofing. Receivers designed with security and robustness in mind are resilient to GNSS vulnerabilities such as jamming and spoofing. Taking advantage of such robust GNSS technology is also cost effective, allowing companies to focus their development on sensor fusion and navigation.

Jamming is a kind of radio interference, which overpowers weak GNSS signals, causing accuracy degradation and possibly even loss of positioning. Unintentional jamming sources include radio amateurs, maritime and aeronautical radiolocation systems as well as electronic devices located close to the GNSS receiver. There are also intentional jamming devices called jammers, which are sometimes found on board of vehicles that trying to avoid paying any road tolls.

Spoofing is an intelligent form of interference, which makes the receiver believe it is at a false location. It appeared in the news in a spectacular experiment where a Tesla car was 'misled' to take an exit from a highway rather than following the highway as it was supposed to. Consequently, both jamming and spoofing can have an adverse effect on INS systems, which make use of GNSS positioning.

While GNSS provides absolute positioning, the IMU measures relative movement, which is subject to cumulative error called drift and needs regular recalibration. In a GNSS/INS system both sensors are fused in such a way that the GNSS provides regular IMU calibration and the IMU provides angles and extrapolation or smoothing of GNSS.

Picture credits: Septentrio

Maria Simsky is Technical Content Writer at Septentrio.

Jamming, which results in loss of positioning, means that the GNSS receiver can no longer be used as part of the INS solution. This can lead to longer INS initialisation times or a switch to dead-reckoning mode (IMU solution only), where the position starts to drift. Jamming can also result in measurement outliers, which impact GNSS/INS algorithms (ie deep or tight coupling). However, it is spoofing which poses the highest security risk for GNSS/INS systems. During a spoofing attack an INS solution can be hijacked if the spoofer uses small increments in positioning, which can go undetected by common anti-spoofing methods.

Using sensors other than GNSS such as an IMU or odometry can help flag spoofing by detecting inconsistencies between GNSS and the other sensors. While such sensors help reduce spoofing risks, they are not sufficient to provide full protection because they only output relative positioning – which is subject to drift. For example, GNSS/INS systems can have a drift of a metre or more when visibility of GNSS satellites is lost for longer periods. Spoofers can exploit this to hijack positioning gradually, in increments comparable with the expected drift.

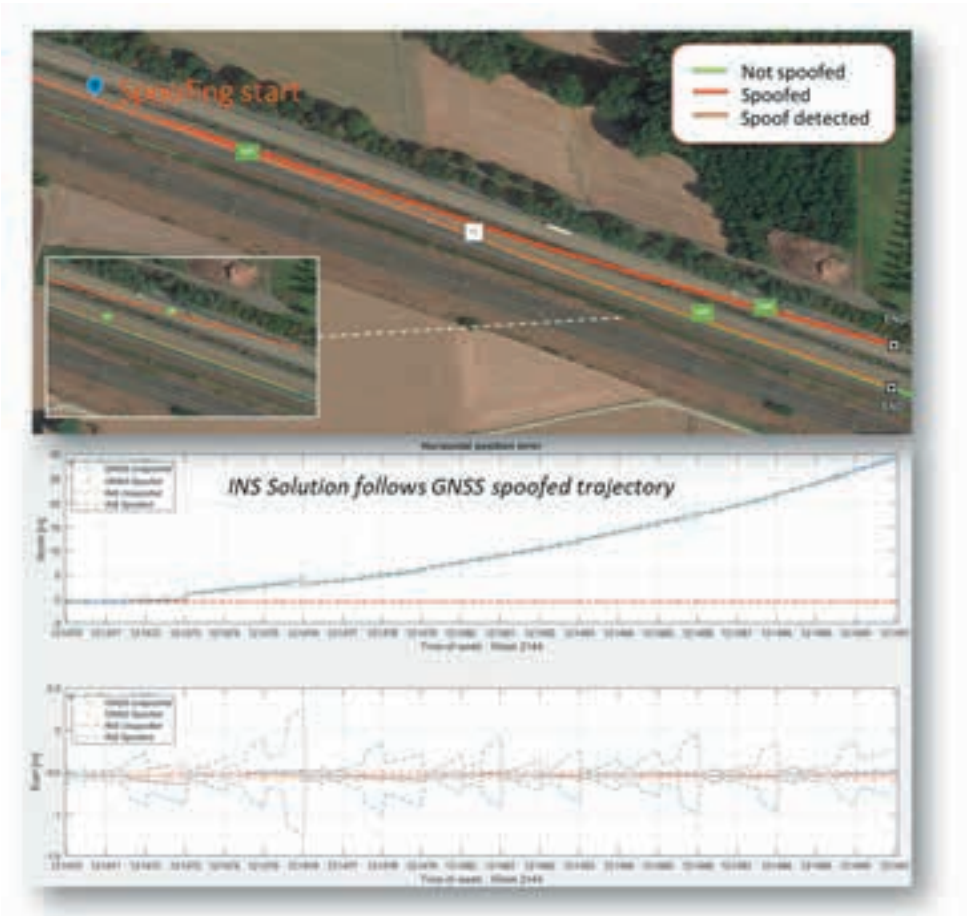
If the spoofing attack keeps positioning increments within the allowed thresholds, which are set to allow for drift, it will go undetected by such a mechanism. That is why, for best system protection and anti-spoofing resilience should be built into several system components on both GNSS and INS levels.

The vulnerability of this common INS spoofing check is shown in the road test below, where the spoofing attack is executed gradually, in small increments perpendicular to the direction of motion. The magnitude of these spoofed increments is small enough to be below the drift threshold of the IMU, which makes it acceptable for the INS system shown by the red line. The system shown by the orange line, with anti-spoofing built into the GNSS receiver, rejects the spoofed signal and switches to dead-reckoning, which allows it to stay on the right track. If the spoofing attack is limited to a few signals, then the GNSS receiver can even avoid the attack by discarding these spoofed signals from its positioning solution.

As shown in the road test, an INS system will be more resilient if the GNSS receiver can indicate spoofing or, even better, if it can mitigate spoofing by itself. Thus, when integrating GNSS/INS solutions it remains crucial to understand the role of protection mechanisms in GNSS and to select a GNSS receiver with strong internal anti-spoofing defence system or a warning system

A GNSS receiver which implements security measures in its design will include spoofing resilience at various levels. Both the GNSS receiver as well as the INS have their own mechanisms for spoofing protection, however the best resilience comes from the combination of detection and mitigation mechanisms working together on component level.

As in any field affiliated with security, continuous improvement is needed to maintain effective anti-spoofing and anti-jamming mechanisms. GNSS manufacturers have a responsibility to strive for the most effective security methods in view of the increasing threats, which confront today's GNSS users. By investing in GNSS receivers with built-in resilience, integrators can leave the security maintenance to the GNSS manufacturer and focus their efforts on core business and sensor fusion. In fact, the concepts discussed in this article are valid not only for GNSS/INS systems but for any sensor fusion system, which includes a GNSS receiver. Smart GNSS technology protects receivers from jamming and spoofing at the core level, ensuring safe and reliable system operation ●



The red line is a GNSS/INS system with a common spoofing check that has been hijacked by a spoofer using small positioning increments. The orange line is a system that stays on track due to spoofing being detected.

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

SCANNA

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

SCANSILC EOD - DR X-RAY

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

SCANX SCOUT - CR X-RAY

A must in every bomb truck!

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

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

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

XR150

XR200

XRS-3

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

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

COVID-19 FRAUDSTERS

Dr Gareth Owenson *reports on the rise of fake vaccine cards on the Dark Web*

While political and social debate caused by the proposed use of COVID Vaccine Cards (CVCs) raged across traditional and social media platforms, underground networks of cybercriminals found new ways to exploit public fear and unease for financial and strategic gain.

This article reviews some key findings from Searchlight Security's report, which investigates the dark web demand for CVCs by analysing listings on popular Dark Web markets. The result of analysis of over 3-million listings from more than 70 Dark Web markets posted between January 2020 and January 2022 help shape recommendations for policy makers and researchers on how to investigate and defend against this emerging threat from the digital underground.

The volume of CVC listings has increased significantly in the past year, with the total number growing on average by 186 percent per month. The lion's share of these originate from a single Dark Web marketplace, suggesting that despite international policing efforts, cybercriminal activity is flourishing. The most common price of a Dark Web CVC listing is $500 (£370). With a very low production cost for these cards, profit margins remain high for cybercriminals, with specific sellers beginning to corner the market from an early stage and set themselves up as key distributors.

Meanwhile, technological improvement to the way governments verify vaccination status, such as QR codes, hasn't stopped criminals from attempting to imitate them. Dark Web vendors were quick to respond, with digitised CVC listings appearing on markets as early as mid-2021. Some even claim to have sourced legitimate QR codes from medical staff, though this can't be independently verified.

When analysing cybercriminal activity, it is worth assessing what factors could be driving the actors involved,

28 PERCENT OF DARK WEB CVC LISTINGS DIRECT BUYERS TO ENCRYPTED MESSAGING PLATFORMS LIKE WHATSAPP

besides the obvious financial incentives. Many Dark Web vendors selling CVCs previously or subsequently advertised unrelated listings covering a wide range of goods and services, including illegal substances and stolen credentials. This supports the notion that existing sellers pivoted to meet the new demand for CVCs, as was the case for earlier pandemic-related products such as masks and purported COVID-19 treatments.

That said, recently there has been an increase in Dark Web market vendors exclusively focused on the sale of CVCs. Perhaps unsurprisingly, nearly 1 in 5 (19 percent) of these listings contain anti-vaccine keywords or rhetoric in their product descriptions. This suggests that many of the users purchasing these illegal cards are doing so for political reasons. Some of the most commonly occurring keywords are "government", "forced", "control" or "autonomy". It could also be the case that some Dark Web sellers with anti-government or anti-vax beliefs decided to begin selling CVCs because it aligned with their worldview, though it seems more likely the use of anti-vax rhetoric is a marketing tactic to entice a particularly active demographic on Dark Web forums and cash in on a politically divided culture.

Furthermore, these marketplaces are not exclusive to the Dark Web. More than a quarter (28 percent) of Dark Web CVC listings direct buyers to Telegram, Wickr or other encrypted messaging platforms such as WhatsApp. Despite the privacy implications of these encrypted messaging services, platforms such as Telegram have come under fire for a range of other ethical issues. The prevalence of Dark Web vendors instructing prospective buyers to communicate via alternative platforms presents authorities with an additional channel through which to monitor and gather intelligence on those suspected of distributing fraudulent CVCs.

The sale of CVCs on the Dark Web is a growing niche which poses a significant threat to public health efforts at curbing the pandemic; it wouldn't take many fraudulent cards to undermine a nation's COVID-19 measures.

Furthermore, with several vendors claiming to have privileged access or connections to official healthcare databases, organisations must stay vigilant to outsider and insider cyberthreats by applying strict information and supply chain security measures and conducting regular audits for potentially breached information or intellectual property.

Increasing the sophistication of vaccination verification systems, such as introducing digitised CVCs, is insufficient alone to prevent fraudulent versions. That said, devising solutions that are more expensive to counterfeit could disincentivise illicit production by reducing profit margins.

Unlike other Dark Web ventures such as drug trafficking, cybercriminals may view selling CVCs as relatively low-risk in terms of legal consequences. Authorities would do well to dispel this assumption by devoting more time and resources to CVC investigations, setting high penalties for manufacturing, distribution, and use of such products, and highly publicising these efforts as a deterrent ●

Dr Gareth Owenson, CTO and co-founder, Searchlight Security is an internationally recognised and published Dark Web scientist. Gareth co-founded Searchlight Security and now oversees the research and development, software engineering and niche cyber capabilities.

2022

EUROSATORY

13-17 JUNE 2022 / PARIS

THE GLOBAL DEFENCE & SECURITY EXHIBITION

SECURITY, A MAJOR COMPONENT OF THE EXHIBITION

86
Official Delegations
from security domain

725
exhibitors
with security activities

14
conferences
dedicated to security topics

30+
media partners
from this domain

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

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

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

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

GICAT

www.eurosatory.com

COGES EVENTS

It’s An Open & Shut Case.

Introducing the new TTK Tactical TSCM Kit

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

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

*Kit contents vary

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

IPS

THE HALLMARK OF SECURITY

Looking For The Most Extensive Mobile Sweep Kit Available?

RISK AND COMPLIANCE

Simon Whitburn *explores the current Legal GRC landscape and reveals how failing to plan for legal GRC could increase risk levels for your organisation*

Governance risk and compliance (GRC) is a vital cog in the machine of any successful business today. Its rise can be attributed to the mid-Noughties when several accounting scandals at various organisations – including Enron, Worldcom, and Tyco – led to the introduction of the Sarbanes-Oxley (SOX) Act in the United States. Launched to protect investors from fraudulent accounting activities, SOX required businesses to provide more comprehensive financial disclosures, thus sending shockwaves around the world.

New regulations were instated and older ones were made more stringent, resulting in a state of greater consciousness where companies of all shapes and sizes began to place the concepts of risk, controls, corporate governance and business efficiencies under the microscope.

From audit and risk to policy and business continuity, many of these efforts were initially dedicated to IT and financial operations. Yet as firms began to reap the rewards of more logical procedures, their same methods were expanded to manage the entire organisation's governance, risk and compliance frameworks.

It is vital that CLOs and their legal teams secure a more holistic view of organisational data

Here, GRC as we know it today was born, the landscape having evolved tremendously in the near-two decades since. And now GRC has relevancy across a variety of functions – none less so than legal. Indeed, legal leaders of today are faced with much of the orchestration and interconnections of legal operations, digital forensics, data privacy and cybersecurity compliance. This is no small undertaking – managing the complexity of the business from a legal perspective, all the while keeping continuous business and legal change in sync is a significant challenge.

To do so effectively, a comprehensive, integrated strategy, process, information and technology architecture is required to meet legal commitments, address legal uncertainty and manage risk in a way that is efficient, effective and agile. Indeed, this makes legal departments the perfect candidates to tap into the many benefits that governance, risk management and compliance can bring to the table.

Before we consider the benefits of legal GRC any further, it is worth considering what the landscape looks like in 2022. Like many critical business functions, corporate legal departments have experienced significant transformation since the pandemic first hit two years ago. And in many cases, it's been a transformation borne out of necessity.

Between the rapid digitalisation of operations, increasing data volumes and growing adoption of new technologies, further complexity and therefore expenses have been added to legal processes. Meanwhile, expectations have risen as company executives demand a granular understanding of how their legal teams operate – whether activities are efficient, technologies are cost effective and how processes might be enhanced. At the same time, a variety of economic, political, social and legal changes have bombarded organisations, resulting in the exponential growth of regulatory requirements and legal obligations.

Be it privacy regulations, compliance, data inventory or discovery operations, legal departments have more on their plates today than ever before – and a change in the winds is not expected anytime soon.

The findings from ACC and Exterro's 2022 Chief Legal Officers (CLOs) Survey reflect these growing pressures, highlighting sentiment among legal professionals globally. Based on the responses of 861 CLOs spanning 20 industries and more than 40 countries, the survey shows that many expect industry-specific regulations and data protection privacy rules to present significant hurdles. 66 percent see the former as the most significant source of legal difficulties, while 55 percent also cite data protection rules as a cause for concern.

Given the survey also reveals that six in 10 expect an increase in privacy-related regulatory enforcement in the coming year, and not a single respondent feels that the volume of regulatory enforcement in the privacy area would ease, the challenges are clear to see. It is for these reasons that demand for legal GRC solutions is rising as industry professionals seek more effective and efficient ways of operating.

This aligns with spending habits, the ACC report showing that the majority of legal departments have upped their expenditure in relation to regulation compliance in the past year, with much of this focused on new technologies. Additionally, firms are also hiring data privacy specialists as well as implementing data privacy policies and providing staff with education and training.

Such investments are driven by a growing need to mitigate litigation and compliance threats that include cyberattacks, data breaches, regulatory fines and other civil sanctions. Without an integrated strategy and process, information and technology architecture that is capable of governing legal affairs effectively and efficiently, the discovery, understanding and management of data in a defensible way is extremely difficult, resulting in a host of risks and exposures.

Indeed, with such a broad spectrum of economic, political, social, legal and regulatory challenges, those who don't have the visibility and means to address them leave themselves at risk of being punished in multiple areas.

CORPORATE LEGAL DEPARTMENTS HAVE SEEN HUGE TRANSFORMATION SINCE THE PANDEMIC

Equally, while many companies today understand the role of GRC in managing risk and compliance across the organisation, some fail to see its role in coordinating legal activities alongside compliance, IT, finance, HR and other critical areas, creating a series of siloed strategies that result in conflicting methods and potential gaps and/or unnecessary overlap.

A lack of a coordinated strategy will almost always result in a failure to deliver critical insights and context, making it near impossible to link legal risks management with wider business goals, from decision-making through to performance analysis.

Thankfully, there are simple, yet effective ways in which organisations can put a successful, optimised legal GRC strategy in place that minimises corporate risk and helps to drive improved business outcomes. As we have discussed, CLOs have taken on a growing variety of responsibilities. According to ACC, four in five are responsible for compliance, 47 percent manage privacy and 40 percent manage risk. If we compare this with 2021's report, CLOs now have more responsibility in 18 of 21 different corporate functions. There are challenges that come with this, from added pressures to growing complexity. Yet it equally provides opportunity.

To operate in such a capacity successfully, CLOs and their legal teams will have to secure a more holistic view of organisational data – something that can be achieved with the adoption of a unified technology platform, rather than stitching the big picture together from multiple point solutions.

Much has been said of difficulties of solution saturation. Here, legal GRC presents the opportunity to achieve greater solution consolidation and departmental interoperability.

Equally, by taking on a greater role, legal GRC professionals will have the opportunity to address some critical risk areas such as cybersecurity, regulation and compliance, and data privacy. Indeed,

more responsibilities in business-critical priorities translates into more work, but it will provide CLOs with the opportunity to adopt new technologies capable of improving efficiencies and streamlining processes.

Indeed, the ACC study reveals that 56 percent of CLOs implemented new technology last year to assist with privacy – technologies that will also serve to optimise workflows and provide the foundations from which even more intelligent solutions, such as automated processes, can be adopted.

COMPLIANCE THREATS INCLUDE CYBERATTACKS, DATA BREACHES AND REGULATORY FINES

Looking ahead, seven in 10 CLOs said that they wanted to invest in contract management technology, while others are also considering document management technology solutions (39 percent), workflow tools (33 percent), collaboration and knowledge management tools (25 percent), and matter management technology (25 percent).

In terms of greater interdepartmental coordination, there is equally significant cause for optimism. In fact, the report further reveals that 84 percent of participants expect greater collaboration between legal and other business divisions, such as compliance and privacy, as a result of increased regulations and the need to optimise internal processes.

Between CLOs settling into their expanded roles, the need for greater technology adoption to make these roles sustainable and scalable, and a push for interdepartmental collaboration to unlock wider business benefits, legal GRC will prove to be a busy yet buoyant arena in 2022. The move towards unified, consolidated legal GRC practices is continuing, if not accelerating, presenting a number of opportunities to legal professionals and organisations alike. Such integrated approaches will be critical – today, they should be viewed as business imperatives in helping firms better manage the risk exposure and compliance concerns that are increasingly threatening to exhaust resources.

Indeed, those organisations that are able to develop parameters that clearly define the breadth and depth of their legal GRC management strategy and process requirements will be perfectly placed to operate effectively and efficiently while supporting wider business objectives. Once this has been achieved, the appropriate technologies can be selected to support legal teams in their endeavours, cultivating the perfect toolset to help manage increasingly complex operational requirements.

The market is not short of solutions. A new class of enterprise software designed to seamlessly orchestrate those tasks and activities required to implement processes and address these business challenges is continually evolving, with many of its modules dedicated to legal GRC. By achieving excellence in each of these areas, legal GRC frameworks can become agile, flexible and scalable, capable of meeting not just the requirements of today, but also those of tomorrow ●

Simon Whitburn is General Manager and Vice President of International Business at Exterro.

Be it privacy regulations, compliance, data inventory or discovery operations, legal departments have more on their plates today than ever before

Sentinel

A TSCM BREAKTHROUGH

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

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

Designed for TSCM Engineers by TSCM Engineers.

FEATURES

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

SENTINEL KIT INCLUDES

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

For further details: contact@qccglobal.com

LONDON

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

SINGAPORE

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

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

LESSONS LEARNED

Bernard Montel *looks back at 2021: a year of turbulence in cyber risk – from lockdown to Log4Shell*

Last year ended as abruptly as it started: January saw a surprise lockdown and return to remote working, bringing added risks in cybersecurity. Businesses readopted with fervour the cloud systems that had seen them through 2020, while still working to comprehend and address the risks this move had introduced. And, after a year of patching problems, 105 zero-day vulnerabilities and a surge in ransomware attacks, Christmas provided no respite as Log4Shell shook the industry.

Over the year, over 40-billion records were exposed by attacks and from that over 1.8-billion files, documents or emails fell victim to bad actors. Attackers throughout 2021 did not limit themselves to digital destruction, and several crossed the chasm from the digital world to the physical. These infrastructure attacks rattled the UK public's faith in fuel and food supply chains, mostly using fairly ordinary means to wreak extraordinary damage.

The global threat and vulnerability landscapes were analysed in a recent, retrospective report by Tenable, aiming to guide business responses and navigation of the modern attack surface. The report calls to attention key evolutions in the attack surface that can put businesses at risk, including supply chains, misconfigurations of systems like Active Directory and interconnection across operational technology (OT) devices, among many others. As businesses across the world revisit their security approach in the wake of last year's constant threat of a breach or attack, multitasking will be key and a forward-thinking, holistic approach to their software supply chain could save them from further exploitation from bad actors.

The brief return to pandemic business operations offered bad actors another opportunity to exploit remote workers, thanks to the adoption of cloud solutions and software leading to an increasingly complex ecosystem. These changes, showing more and more permanence even as the COVID-19 threat subsides, are transforming how we define "the perimeter" when it comes to network boundaries. But exciting as this evolution in digital transformation may be, allowing for a better work/life balance and more diverse, international employee teams, an increase in this hybrid set-up inevitably led to a riskier software supply chain; an element effectively exploited by attackers in 2021. Think back to ransomware attacks and breaches like SolarWinds and Kaseya, which made use of the age-old tactic of daisy chaining vulnerabilities in order to expedite breaches; these are core examples of the insecurity in software supply chains that businesses must rectify.

As mentioned previously, January 2021 saw the industry deal with the aftermath of the SolarWinds attack as nation-state actors, Nobelium, compromised an update protocol for the SolarWinds Orion platform to distribute

Ransomware operators inflicted the most damage in 2021 to the healthcare sector, accounting for 24.7 percent of all recorded breaches

malware to public and private organisations. Then in the summer of 2021, managed services providers were hit by a similar supply chain incident as remote monitoring and management software from Kaseya was exploited by a large scale ransomware campaign. The campaign, for which a Ukrainian citizen with links to the REvil ransomware group was eventually charged, also leveraged multiple zero-days in its attempt to disrupt networks. Importantly, these attacks groups – like Nobelium, have continued to target supply chains, compromising targets via resellers and service providers which puts connected organisations on the radar of these attackers. Threat actors have exploited new zero days in products from both SolarWinds and Kaseya since their supply chain incidents were disclosed.

Ransomware attacks increased in both volume and sophistication in 2021, with the Kaseya incident being only one of many such breaches. Last year, ransomware groups leveraged zero-days and legacy vulnerabilities alike to target sensitive sectors like healthcare, education and the physical supply chain. Double extortion became the linchpin of most ransomware groups and a key factor in the record breaking profits for ransomware operators.

Healthcare was the sector upon which ransomware operators inflicted the most damage in 2021, accounting for 24.7 percent of all recorded breaches. Hospitals, doctors' offices, billing companies, dentists, therapists and more were impacted by a variety of threats. One of the most notable healthcare breaches linked to ransomware was conducted by the Conti ransomware group, which crippled Ireland's Health Service Executive in May 2021. As a result of the breach, all IT systems had to be shut down for weeks and services like blood test results and patient diagnostics were severely affected.

In addition to healthcare, the education sector was also heavily impacted by ransomware. An astounding 52 percent of breaches were linked to ransomware attacks, leading to severe ramifications for students, educators and parents alike. Many were impacted through cancelled classes and inaccessible learning platforms, and educators must recognise the uphill battle they face securing and protecting devices in the age of hybrid education. It is not clear whether ransomware operators specifically targeted education organisations, or if these results have grown from opportunistic attacks targeting easy-to-find devices, but no matter the motivation, educators should remain conscious of the trend's consequences.

THE CONTI RANSOMWARE GROUP CRIPPLED IRELAND'S HEALTH SERVICE IN MAY 2021

In the wake of major attacks on critical infrastructure in 2021, concerns surrounding the security of OT environments have never been higher. Colonial Pipeline, the largest pipeline in the United States, suffered an attack linked to the Darkside ransomware group in May it impacted its pipeline operations. Consumers and businesses alike were affected with drivers facing long lines to purchase fuel, while gas prices climbed to worrying heights. Colonial's CEO later testified before the United States Senate that the attack was due to a legacy VPN account, which lacked multifactor authentication and had not been decommissioned.

Additional risk to critical infrastructure is introduced when security controls and code audits are not in place. A common thread in such risks is the use of insecure protocols such as file transfer protocol and telnet; though they served an important purpose in the past, they can add unnecessary risk running sometimes without a business's knowledge.

The use and re-use of software libraries and real-time operating systems (RTOS) across multiple devices and manufacturers is widespread, making patch management and asset enumeration for these issues tough problems to solve for many organisations. In exceptional cases, mitigations and network segmentation may be the only feasible option for devices that are no longer manufactured or supported by vendors.

Ransomware also took advantage of misconfigurations in Active Directory (AD) in 2021, as threat groups of all kinds exploited this to elevate privilege and traverse networks to further infiltrate target organisations. In fact, when it came to AD, ransomware was responsible for more than half of the breaches analysed; though a small percentage of these were as a result of misconfigured or unsecured cloud databases. Openly accessible cloud databases and overly permissive AD configurations give attackers access to

an organisation's most sensitive information providing valuable fodder for ransoms.

As previously mentioned, 2021 closed with security teams alerted to a critical vulnerability in Log4J dubbed Log4Shell – found in a wide range of services, applications and devices across all industries and geographies. The reason this vulnerability was deemed to be so severe, compared with others, is because it's so ubiquitous. It really does touch so many different types of software and services. It's not as simple as looking for a particular piece of software and checking the version that's being run. Because of the way modern applications and services are written, there can be a number of dependencies that could contain this library, and organisations may not even realise it.

FINANCIALLY MOTIVATED RANSOMWARE GROUPS WANT MINIMAL EFFORT WITH MAXIMUM PROFIT

Threat actors have moved quickly to take advantage of this vulnerability. To date there have been at least 11 publicised attacks that have used Log4Shell. In the UK, the NHS warned that unknown hackers were targeting VMware Horizon deployments with Log4Shell exploits. While unclear if this was connected, ransomware gang NightSky_were identified as using Log4Shell to gain access to VMWare Horizon. Meanwhile APT34, another well-known ransomware group, was confirmed as exploiting Log4Shell to distribute a new modular PowerShell toolkit.

Ransomware groups are financially motivated, but want minimal effort with maximum profit. They look for low-hanging fruit such as known but unpatched vulnerabilities, gaps in legacy technologies like VPNs, combined with AD misconfigurations to impact organisations.

But there is hope when it comes to addressing this risk. Organisations can take steps to protect themselves via a holistic security approach. Businesses must examine devices on their network, assessing which controls are already in place to prevent unneeded network access to devices. It is also important to think like employees, recognising the importance that OT devices have in our everyday lives as organisations revisit their security. Hybrid and remote working is not going away – many companies are adopting permanent hybrid models and some are doing away with office spaces altogether – so organisations must redefine their perimeter by examining how cloud and OT assets are secured and integrated within their organisation.

When looking back and learning from 2021, organisations must understand the need to redefine while continuing to protect the evolving perimeter, adopting cloud infrastructure with care and employing security protocols that work across diversified networks. Such care and attention should also be applied to the use of AD addressing misconfigurations. Legacy systems should also be identified and either removed or ringfenced to avoid unidentified attack pathways to exist.

The string of supply chain-related breaches and attacks in 2021 only highlight the need to build on protection for the software supply chain. In fact, 61 percent of security leaders reported that their organisation was exposed to increased risk related to its expanding supply chain in 2021; and though this awareness could make for more action to protect growing corporate networks, for many it was already too late. When assessing events like SolarWinds, Kaseya and finally Log4Shell, businesses must recognise that now more than ever, getting ahead of cyber espionage and ransomware attacks is paramount to security ●

Bernard Montel is EMEA Technical Director and Security Strategist at Tenable. With over 20 years in the security industry, Bernard's expertise includes cryptography, Identity & Access Management, and SOC domains. He has published numerous articles and is regularly invited to speak about cybersecurity – providing insight into current cybersecurity threats, cyber risk management and cyber exposure.

Colonial's CEO revealed the attack was due to a legacy VPN account lacking multifactor authentication that had not been decommissioned

IDENTIFY YOURSELF

Joseph Carson *reveals why organisations need to embrace identity as the future perimeter*

The world of work has long been a place as much as a function. Technical limitations meant that workers needed to be onsite to access resources. Even as technology advanced, tradition held. Consequently, network security has historically been concentrated on specific workplaces too, with most strategies relying on a static, secure perimeter at the location.

And then came COVID. The pandemic not only opened the door to the possibility of remote working, it forced organisations through it, whether they were ready or not. It accelerated business transformation and the adoption of remote working.

Two years down the line, with normality resuming, the door to remote working remains open. While most organisations have returned to office-based work, a significant amount have retained some level of flexibility. The ONS found that between 16 and 27 February 2022, 15 percent of UK employees worked from home because of COVID. In this hybrid working world, in which the boundaries have shifted, identity is the new perimeter.

Relying on legacy security to protect the network layer, while also enabling remote workers and making use of cloud-based assets presents a number of problems. For example, the strategy might rely on the presence of enterprise-grade secure routers, while workers at home

The biggest issue with a legacy perimeter-based approach to security is the way in which it handles identity

will almost certainly be using commercial routers that cannot offer the same level of protection – typically with default credentials. But it is not feasible to equip potentially thousands of individuals with a router for each location, nor to mandate that they purchase one themselves.

Similarly, cloud-based assets and infrastructure will not benefit from any location-based perimeter security, rendering these legacy solutions increasingly moot as cloud migration continues. We have started to shift from BYOD (Bring your own Device) to BYOO (Bring your own office) and employees' homes are almost becoming mini cloud sites where the employee operates from.

The biggest issue with a legacy perimeter-based approach to security is the way it handles identity. The standard username/password combination has been the staple of user identity for many years, and organisations still have critical assets that can be accessed without any further security controls or verification.

Threat actors are well aware of this and the majority of attacks concentrate on exploiting this critical weakness. The 2021 Verizon Data Breach Investigations Report found that 61 percent of all breaches were the result of attackers exploiting data through leaked or stolen credentials, or via brute force and credential stuffing attacks. The report also highlighted a continued increase in phishing attacks as adversaries attempt to trick targets into sharing their credentials by impersonating colleagues, IT personnel and systems themselves.

However, criminals often don't even need to go to the effort of creating a social engineering campaign. Weak, manually, human-generated passwords can be quickly guessed by automated brute force attacks. The tendency to re-use the same passwords in multiple places also opens the threat of credential stuffing attacks that attempt to use credentials stolen in previous breaches.

Once an attacker has a working set of credentials they will be able to walk right in unless the organisation has other layers of identity security in place. The effect is a locked portcullis that can be opened by anyone who finds, steals or duplicates a key – and there happens to be thousands of copies around.

Once an attacker is inside, research indicates that the average dwell time stands at 24 days – ample time to exfiltrate data, plant targeted malware, and establish back doors. It also provides the opportunity for more organised threat actors to expand their attack into the supply chain.

Privileged accounts with elevated levels of system access and admin power are the ultimate target of most cyber attacks. Accounts such as local and domain admins have a large array of capabilities that can be exploited. Threat actors can use Active Directory to create more accounts with increased authorisation, access and edit critical data and systems, and change logs to hide their tracks.

Nevertheless, we often find accounts are poorly managed. Many enterprises still have privileged accounts governed by weak passwords open to brute forcing and credential stuffing. Privileged account creds are also frequently saved in unencrypted Excel or text files, and freely traded across email and channels like Teams and Slack. This means that compromising a single standard user can quickly grant access to powerful superuser abilities.

Another common mistake is to focus on employees and overlook non-human users. Modern IT infrastructure relies on service accounts to provide access for automated systems, which often have a high level of privilege. While most workers will not even be aware they exist, they can be exploited by threat actors in the same way as human-facing admin accounts.

Identity is now the focal point for cyber-attacks and so it should be the main security control. User accounts should be thought of not as simple combinations of usernames and passwords, but as trusted digital identities tied to specific individuals and their specific roles.

The Zero Trust framework has emerged as one of the most effective ways of managing this. Simply having a set of credentials is the first step – users must also prove they are trustworthy before they can access anything on the network. How this is earned will vary depending on the situation, with a risk-based process accounting for the importance of the assets requested, as well as factors such as the user's location and endpoint device they are using.

A user sitting at their desk from their recognised machine will be given relatively easy access, while someone using an unfamiliar machine in an unusual location will need to jump through a few more hoops to confirm they aren't an imposter. It will act like a digital polygraph test asking the right questions to confirm the identity is authentic.

MULTIPLE LEVELS OF SECURITY HELPS VERIFY THE USER IS REALLY WHO THEY ARE CLAIMING TO BE

When it comes to special privileged accounts shared by multiple users, a rigid adherence to least privilege is required, ensuring that accounts and systems can only be accessed as part of core job functions. A Privilege Access Management (PAM) solution is also important to keep credentials safe and keep track of how these accounts are being accessed and used.

Identity should be separated into two elements. First is verification, confirming that the user is who they claim to be. Second is authorisation, governing what they are allowed to do once their identity is confirmed. A modern equivalent could be a well-guarded bank, complete with vault and safe deposit boxes. Getting into the building itself is accomplished with a mere visual check from the guard, which will provide a bare minimum of security, keeping out known undesirables. Accessing the safe deposit room, however, requires another level of authentication to prove the visitor has the right to be there, such as further ID or the use of biometrics. Finally, actually opening the safe box requires the use of a key, while also under the watchful eye of a security guard.

In this convenient example, the contents of the safe deposit box are protected by multiple layers of security to authenticate the visitor's identity and authorise them to access the box. However, this also creates a cumbersome process for legitimate customers to go through. This is bearable for occasional visits, but quickly creates friction if it must be repeated on a regular basis. In a digital setting, users will need to verify their identities several times every day as they navigate the system and access restricted data and applications. Having to jump through hoops every time creates a negative user experience that can also start impacting productivity. Security must be balanced against usability.

The answer to this problem is to establish a pyramid of controls that allow users to move laterally based on

the level of trust they have earned. So going through the lowest level of authentication using credentials, allows access to only low-security areas of the network. Attempting to access something more secure requires additional authentication through multifactor authentication (MFA) or a VPN. Once this has been completed, the user is free to access other applications at the same security level without authenticating again unless the risks change or time has expired.

ONCE AN ATTACKER IS INSIDE, RESEARCH INDICATES AVERAGE DWELL TIME IS 24 DAYS

Attempting to move up again, let's say accessing AD to create a new user account, requires the strongest form of authentication, such as a more strict form of MFA or authorisation from a colleague. Authorising at this level means the user is free to access anything further down the pyramid for the rest of the session.

For an excellent example of this process at work, one can look to the Estonian government, which has launched a raft of digital services in recent years. Once a user has signed into the service portal using their government ID as the trust anchor, they can move laterally to access multiple different provisions such as renewing their driver's license or updating their personal details. The process provides an efficient and frictionless experience for users without compromising on security. Having multiple levels of security from authentication to digital signatures, helps verify the user is really who they are claiming to be.

Moving towards identity-based security can be a significant task, and many enterprises are still stuck with security strategies geared to an outward-facing perimeter around their network. A combination of limited budgets and the baggage of years of legacy infrastructure and technical debt can make it difficult to make the jump, even as firms also pursue cloud and remote working.

However, an identity-based model and Zero Trust approach do not have to be accomplished in a single bound. Enterprises should look at small-use cases in the first instance to get a feel for the process and prove the value of the approach, and then gradually spread out to other parts of their operations. Critical systems and privileged accounts that pose the greatest risk should be the priority here.

LAYERED DEFENCE

An important initial step is to evaluate the current IT and security stack and scope out areas that can be better integrated. The ultimate aim is to create a single, centralised control point that can manage identity across the entire infrastructure. Future investments should be centred on interoperability – creating a layered defence of solutions that can work together.

A highly integrated stack will also make it easier to implement automation – the second priority. Authentication, authorisation, monitoring and all other secure access processes should be guided by automated policies that can apply adaptable risk-based rules and create a frictionless user experience.

The third priority is orchestration. Everything should work together seamlessly, with no gaps or blind spots that could be exploited by threat actors. PAM tools are useful here as they can help the security team manage and secure credentials across the entire organisation, for example removing the risk of manually created passwords waiting to be discovered in text documents.

Traditional, static perimeters can only guard against the threats of the past and are easily bypassed by today's threat actors. Establishing identity as the new perimeter, supported by a frictionless authentication system, will enable organisations to continue adapting to the latest working developments without leaving the door open for threat actors ●

Joseph Carson is Chief Security Scientist and Advisory CISO at Delinea

The tendency to re-use passwords in multiple places opens up the threat of attacks

INTERNATIONAL SECURITY EXPO

27-28 SEPTEMBER 2022. OLYMPIA LONDON

THE CRITICAL LINK IN YOUR BUSINESS STRATEGY

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

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

10,000+
SECURITY BUYERS

350+
INTERNATIONAL EXHIBITING COMPANIES

SECURE YOUR STAND **TODAY**

VISIT: www.internationalsecurityexpo.com

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

INCIDENT BRIEF

Europe

30 March, Belfast – Northern Ireland
A man was charged with a number of offences after the driver of a van was threatened by two gunmen and forced to drive a device he believed to be a bomb to a peace event. The threat led to Ireland's foreign minister being evacuated.

30 March, Zwolle – Netherlands
Two people were killed after a gunman opened fire in a McDonald's restaurant in the northern Dutch city.

6 April, Berlin – Germany
Former security guard at the British embassy in Berlin, David Smith, was charged with spying for the Russian state after being extradited back to the UK.

6 April, Germany
German authorities swooped on neo-Nazi militant cells and arrested four suspects believed to be involved with Knockout 51, Combat 18, the US-based Atomwaffen Division and Sonderkommando 1418.

12 April, London – UK
Extinction Rebellion protesters forced the closure of the insurance market Lloyd's of London, after using superglue, chains and bicycle locks to block entrances to the building.

14-7 April, across Sweden
Unrest broke out across the country despite police moving a rally by the Danish anti-Islam far-right Stram Kurs party, which was planning to burn a Qur'an, to a new location as a preventive measure. Demonstrators threw stones and burned vehicles as protests continued over three nights.

Americas

1 April, San Francisco – USA
Police stopped a vehicle operated by Cruise – the autonomous car company backed by General Motors – as it had been driving without headlights, only to find it was empty.

3 April, California – USA
Twenty six people were injured – three critically – as a soccer match descended into violent clashes between opposing fans.

6 April, USA
The US disrupted a global 'botnet' controlled by Russia's military intelligence agency. Attorney General Merrick Garland announced the Russian government had recently used similar infrastructure to attack Ukrainian targets.

12 April, Brooklyn – USA
A gunman wearing a gas mask filled a crowded New York subway car with thick black smoke from a canister and opened fire on morning rush-hour passengers, injuring more than 20, including 10 with gunshot wounds.

16 April, South Carolina – USA
A 22-year-old man was arrested in connection with a shooting at a Columbia shopping mall in which 14 people were either shot or injured during a stampede to escape.

15 April, Arizona – USA
A Mexican woman attempting to climb the US border wall in eastern Arizona died after her leg became trapped in a climbing harness and she was left hanging upside down for a "significant amount of time" according to local authorities.

Asia

27 March, Hadera – Israel
Islamic State claimed responsibility for an attack in which two Israeli police were killed in the northern city.

31 March, West Bank – Israel
A Palestinian stabbed a 28-year-old Israeli man on a bus before being killed by a bystander.

31 March, West Bank – Israel
Israeli forces raided a refugee camp in Jenin, setting off a gun battle in which two Palestinians were killed and more than a dozen were wounded.

1 April, Mirihana – Sri Lanka
As many as 50 people were injured after authorities used teargas and water cannons on crowds that stormed the home of President Gotabaya Rajapaksa.

2 April, West Bank – Israel
Israeli security forces killed three Palestinian men in the occupied West Bank in a pre-dawn incident. Israeli police said the men were armed and were: "killed in a shoot out".

5 April, Auckland – New Zealand
New Zealand's bomb squad was called into a chip factory after a potato trundling down the production line turned out to be a grenade. The weapon was dug up from a potato farm in Matamata, in the Waikato region.

12 April, Ashkelon – Israel
A Palestinian man stabbed a police officer with a kitchen knife and was shot dead in the Israeli port city. The officer was hospitalised with light wounds.

18 April, Jerusalem – Israel
More than 20 Palestinians and Israelis were wounded in and around Jerusalem's al-Aqsa mosque compound after Palestinian demonstrators started gathering piles of stones, shortly before the arrival of Jewish visitors.

19 April, Rambukkana – Sri Lanka
One person died and several others were left in a critical condition after police opened fire on a crowd who were protesting against rising fuel prices.

Africa

29 March, Kaduna – Nigeria
Gunmen attacked a train travelling from the Nigerian capital in an "unprecedented" act of violence. Authorities could not immediately confirm the number of passengers on the train but local media reported around 1,000 passengers.

7 April, Lake Chad – Nigeria
At least 10 Islamic State of the West African Province (ISWAP) terrorists, including top commanders, were executed by its affiliates, Jama'at Ahl as-Sunnah lid-Da'wah wa'l-Jihad faction of Boko Haram.

7 April, Goma – DRC
An explosion – reportedly caused by a grenade – at a military camp bar on the outskirts of eastern Congo's largest city killed eight people.

20 April, Geidam – Nigeria
The Police Command in Yobe confirmed that 10 people were killed and several others wounded in an attack orchestrated by Boko Haram insurgents in the Damaturu town.

22 April, Sambisa Forest – Nigeria
Boko Haram and ISWAP terrorists clashed, resulting in the killing of two commanders and 32 fighters in Borno State.

23 April, Mogadishu – Somalia
Three people were killed and eight others injured when a suicide bomber detonated his device at a beach restaurant.

24 April, Sevare, Niono and Bapho – Mali
Six soldiers were killed and 20 injured in simultaneous attacks – by militants wearing suicide vests – targeting three army bases.

24 April, Darfur region – Sudan
Clashes between rival groups in Sudan's Darfur saw at least 168 killed and 98 wounded. The violence broke out when armed tribesmen attacked villages of the non-Arab Massalit minority in retaliation for the killing of two tribesmen.

25 April, Gubio Local Government Area – Nigeria
At least one person was killed and many others injured during an attack by ISWAP fighters when they invaded the community in Borno as villagers fled to the woods for cover.

NEWS

Europe

Street lighting increases rather than deters theft from cars

New research suggests that when it comes to reducing theft from cars, it might be best to leave street lighting off. Researchers found the level of night-time thefts from cars almost halved when street lighting was turned off between midnight and 5am, compared with staying on all night. The authors suggest possible reasons for this include that it is harder for offenders to see valuables inside a car or assess a vehicle's security without lighting. Three types of changes to street lighting, aside from it being on all night, were examined: illumination being switched off between midnight and 5am, using white all-night illumination and the dimming of lighting in the small hours. IN short, the team concluded that all forms of crime analysed were more common at night than during the day.

Abloy UK unveils new Digital Access Solutions Academy

Abloy UK has launched a new purpose-built facility to showcase, work with, install and test its extensive range of products, with particular focus on new digital solutions and ecosystems. The new Digital Access Solutions Academy is a significant milestone in the ongoing development of the comprehensive training and continuing professional development offering from Abloy. Education has been a critical focus for the company since it first launched the Abloy Academy back in 2008. Abloy UK recognised there was a need to create a new area of the Academy for its growing customer base, to focus specifically on its expanding range of digital access solutions. Ian Miller, Digital Access Solutions Academy Manager at Abloy UK, explained: "The first focus of training at the new facility centres around our Incedo access control product range and is aimed at security engineers and sales teams. I believe people learn best by doing something, so the training is designed to be hands on and shows how to specify, install and support their customers requiring an access control solution".

Saab's Digital Tower gets approval from UK regulator

Saab has achieved a regulatory approval required to supply the United Kingdom's Armed Forces with Digital Tower technology. The company has been successfully accredited under the Air Traffic Management (ATM) Equipment Approved Organisation Scheme (AAOS) by the UK Military Aviation Authority and is approved to develop, provide, install and maintain ATM equipment for customers in the UK Ministry of Defence – an important step required to be able to deliver ATM equipment to the UK Armed Forces. The AAOS approval was achieved following a year-long effort of working alongside the UK's Military Aviation Authority (MAA). It is noteworthy as being the first AAOS ever issued for a delivery organisation for military Digital Tower ATM equipment, a unique achievement for Saab. "This is an important step for us to support the UK MOD with the expansion of digital towers and we are proud to have the only accredited solution that complies with their regulations," said Per Ahl, CEO of Saab Digital Air Traffic Solutions. Other Saab Digital Air Traffic Solution approvals include certification to provide Air Traffic Services and MET-observation services according to EU-regulation and providing digital ATC as a service at four Swedish airports.

BBC hands over 'Troubles' footage to help police

The BBC will hand over broadcast and unbroadcast material from a documentary series that was made about Northern Ireland's Troubles to the police as part of investigations into terrorist activity, a judge has revealed. An order was made at Belfast Crown Court following agreement between the Police Service of Northern Ireland (PSNI) and BBC on material from a series first broadcast in 2019. The material includes interviews with Catholic priest Patrick Ryan, who told the programme he had maintained a network of Europe-wide contacts to generate arms and money for the IRA. It also features interviews with convicted killer Laurence Maguire about his involvement with the Mid Ulster UVF. Judge Neil Rafferty praised counsel for both the BBC and the PSNI noting: "In respect to material that is identified to me, I am satisfied that, given the nature of the material and the spirit in which the order has been drawn up, I am satisfied the public interest is in favour of granting an order."

COVID loan scheme fraud not being addressed say UK MPs

British MPs have criticised the government for its failure to draw up plans to recover nearly £5-billion taken from the Coronavirus emergency bounceback loan scheme by fraudsters. The government must give more resources to counter-fraud agencies and account for how much of the money will be lost forever, according to a report published by Parliament's influential public accounts committee. The bounceback loan scheme (BBLS) was aimed at supporting small businesses, while the furlough scheme covered 80 percent of the wages of people unable to do their jobs. However, the MPs said that the government was "complacent in preventing fraud" in particular in bounceback loans, which were given by banks but guaranteed by the state – leaving taxpayers with the bill. An estimated £4.9-billion of the £47-billion spent was lost to fraud, while a further £5.7-billion is estimated to have been lost from fraud and error within the furlough and self-employment schemes, two of the other key support schemes during the crisis.

NEWS

Americas

Phishing campaign targets US election officials

The FBI has warned US election officials of a widespread phishing campaign by unidentified hackers attempting to steal their credentials. The threat: "is still very real" and is heading into the 2022 election season, warned the bureau, citing at least three separate: "coordinated" phishing attempts in nine states since October 2021. Though the FBI didn't disclose the exact states or names of officials who were targeted, they cautioned that had the attempt been a successful one the sensitive information of those concerned may have been compromised.
The FBI advised that: "proactive monitoring" of election infrastructure, including official email accounts, and communication between itself and state, local, territorial and tribal partners about this type of activity will provide opportunities to mitigate instances of credential harvesting and compromise, identify potential targets and information sought by threat actors and identify threat actors.

US rocked by three separate mass shootings during Easter

Two teenage boys were killed and eight others wounded after gunfire erupted at a party in a short-term rental home in Pittsburgh on Easter Sunday, one of at least three mass shootings across the US over Easter weekend. The other two shootings – both in South Carolina – left a total of 18 people with bullet wounds, once again reigniting calls among advocates for more meaningful gun control legislation. In Pittsburgh, police said equipment that detects gunfire prompted officers to go to an address on Suismon Street where as many as 10 people had been shot. First responders brought several of the victims to a hospital, including two 17-year-old boys which doctors later pronounced dead. There had been at least 50 gunshots fired in the home in question by multiple people who had been drawn into some sort of fight, police said. A handful of other partygoers who were injured but not shot had suffered cuts and broken bones while jumping out of windows to get to safety. Meanwhile, the same day, gunfire which erupted at a nightclub in Hampton county, South Carolina, injured nine people. Finally, 90 miles South, a separate shooting at a mall in South Carolina's capital of Columbia left nine with bullet wounds. The wounded ranged in age from 15 to 73.

Colombian army botches raid that leaves four civilians dead

Colombian authorities are facing growing calls to investigate a botched raid by the army in which at least four civilians – including a 16-year old boy, a pregnant woman and an indigenous leader – were killed. The raid took place on 28 March in a remote village in the southern province of Putumayo and was intended to target dissident guerrillas from the now-defunct Revolutionary Armed Forces of Colombia (Farc) who are now involved in the cocaine trade. However, the mission left 11 dead, including the civilians, in circumstances that remain shrouded in mystery. Witnesses and local journalists have said that the victims' bodies and the scene of the killings appear to have been tampered with, adding to the suspicion.
Colombia's army has repeatedly been accused of killing civilians and has vehemently denied any wrongdoing, characterising the raid as a legal operation to take out violent terrorists. Human rights organisations, however, have questioned the official account.

FBI seizes control of popular hacking forum

US law enforcement agencies have partnered up with their international counterparts to take control of a popular website where hackers have advertised data stolen from US consumers and corporations – the latest in a long-running effort to crack down on forums where cybercriminals congregate. "This domain has been seized by the FBI, US Secret Service and Justice Department", read a notice in early April on the home page of RaidForums, a website known more for advertising hacked data in English rather than Russian. Law enforcement agencies from the UK and Sweden were involved in the seizure, according to the statement. With over 530,000 registered members, according to threat intelligence firm Recorded Future, RaidForums has great reach and influence among low to mid-level cybercriminals. This is just the latest move in a sustained international law enforcement effort to up end the marketplaces where cybercrime flourishes. Just a week earlier German police seized the computer servers of Hydra, a popular Russian Dark Web market that's been connected to $5-billion in transactions since 2015.

Governor signs Texas-Mexico border security MOU

Texas Governor Greg Abbott met with Tamaulipas Governor Francisco García Cabeza de Vaca in Weslaco to discuss ongoing challenges along the Texas-Mexico border. The Governor signed a memorandum of understanding (MOU) between the states of Texas and Tamaulipas to enhance border security measures that will prevent illegal immigration from Mexico to Texas and improve the flow of traffic across the international bridge. The MOU goes into effect immediately.
"I am grateful for the partnership of Governor Cabeza de Vaca as we work to secure our border," said Governor Abbott. "With the State of Tamaulipas' detailed plan to secure the border, the Texas Department of Public Safety can return to its previous strategy of random searches. While President Biden ignores the ongoing crisis at the border, the State of Texas will continue to work with heads of state in Mexico to further strengthen our comprehensive border strategy."

NEWS

Asia

Afghan family unable to get to UK without biometrics

A family in hiding in Afghanistan that is eligible for sanctuary in the UK but can't escape the country because they can't get biometrics done have taken their case to the high court. The case has highlighted the different treatment given to those fleeing conflict in Ukraine and Afghanistan when it comes to biometrics requirements. When Russia first invaded Ukraine, the Home Office said Ukrainians applying for visas had to provide their biometrics before coming to the UK. However, this was relaxed in mid-March and Ukrainians with passports were permitted to do applications online and get biometrics done after reaching the UK. The family bringing the legal challenge consists of a father who is a British citizen, his wife and the couple's five children, aged between seven and 17. They were unable to be airlifted out of Kabul last August due to a lack of space on evacuation flights. It is thought that many more families in the same situation are in hiding in Afghanistan.

Israel's PM urges citizens to arm themselves after Tel Aviv attack

Israeli prime minister Naftali Bennett has called on citizens with gun licences to arm themselves after the bloodiest attack in years took place in greater Tel Aviv – marking the third such killing spree in a week. Bennett spoke from his home – where he is in quarantine after testing positive for Covid– and warned that the country was facing a: "new wave of terror". A series of attacks have left Israelis and Palestinians braced for further violence, while defence minister, Benny Gantz, has ordered 1,000 soldiers to bolster police forces as Israel's military presence in the Palestinian territories it occupies has been reinforced. The bloodshed comes at a particularly perilous time for the country as May sees a rare convergence of Ramadan for Muslims, Passover for Jews and Easter for Christians expected to raise tensions as people take time off from work and head into the streets. Israel tightly controls access to Jerusalem's holy sites for all three religions, which has previously led to confrontations.

Solomon Islands will not allow China to build military base

The Solomon Islands has said it won't allow China to build a military base as it seeks to counter international fears over its new security alliance with the state. Unfortunately, such reassurance is doing little to placate concerns about the pact from the nation's traditional partners, which include New Zealand, Australia and the United States. The Solomon Islands' government stated that a draft agreement of the new security pact had been initialled by representatives from Solomon Islands and China and would be: "cleaned up" and signed before adding that: "contrary to the misinformation promoted by anti-government commentators" the agreement did not invite China to establish a military base. Prime Minister Manasseh Sogavare was keen to highlight that his nation sought only peace and prosperity, citing its foreign policy mantra: "We are friends to all and enemies to none." He said it wasn't a secret deal, but a sovereign issue. Under the terms of the draft agreement, China can send police, military personnel and other armed forces to Solomon Islands: "to assist in maintaining social order" and for a variety of other reasons. It can also send warships to the islands for stopovers and to replenish supplies, which has led to speculation about the possibility of China establishing a naval base on the South Pacific islands.

GA-ASI selected for Japan coast guard RPAS project

General Atomics Aeronautical Systems, Inc. has been selected to support the Japan Coast Guard's (JCG) RPAS Project. Operations will feature GA-ASI's MQ-9B SeaGuardian and begin in October 2022. SeaGuardian will be used to conduct wide-area maritime surveillance to support JCG's missions, which include search and rescue, disaster response and maritime law enforcement. This project follows a series of successful JCG flight trials in 2020 that used SeaGuardian to validate the same JCG missions in accordance with Japan's Policy on Strengthening the Maritime Security Systems using unmanned aerial vehicles to perform maritime wide-area surveillance. SeaGuardian features a multi-mode maritime surface-search radar with an Inverse Synthetic Aperture Radar imaging mode, Automatic Identification System receiver and High-Definition – Full-Motion Video – sensor equipped with optical and infrared cameras. This sensor suite enables real-time detection and identification of surface vessels over thousands of square nautical miles and provides automatic tracking of maritime targets and correlation of AIS transmitters with radar tracks.

Chinese hackers target India's power grid

India's power sector has been targeted by hackers in a long-term operation carried out by a state-sponsored group from China, according to Massachusetts-based Recorded Future. Over the last few months, the Insikt Group, the threat research division of the cybersecurity company, has collected evidence of hackers targeting seven Indian state centres responsible for carrying electrical dispatch and grid control. The group primarily used the ShadowPad trojan – developed for China's Ministry of State Security – leading to the conclusion this was a state-sponsored attack. China's Foreign Ministry spokesman Zhao Lijian said the report had been: "noted" by Beijing, but that China: "will not encourage, support or condone any cyberattacks".

Milipol Qatar
Exhibition 2022

International Event for
Homeland Security & Civil Defence

14th Edition

24 - 26 May 2022

DECC - DOHA

@Milipolqatar

www.milipolqatar.com

NEWS

Africa

Nigerian train attack passengers still unaccounted for

More than 160 passengers who were on a train that was attacked in the city of Kaduna in northern Nigerian at the end of March still remain unaccounted for, according to local reports. As many as ten people were killed on 28 March when a collaboration between Boko Haram jihadists and local bandits saw gunmen bombing the tracks, derailing the train, gunning down passengers and staff and then abducting people. The Nigerian Railway Corporation that runs the service revealed in April that 168 people were unaccounted for, including over 140 passengers it had not been able to reach through registered contacts, while at least one person paid a ransom and was released. The attack was initially suspected to be carried out by mainly ethnic Fulani gunmen who are heavily armed and coordinated and have grown to become more deadly than jihadist groups.

Russian mercenaries and Mali army accused of killing 300

Human Rights Watch (HRW) has claimed that suspected Russian mercenaries participated in an operation with Mali's army in March in which as many as 300 civilian men were killed over the course of five days. Witnesses and local community leaders said hundreds of men were rounded up and killed in small groups during the anti-jihadist operation in the central town of Moura – located in the Mopti region, a hotspot of jihadist activity that has intensified and spread to neighbouring countries in the Sahel region. Local security sources claimed that more than 100 Russian-speaking men were involved in the operation, which has been described as the worst single atrocity reported in Mali's decade-long armed conflict. Witnesses spoke of white soldiers talking in an unfamiliar foreign language they believed to be Russian. Mali's army has long been accused of rights abuses during counter-insurgency operations. A Mali military spokesperson refused to respond to a request by Reuters for comment on the HRW report.

'Youth bulge' to blame for rising terrorism in Nigeria

The Financial Derivatives Company Limited (FDC) has suggested that the rising level of insecurity and terrorism in Nigeria is down to feelings of frustration, economic marginalisation and alienation of the country's teeming youth population. The Lagos-based research and investment company made the claim in its latest bi-monthly economic report. The report pointed out that in the past decade, an estimated 87,903 people have died through Boko Haram, state actors, sectarian actors and other armed bandits in the country. According to the firm headed by Bismarck Rewane, a member of President Muhammadu Buhari's Economic Advisory Council, Nigeria, is experiencing 'youth bulge' – a pattern usually experienced when countries succeed in reducing infant mortality while keeping fertility rate high. According to the report the unemployment rates for persons between the ages of 15 and 24 and 25 and 34 are estimated at 53.4 percent and 37.2 percent respectively.

Nyusi Praises role of veterans in fighting terrorism

Mozambican President Filipe Nyusi has stressed that the veterans of Mozambique's war for independence have played a vital role in securing the gains made in the fight against jihadist terrorism in the northern province of Cabo Delgado. Speaking in the southern city of Matola at the opening of a meeting of the National Committee of the Association of Veterans of the National Liberation Struggle (ACLLN), Nyusi observed: "We are holding this meeting at a special moment, when our country is registering encouraging signs in various areas. Although volatile attacks continue in some parts of Cabo Delgado province, we are pleased to note the positive evolution in the struggle against terrorism and extremism thanks to the determination of our defence and security forces". The gradual resumption of social and economic life in areas once severely hit by terrorism, he said, was due, not only to the support of the troops from Rwanda and from the Southern African Development Community, but also the involvement of the veterans who have lent their experience to the Mozambican forces and their allies. "I would like to praise the direct involvement of the veterans of the national liberation struggle who have decided to make use of their experience to end the murders, kidnappings, rapes, destruction of infrastructures and all the heinous crimes perpetrated by groups of terrorists since October 2017", Nyusi declared.

African countries call on Ghana for collaboration and support

The Gambia, Sierra Leone and Mozambique have called on Ghana's Cyber Security Authority (CSA) for collaboration and support for the development of cyber security in their respective countries. The calls were led by senior officials of the cyber security institutions of the aforementioned countries on the side-lines of the Africa Union – Global Forum on Cyber Expertise Africa Cyber Experts Kick-Off Meeting in Accra as part of improving bilateral relations with Ghana. Within the last five years, Ghana has taken progressive steps towards the development of cyber security and has also ensured the institutionalisation of cyber security to foster regional cooperation through the adoption of the ECOWAS' Regional Cyber security Cybercrime Strategy and the Regional Critical Infrastructure Protection Policy to strengthen its response in fighting cybercrime and improving its cybersecurity.

DIARY DATES

2022 Conference and Exhibition planner

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

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

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

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

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

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

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

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

20-25 June Interschutz 2022
Hannover, Germany
Organiser: Interschutz
Tel: +49 (0)511 89-0
www.interschutz.de

MGT europe

DroneTERMINATOR

USING EVOLUTION JAMMER TECHNOLOGY

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

DroneTERMINATOR utilizes RADAR on the Ku / X band, 2 Watt, 1 GHz bandwidth Long-Range Radar System to detect UAVs at a distance of up to 6 km, with micro-drones typically detected at 1-2 km realistically

JAMMING FREQUENCIES:

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

FEATURES:

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

MGT Europe www.mgteurope.com

YOUR MOBILITY SPECIALIST FOR ARMOURED VEHICLES

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

TSS International official distributor for:

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

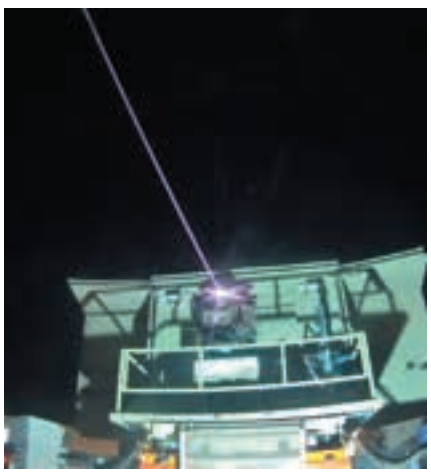
TSS

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

SHOWCASE

Laser interception system successfully completes live tests

RAFAEL, alongside Israel's Ministry of Defence's Directorate of Defence Research and Development (DDR&D) has successfully completed a series of ground-breaking tests with a high-power laser interception system against steep-track threats. The demonstrator successfully intercepted UAVs, mortars, rockets and anti-tank missiles in various scenarios. The tests are the first phase of a multi-year programme led by the DDR&D and defence industries. It aims to develop a high-power ground and aerial laser system equipped to deal with long-range, high-intensity threats. The laser will complement the company's Iron Dome system and will be an effective and economically efficient addition to Israel's multi-tiered air defence array. The system's development plan is led by the Research and Development Division in the Ministry of Defense's DDR&D. CEO and President of Rafael Advanced Defense Systems, Maj. Gen. (Res.) Yoav Har Even observed: "The successful tests included the interception of a wide range of threats and have proven the system's remarkable capabilities. Our cooperation with the DDR&D and the Ministry of Defense has led to this extraordinary development, constituting a significant milestone in the process to achieve operational capability."



Bittium's Tough VoIP field phone for tactical comms

Bittium has unveiled its Bittium Tough VoIP Field Phone 2. The Field Phone 2 is a next-generation VoIP phone that enables reliable communications in demanding conditions for military use. Together with the distributed and survivable Bittium Tough VoIP Service, calls between Field Phone 2 users are enabled regardless of where and how they have connected to the network. The service adapts quickly to the changes in the network structure and thus enables user mobility. "Bittium Tough VoIP Field Phone 2 is an excellent addition to our Tough VoIP product family and responds to customers' need of a next-generation field phone that has been designed for demanding military use. Field Phone 2 can be easily and seamlessly integrated with Bittium and third-party tactical communications networks. This helps leading the troops and maintaining situational awareness in the quickly changing conditions of the battlefield", says Jari Sankala, Senior Vice President of Bittium's Defence & Security product and service area.

Jacksons Fencing adopts a different angle

Jacksons Fencing has launched its new angled slotted fence post, which offers adaptable fence installation to outdoor spaces with difficult fence runs. The launch follows research and feedback with its regular customers, some of which revealed difficulty finding fencing solutions for spaces that don't conform to straight or 90° fencing. The new angled fence post makes a change of orientation possible between 30° to 45' degrees without any unsightly or less secure hacks that would have previously had to be used. As with many fence posts, it is recommended that they are set in concrete at least 0.60 metres into the ground. Peter Jackson, Managing Director, Jacksons Fencing remarked: "Our new angled slotted fence posts are available to those without 90° corners, and we hope with this new product we can continue to provide products that are perfectly manufactured, easy to install, low maintenance and highly durable".

Axis M5000-G multi-directional 15-megapixel camera

Axis Communications has announced the AXIS M5000-G PTZ, a multi-directional 15-megapixel camera offering total situational awareness of indoor areas up to 400m^2 (4300ft^2). It can communicate with as many as six devices in a system setup, while delivering sweeping overviews and detailed images. The cost-effective camera offers the benefits of four cameras while installing just one. With all four views displayed on one monitor, it's possible to move from overview to detailed views in a single click. The camera also features autofocus capabilities as well as indication lights to help deter antisocial and criminal behaviour. Additional key features include three 5-megapixel sensors for situational awareness; a 10x optical zoom with HDTV 1080p; and Z-Wave for smart home devices. The multidirectional PTZ camera is now available through Axis distribution.

PureTech Systems integration with radar

PureTech Systems has announced the successful integration of the OWL GroundAware GA1360 2D digital multi-beam forming radar system with the PureActiv Rapid-Deploy Autonomous Perimeter Surveillance System (R-DAPSS). R-DAPSS is equipped with PureTech's geospatial and AI boosted video analytics, PureActiv, which provides among the highest probability of detection while maintaining near-zero nuisance alarms for perimeter and wide-area protection. The trailer is equipped with radar, PTZ Cameras and PureActiv Auto-verification to eliminate nuisance alarms and perform auto-tracking, and deterrents such as loud hailers and strobe lights. It is solar and back-up generator powered, needing little to no fuel, depending on installation location. The GA1360 system combines advanced digital beamforming radar technology, classification intelligence, reconfigurability and easy integration with other security systems (such as video management and access control systems) to bring 360° of real-time, all-weather situational awareness for the physical security of perimeters and other sensitive areas of critical sites. As the foundation for event-based layered security, GA1360 enables automated detection, tracking, deterrence, and response to intrusions within a 1km radius of critical sites.

HEALD®

INNOVATORS, MANUFACTURERS AND INSTALLERS OF AWARD-WINNING PERIMETER SECURITY PRODUCTS

THE EVO BOLLARD

THE VIPER

THE RAPTOR

@healduk Heald Ltd

www.heald.uk.com

Secured by Design MADE IN BRITAIN MADE IN YORKSHIRE PSSA

SMART SECURITY

CHECKPOINT SCREENING

ADANI LIMITED

LINEV GROUP Company

TRANSMISSION X-RAY TECHNOLOGY

POWERED BY AI-EYE

ARTIFICIAL INTELLIGENCE SOFTWARE

+44 333 577 9813 | easales@adanisystems.com