

intersec

The Journal of International Security

June 2025

ON THE BRINK

**What next for
India-Pakistan
conflict?**

TAKE A STAND

Africa fights back against terror



POLMIL®

On-Ground Relocatable Security Fencing for Nuclear and Critical Infrastructure Sites



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® ON-GROUND
10M BIFOLD GATE**



**POLMIL® HARSH WEATHER TESTED
FOR MICROPHONIC PIDS**



POLMIL® RAPID DEPLOYMENT

Award winning on-ground physical security - designed and manufactured by Blok 'N' Mesh Global Ltd, Liverpool, England

UK Office:
info@polmilfence.com

IE Office:
ksherlock@bloknmesh.com

FR Office:
drose@batisec.fr

www.polmilfence.com - 0044 (0) 1226 654040

intersec

Volume 35 Issue 6
June 2025



Cover photograph: DVIDS

Editor

Jacob Charles

Principal Consultant Editor

Maj. Gen.

Julian Thompson CB OBE

International Arctic Correspondent

Barry Scott Zellen

Design & Production

jellymediauk.com

Published by

Albany Media Ltd

Warren House

Earlsdown, Dallington

Heathfield, TN21 9LY

Tel: +44 (0) 1435 830608

Website: www.intersec.co.uk

Advertising & Marketing

Director of Sales

Arran Lindsay

Tel: +44 (0) 1435 830608

Email: arran@intersec.co.uk

Editorial Enquiries

Jacob Charles

Tel: +44 (0) 7941 387692

Email: jake@intersec.co.uk

Subscriptions/Accounts

Faye Barlow

Tel: +44 (0) 1435 830608

Email: subs@intersec.co.uk

www.intersec.co.uk

EDITORIAL COMMENT

In a particularly worrying case of ‘do as I say not as I do’, it’s been revealed that more than 1,200 devices that could contain potentially sensitive data were reported lost or stolen across key government departments last year. The revelation came to light as encrypted USB data storage device manufacturer Apricorn announced the findings from its annual Freedom of Information requests into device loss and data breaches.

Disappointingly, the figures indicate that device security issues remain endemic across the public sector, with several departments reporting an increase in lost and stolen devices compared with 2023.

Across the 17 departments questioned, more than 1,200 organisational devices were reported lost or stolen between January and December 2024. HM Revenue and Customs accounted for 804 of these losses, including 499 mobile phones. While this represents a modest decrease compared with the 1,015 devices lost by HMRC in 2023, the number remains troubling given the sensitivity of the information being handled.

Other departments showed a more disconcerting trend with The House of Commons reporting 100 devices lost or stolen, a significant increase from 65 the previous year. Similarly, the Department for Education saw losses climb from 78 to 107. The Department for Energy Security and Net Zero also reported a rise, from 122 last year to 150. Meanwhile, the Department for Science, Innovation and Technology reported 113 missing devices.

Although there is some improvement in some departments, it’s very clear that

the high levels of loss of devices across the government highlights that serious issues have not been resolved and there is still much work to do. As Jon Fielding, Managing Director, EMEA, Apricorn points out: “Every lost or unaccounted device carries a risk for those individuals whose data could be exposed”.

When it comes to personal data breaches, The House of Commons disclosed 49 incidents involving personal data during 2024, up from 41 the previous year. Despite these breaches, the House of Commons still doesn’t have to disclose such events to the Information Commissioner’s Office. The figure highlights the continued vulnerability of sensitive personal information within Parliament and other institutions.

Arguably more worrying still, several departments that had previously been open about incident reporting have declined to respond in full this year. The Ministry of Justice and Department for Education both refused to disclose details on data breaches and reports made to the ICO, citing exemptions under the Freedom of Information Act. Meanwhile, seven departments were yet to respond as we go to press including the MoD Police Force, British Army, British Navy, Royal Air Force, Royal Marines, UK Health Security Agency and Home Office/HM Passport Office.

Not only does this lack of transparency raise concerns about the true scale of breaches, but it also doesn’t set the best example for others to follow. Clearly, there is still much work to be done here...

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: June 2025

All rights reserved. No part of this publication may be reproduced in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without prior written consent of the publisher. Opinions expressed in articles or advertisements appearing in *intersec* are those of the author or advertiser and do not necessarily reflect those of the publication nor of its publisher.

CONTENTS

June 2025

www.intersec.co.uk

intersec

Features

7 DETECTING EXTREMIST PLOTS ONLINE
Dr Brenton Cooper explains why policing needs AI-driven open-source technology

8 AFRICA FIGHTS BACK
Jeanne McKinney explores the challenges of overcoming Africa's tyranny of distance to fight terror

12 URBAN SECURITY
Lucy Ketley explains the importance of having a focus on access control for public safety

16 ON THE BRINK
Matthew Borie explains the serious escalation in the ongoing India-Pakistan conflict

22 100 DAYS THAT SHOOK THE WORLD
Barry Zellen, PhD, reports on President Trump's grand strategy for a new American empire

28 SILENT POWER
Mark Findlay discusses the electrified future of the defence sector and how the industry can prepare for electric and hybrid vehicles.

30 RETAIL RANSOMWARE
Jon Bance urges CIOs to take control of their security awareness within their business and review their cyber controls before it's too late

32 MILITARY MINDSET
Tom Exelby reveals why SMBs need to change their thinking to combat the growing menace of ransomware

36 NETWORK PROTECTION
Tyler Gannon explains why securing hugely complex OT and IoT networks puts PAM technology centre-stage

Regulars

03	Leader
40	Incident Brief
42	News
48	Showcase
50	New Technology Showcase





SINGLE AND THREE-AXIS MAGNETIC FIELD SENSORS FOR INCORPORATION IN ACCESS CONTROL SYSTEMS

- Low-cost fluxgate sensors
- Measuring ranges from 100-1000 μ T
- Noise levels 10-25pTrms/ $\sqrt{\text{Hz}}$ at 1Hz

Mag690

Mag646/710

bartington.com
bartingtonshop.com

 **Bartington**
Instruments

MCQUEEN TARGETS

LIVE FIREARMS TRAINING TARGETRY

AIM FOR THE BEST.



CIVILIAN
TARGETS



MILITARY
TARGETS



POLICE
TARGETS



THREAT
ASSESSMENT



3-D FOAM
TARGETS



3-D FOAM
ACCESSORIES

Hit the mark every time with

MCQUEEN TARGETS

GALASHIELS, SCOTLAND



info@mcqueentargets.com

+44 (0)1896 664269

mcqueentargets.com

DETECTING EXTREMIST PLOTS ONLINE

Dr Brenton Cooper *explains why policing needs AI-driven open-source technology*

The foiling of an extremist bomb plot targeting the huge audience at a Lady Gaga concert in Brazil shows the value of open-source intelligence. The anti-LGBTQ extremists sought to radicalise teenagers online through digital cells, inspiring them to use improvised explosives in the attack against the estimated two-million audience. Brazilian authorities gained advance warning of the plot, which gave them time to intervene and arrest two people, preventing any potentially lethal casualties from occurring.

Reports say the extremists, used violent and self-harm-related content to build an online community of teenagers, employing coded language and extremist symbols. This use of violent, graphic content that attracts young people to extremist causes is a trend that threatens to overwhelm police authorities and intelligence organisations.

The problem for the authorities is dealing with the volume of material posted online, usually under pseudonyms and often on obscure platforms. Statista estimates 5.42-billion people will use social media this year, generating a huge volume of data.

Problems are amplified by a lack of moderation on many platforms and algorithms that help spread content, leaving authorities to determine whether those posting malicious material are part of a wider group and what their aims are.

Intelligence teams must also keep up with the changes in platforms that extremists use, which include 4chan, 8chan/8kun, Discord, Telegram, TikTok, WeChat and Weibo. The 'chan' sites are often home to the far-right, providing anonymity for users to share radical beliefs.

The task of analysing this information from fast-emerging groups with little formal structure is substantial and often beyond the resources of policing or counter-terrorism analysts. The volume and velocity of online data growth is too great for human capabilities. Many policing organisations only have embryonic open-source intelligence (OSINT) capabilities and therefore cannot afford to employ an army of fully trained open-source data analysts.

To filter and analyse this mass of data at scale and speed, organisations must adopt more advanced technology. Automation saves analysts days of manual data analysis. AI-powered, OSINT tools are purpose built for detection of extremist content and can use analytics to establish connections between individuals and groups. Without requiring expertise in data science or data-management, intelligence teams can configure AI-enabled risk detectors to uncover content relevant to their investigations across publicly and commercially available information. The technology will map online entities and establish links between threat groups and extremist ideologies, creating a new set of vital capabilities.

Combined with other forms of human and traditional classified intelligence, OSINT technology provides vital



insights that teams wouldn't be able to extract themselves. It goes beyond keywords to assist in analysing images, videos, memes, posts and other forms of multimedia content. Advances in OSINT algorithms enable solutions to keep up with the changes in the meaning of online jargon or symbols as threat groups adopt them. If the technology cannot reveal the main entity behind content, associates with online links can often be identified through the power of analytics.

Policing intelligence teams can store video from multiple accounts, reviewing material as required – a critical advantage when groups may post content and then quickly take it down in a bid to thwart detection.

Well-honed capabilities highlight not only content, but also suspicious patterns of behaviour, establishing levels of engagement and probable goals. Such insights would never otherwise be attainable. Platforms using OSINT algorithms detect text in images through optical character recognition technology and can deploy sentiment and emotion analysis and smart prioritisation cuts out noise, allowing augmented intelligence to enhance human decision-making. This means that no time is wasted once human intelligence officers believe the evidence suggests a high likelihood of a plot.

Once investigators are on the trail of a plot or believe online extremists are actively seeking to recruit, OSINT technology can expand the search across many diverse online data sources, including the Dark Web, marketplaces, people databases, watch lists and curated datasets of known threat groups.

As the frequency of new threats grows and more young people are at risk of exposure to extreme content, policing organisations need advanced open-source social media intelligence technology to supercharge their own intelligence skills and experience. Benefiting from automation and highly sophisticated algorithms, AI-driven open-source intelligence platforms are set to play a vital role in protecting our youth and communities at large from the scourge of online extremism ●

Approximately 2.5-million people attended the free concert held on Copacabana Beach

Dr Brenton Cooper is CEO & Co-founder of Fivecast.



AFRICA FIGHTS BACK

Jeanne McKinney explores the challenges of overcoming Africa's tyranny of distance to fight terror

Stabilising is a tall order on a large continent with many crises happening at once within the nation states. When it comes to Africa, it is not only about countering terror groups but also deterring malign actors like China and Russia seeking dominant influence through economic, political or military power. Each African country has its own culture and way of doing things. How can one organisation help support the critical security needs of such a diverse collection of independent states?

Ask AFRICOM, whose area of responsibility (AOR) encompasses all of Africa except for Egypt. It tells us what terror groups and other security challenges it

currently faces that threaten the US homeland, forces and interests. In Africa – the US gives a lot to sustain the survival of irreplaceable African resources – mainly its people who deserve to live a life free of terror, free of hunger and displacement. The African people deserve to benefit from the land of their ancestors. There is no continent in the world like Africa and it has a lengthy list of bad guys leaving a bloody trail to extort what is not theirs in the most violent ways possible.

In the East, al-Shabaab in Somalia has a presence and is a long-standing security challenge. Moving West into the Sahel, Jama'at Nusrat ul-Islam wa al-Muslimin (JNIM) is operating, an affiliate of al-Qaeda. Various Isis-linked groups, including Isis-Somalia and Isis-Sahel are also driving armed conflict and inter-communal



AFRICOM's logistics planners and leaders are in a constant state of honing plans to get people and equipment where it is most needed

violence. In central Sahel, Burkina Faso, Mali and Niger populations are getting hit with al-Qaeda's JNIM and the Islamic State Sahel Province.

"Armed Islamist groups perpetrate recurrent abuses and attacks against civilians. These groups systematically use sieges, threats, kidnappings, improvised explosive devices (IEDs) and landmines as deliberate tactics of war as they seek to control supply routes and increase areas of influence. They have also enforced their own interpretation of Sharia law in areas under their control, imposing severe gender discriminatory rules," reports the Global Centre for the Responsibility to Protect.

"AFRICOM promotes African-led stability and supports our partners' efforts to defeat these terrorist organisations through security cooperation, exercises and disaster preparedness. In short, our activities support the growing effectiveness of our African partners' efforts against terrorism, which in turn forestalls the growth and metastasis of these groups' efforts to the homeland," says AFRICOM spokesperson, LTC Douglas Halleaux, US army.

While foreign collaboration can be a deterrent as well as both air and ground operations assist, the inner political conflicts cannot be effectively controlled by force. Stability and prosperity may have to rely on non-combatant foreign engagement from the US State Department through their embassies to promote non-lethal solutions and cooperative agreements. Yet when those African states are not prepared for insurgencies and/or disloyal factions fuelled to overthrow, it is a fireball that sometimes requires emergent interactions from foreign forces trained and ready to act with regional forces.

"On January 29, 2025, the Economic Community of West African States (ECOWAS) published an official press release announcing the exit of Burkina Faso, the Republic of Mali and the Republic of Niger from the coalition." These three states formed the Alliance des États du Sahel (AES), or Alliance of Sahel States [their own defence pact]," states Georgetown Security Studies Review.

The political fracture has led to regional security deterioration, a loss of democracy in the Sahel and alienation to the "liberal international order."

"Of the last seven successful coups in Africa in the past three years, five occurred within the three AES member states."

"AES states have eviscerated ECOWAS for its ties to formerly colonialist Western powers, preferring the cultivation of less "invasive" relationships with Russia and the People's Republic of China (PRC). AES members have blamed ECOWAS for many of the region's woes," reports Georgetown Security Studies Review. Yet are they seeing the writing on the wall when it comes to China or Russia?

AES expulsions of Western security backers like the US and France "have left societies in these countries largely undefended from jihadist expansion. Attempts to replace Western cooperation with Russian Wagner mercenaries have failed to stem the violence. . ."

continues Georgetown Security Studies Review, adding: "Russian presence in the Sahel has intensified these conflicts – Wagner mercenaries are notorious for committing human rights violations and atrocities against civilians, potentially legitimising jihadist and

insurgent militias' influence on local populations." Although AFRICOM currently does not have activities in Burkina Faso, Mali and Niger, it is busy elsewhere when either their commander-in-chief calls on it or a State Department need arises. Instability in one place on the huge continent can and does expand to cause more destruction and death.

AFRICOM has been working with regional governments and forces since it "became fully operational capable on 1 October, 2008. A full-spectrum combatant command, US AFRICOM is responsible for all US Department of Defense operations, exercises and security cooperation on the African continent, its island nations, and surrounding waters." (Patriot Profiles)

AL-SHABAAB HAS A PRESENCE IN SOMALIA AND IS A LONG-STANDING SECURITY CHALLENGE

US Africa Command covers 53 African states, more than 800 ethnic groups, over 1,000 languages, vast natural resources, a land mass that is three-and-a-half times the size of the US, with nearly 19,000 miles of coastland. (AFRICOM)

Spokesperson LTC Halleaux relays that AFRICOM partnerships are key for fast, effective crisis response across the continent. Host nation governments that support logistics movements mean the difference of hours in response time, depending on where chaos suddenly erupts. Then there is ongoing chaos to disrupt, deter and disable. The Director of National Intelligence describes Somalia's problems with the al-Shabaab terror network: "al-Shabaab has claimed responsibility for many bombings – including various types of suicide attacks – in Mogadishu and in central and Northern Somalia, typically targeting Somali government officials, AMISOM and perceived allies of the FGS. Since 2013 al-Shabaab has launched high-profile operations in neighbouring countries, most notably the September 2013 Westgate mall attack in Nairobi, the May 2014 attack against a restaurant in Djibouti popular with Westerners and the April 2015 massacre of university students in Garissa, Kenya. The Westgate attack killed 67 Kenyan and non-Kenyan nationals and a siege continued at the mall for several days. The Garissa attack killed some 150 mainly Christian students." (DNI)

In 2011, al-Shabaab was responsible for blocking some Western relief aid during a virulent famine that killed Somalis by the tens of thousands. al-Shabaab (a clan-based insurgency) operates with plenty of money. "Cutting off al-Shabaab's estimated \$100-million in extortion-generated annual revenue will require restoring the integrity of Somalia's compromised financial, judicial and intelligence agencies," reports the Africa Centre for Strategic Studies, 2023.

"In 2018, American forces, in coordination with the Federal Government of Somalia, conducted a military air strike in self-defence against al-Shabaab militants," US Africa Command stated. The 21 September strike was undertaken after US and

Somali partner ground forces came under attack by al-Shabaab.

“US AFRICOM assessed eighteen terrorists killed in the strike. Somali forces killed two other terrorists with small arms fire during the confrontation. No US or Somali forces were killed or wounded in the attack,” said AFRICOM spokesman, Nate Herring, as reported by AP. “No civilians were injured or killed because of the air strike.”

UNFORTUNATELY INNER POLITICAL CONFLICTS CANNOT BE EFFECTIVELY CONTROLLED BY FORCE

At that time, al-Shabaab had been fighting to overthrow the UN-backed government for over a decade, conducting lethal attacks with bombs and guns. (Patriot Profiles)

Seven years later AFRICOM is still working with the Federal Government of Somalia and Somali Armed Forces, targeting Isis, the newer terror game in town.

On 25 March, 2025, AFRICOM released news of an airstrike targeting Isis-Somalia. The airstrikes occurred in the vicinity of the Golis Mountains with AFRICOM stating: “Isis-Somalia has proved both its will and capability to attack US and partner forces. This group’s malicious efforts threaten US security interests.”

AFRICOM also overcomes the tyranny of distance “through careful, deliberate planning in conjunction with our colleagues at our adjacent US Combatant Commands, the US State Department, and our allies and partners who also have equities in Africa,” says Spokesperson LTC Halleaux.

AFRICOM’s logistics planners and leaders, widely considered some of the best in the world, are in a constant state of honing plans to get people and equipment where it is most effective to support the mission at hand. The components of these plans are tested regularly to help warfighters become familiar with the details.

There are currently approximately 6,500 US Africa Command personnel – military, civilians and DoD-funded contractors – on the continent on any given day. They are all working diligently to stop violent extremists wherever they touch down on Africa.

On 3 April, 2025, USMC Gen Michael E. Langley, Commander, US Africa Command, addressed the intent and goals towards strategic competitors like China and Russia. Standing before the Senate Armed Services Committee he described “the Chinese Communist Party intent on using Africa to become the global hegemon and a Russian Federation that seizes opportunity created by chaos and instability.”

“In order to protect our homeland and United States’ interests. We must deter these nations and their malign actors from their goals on the African continent.” That takes clear threat assessment, a network of like-minded allies, and appropriate military resourcing ●

Jeanne McKinney

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

General Michael Langley visits a Somalia outpost to engage with US and partner troops



Picture credit: Lt. Cmdr. Bobby Dixon

SAVE THE DATE

**18-21
NOVEMBER. 2025**

PARIS NORD VILLEPINTE

MILIPOL PARIS



**Leading Event for Homeland
Security and Safety**

COMEXPOSIUM

www.milipol.com
X in  [#MilipolParis](https://twitter.com/MilipolParis)



URBAN SECURITY

Lucy Ketley explains the importance of having a focus on access control for public safety

It has been nearly 50 years since the famous psychologist from Stanford - Philip Zimbardo - launched one of the most influential theories of criminology; the 'Broken Windows Theory'. In his field study, Zimbardo abandoned two identical cars in two very different neighbourhoods. One within a notoriously crime-ridden area of New York City and the other in an affluent neighbourhood - Palo Alto in California. Both cars were parked with their number plates removed and the bonnets open.

Within ten minutes of the cars being placed within New York City, the first was gradually stripped of its spare parts and vandalised; meanwhile the second remained untouched for over a week. Eventually, Zimbardo took a sledgehammer to the car located in California and only then did passers-by give the car the same treatment as in New York City. This theory demonstrated how something which is clearly neglected can quickly become a target for criminality; this became the 'Broken Windows Theory'.

This same theory can be applied to the wider community and urban areas. In a study of over 400



Understanding the different pieces and knowing how they come together in a coherent security plan is the best way to ensure area has adequate protection

convenience store robberies, one significant difference between stores which had been targeted and those which had remained untouched was the distance from the nearest graffiti.

Whatever the security expertise; be it physical security, surveillance or cyber security, one of the most important factors of ensuring an urban area or community is safe for pedestrians and residents is crime prevention through environmental design. The three questions you need to consider when assessing the environmental design of an area from the perspective of a criminal: will I be seen (surveillance); can I get in and out easily (access) and, does anyone care what happens to the area/target (territoriality)?

If criminality won't be detected, it is easy to conduct. If no-one really cares about criminality happening, the target will be significantly more vulnerable than an area which utilises surveillance, security measures (if appropriate) and presents as being an area where care is taken. Not only can security products such as physical access control barriers help to provide a visual deterrent, but they can also add to the aesthetics and demonstrate the care taken within an area.

Access control barriers are a critical aspect of urban security and play a fundamental role in providing a visual deterrent as well as a working, proven and tested vehicle barrier – protecting against vehicle as a weapon and vehicle-borne improvised explosive device attacks. Behind a physical access control barrier, you will find software, an access control methodology, surveillance protocols and other visual accessories such as traffic lights and signage to inform system interaction.

Having the right combination of physical products, supporting access control software and hardware as well as the 'know-how' to use them correctly will augment the security system and provide the best level of protection for any urban area. Understanding the different pieces and knowing how they come together in a coherent security plan is the best way to ensure that an area has adequate and proportional protection.

As with any other aspect of urban security, the first stage is always careful planning. Before knowing how to implement an effective plan, an all-inclusive site assessment will need to be conducted, involving all relevant stakeholders and identifying potential access points and vulnerabilities needing to be addressed. This site assessment should look at every potential vulnerability including the uses and potential future uses of the urban zone in question, as well as the surrounding areas. This of course from the perspective of an attacker – ignoring sentiments such as one-way streets for example.

One of the main reasons for performing a thorough site assessment early in the process is to design plans that work effectively. By identifying every potential weak point and vulnerability being addressed by physical access control systems (and ascertaining how they integrate into a wider urban security plan), a project is less likely to require later adaptations and therefore likely to stay on budget and be more effective long-term.

Security objectives must be clear, areas can be protected using a layered approach. For instance, areas which are constantly subjected to high pedestrian footfall and have a heightened risk of attack are likely

to require a permanent protection strategy. Areas used for events might only require protection measures for a short duration. If these events are rare, temporary security measures may be more appropriate. If events happen regularly and within the same urban spaces, a semi-permanent security strategy might be advisable.

Behind each physical access control system is an operating methodology. Without secure protocols to make sure that the physical security solution works as well as it can, the whole thing falls apart and exposes vulnerabilities. After all, any security system is only as strong as its weakest link.

REGULAR SERVICE AND MAINTENANCE ENSURES SECURITY EQUIPMENT FUNCTIONS AS IT SHOULD

When it comes to designing operating methodology, considerations include, establishing parameters for entering and exiting an area; implementing strict procedures to ensure correct system use; the implementation of authorisation mechanisms, such as cards, biometrics or PIN codes – proportionate to the level of security necessary and finally, creating a hierarchy of access privileges based on roles and responsibilities of different stakeholder groups. The final step, but far from least important in access control strategies is continuous monitoring and surveillance.

Deploying surveillance cameras at access points not only assists stakeholders such as the emergency services, but also provides supporting evidence for any unauthorised access attempts, adding to security surveillance strategies. Having adequate and proportionate surveillance systems in place will assist in keeping an audit trail if necessary and provide real-time evidence should it be needed in the event of security breaches.

It is important to consider the regulations and standards that are needed when designing and specifying a physical access control system. If the system is being utilised for hostile vehicle mitigation, the physical barrier chosen will need to comply with internationally recognised impact test standards (ISO 22343, IWA 14-1 or BSI PAS 68). The relevant risk profile should be highlighted during site assessment stage, which in turn will inform the security rating required on any mitigation products being planned. Manufacturers should be able to share all relevant testing results and criteria for any products proposed.

In addition to the physical barrier being appropriately rated, the operating systems/protocol behind the barrier should also meet the relevant standards. This applies when placing an automatic system into a public highway and is also applicable to any monitoring systems to ensure the right security credentials are in place to prevent perpetrators from accessing software to circumvent physical security systems.

When specifying physical access control equipment, it is often the case that additional physical

components which are fundamental to operation are forgotten about or overlooked. In addition to the physical barrier (certainly when placing such systems within a public highway), a cabinet to house the hydraulic pump unit (HPU) and the system PLC is required and should be placed (ideally) within 25 meters of the physical access control system. Traffic lights and warning signs are also required to ensure safe system transactions. These additional elements require thought, careful placement and possibly some security as standalone items (LPS 1175 for example) to ensure systems are not able to be compromised.

ACCESS CONTROL BARRIERS PLAY A VITAL ROLE IN PROVIDING A VISUAL DETERRENT

Following the completion of specification and system design, plans that have been developed can be implemented which involves planned execution and installation. Once installed, it's important to think about maintenance. Developing a strict maintenance and inspection schedule is crucial for keeping physical access control systems running smoothly, especially as they contain a multitude of moving parts. A regular service and maintenance regime ensures that security equipment is functioning as it should. Bollards, for example, need to raise and

lower properly; regular checks can therefore identify any issues that might affect this, such as mechanical failure or corrosion.

Malfunctioning equipment can seriously compromise security. For instance, if a bollard does not deploy when needed due to poor or non-existent servicing, unauthorised vehicles could gain access to areas that are supposed to be secure. This can, potentially, highlight site / area vulnerabilities and put people at risk. By contrast, well-maintained physical access control equipment enhances security and ensures greater effectiveness. Guaranteeing that bollards and other security measures are in optimal condition heightens the visual deterrent to threats and the care being put into an area (going back to the prelude 'Broken Windows Theory').

Training is a key part of correct system use. Physical access control systems rely on making sure that the stakeholders using the equipment are familiar with the products and the systems to an intimate degree, and part of that is educating the users to ensure operating protocols are followed. Again, a physical access control system is only as secure as its weakest link and sometimes, sadly, this is the user itself. Invariably, you cannot completely design out 'human error.'

Urban security plays a proactive role within the care and consideration of an area, positively contributing to a public realm that the community and residents can be proud of. Measures implemented should be layered and plans should be designed to prevent criminality, further enhance the aesthetics of an area and provide a safe place for people to live, visit and work without fear ●

Lucy Ketley is Sales & Marketing Director at ATG Access Ltd.

It is important to consider the regulations and standards that are needed when designing and specifying a physical access control system



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

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

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

Kestrel TSCM® Professional Software | Kestrel® SIGINT Professional Software

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

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

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

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

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

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

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



Kestrel-net™
Actionable RF Intelligence



www.kestreltscm.com



United Kingdom & European Union Master Distributor

VILUTION
Your vision, Our solution



Professional Development **TSCM** Group Inc.

www.kestreltscm.com

www.pdtg.ca

www.ctsc-canada.com

ON THE BRINK



Matthew Borie *explains how events in late April led to serious escalation in the ongoing India-Pakistan conflict*

On 22 April, a shooting attack by suspected Pakistani-linked militants killed 26 civilians in the Indian-administered Kashmir region. This was the largest number of civilian deaths in a terrorist attack in Indian-administered Kashmir since the May 2006 Doda massacre, and the largest number of casualties in any attack in Indian-administered Kashmir since 14 February 2019. India responded initially with a set of diplomatic measures as announced by the Ministry of External Affairs on 23 April and Pakistan reciprocated on 24 April. The Indian prime minister reportedly stated on 29 April that he has: “complete faith and confidence in the professional abilities of the armed forces” and: “it is our national resolve to deal a crushing blow to terrorism”. Pakistani defence officials have reportedly denied any involvement in the 22 April attack and blamed it on Indian “homegrown terrorists”.

On 10 May, Pakistan and India reportedly reached an immediate and full ceasefire agreement – to include along the Line of Control (LoC) separating Pakistani-administered Kashmir and Indian-administered Jammu &

Kashmir as well as the entire shared border – reportedly brokered by the US following armed clashes from 6-10 May. From 13-22 May, there have been no ceasefire violations reported between India and Pakistan, and the agreement continues to hold. India stated on 18 May that the ceasefire agreement with Pakistan has no expiry date.

Both India and Pakistan have said they will abide by the ceasefire, but have vowed to respond to any violations should they occur. Pakistan has stated that the ongoing Indian suspension of the Indus Waters Treaty puts the ceasefire at risk, but has not indicated what a response to the ongoing abeyance will be. The US, Canada, UK, Australia and France issued travel security advisories to their citizens in India in the wake of the above activity and the 22 April terrorist attack.

INDIA-PAKISTAN CONFLICT: KEY EVENTS FROM 6-12 MAY

On 12 May, the Indian Army stated that a “small number of suspected drones have been observed near Samba” near LoC in Indian-administered Jammu & Kashmir and that: “they are being engaged” by air defences. In addition, on 12 May, the district commissioner of Jalandhar in India’s Punjab state said that: “one surveillance drone was



Police in Kashmir clash with protestors in December 2018

brought down by the armed forces". No casualties or material damage have been reported.

No ceasefire violations were reported on 11 May; however, violations did take place on 10 May. Indian air defences reportedly shot down at least 12 Pakistani military drones in breach of the ceasefire over Jammu & Kashmir region near the LoC as well as further South along the shared border over Rajasthan and Gujarat states on 10 May. Pakistan reportedly shot down multiple Indian military drones in breach of the ceasefire over Peshawar in Khyber Pakhtunkhwa province on 10 May. Armed clashes with small arms and mortar/artillery fire were also reported sporadically along the LoC in wake of the ceasefire on 10 May.

The security situation along the entirety of the India-Pakistan border remains fluid and subject to rapid change. Prior to the ceasefire on 10 May, the Indian military reportedly launched drones at Pakistani Air Force (PAF) Base Sargodha (OPMH/MSF) in Punjab province, PAF Base Sialkot (OPST/SKT) in Punjab province, PAF Base Sukkur (OPSK/SKZ) in Sindh province, PAF Base Shahbaz (OPJA/JAG) in Sindh province and PAF Base Bholari in Sindh province as well as PAF Base Peshawar (OPPS/PEW) in Khyber Pakhtunkhwa province and Pakistani air defences were activated in response.

Overnight on 9-10 May, Pakistan reportedly launched ballistic missiles at Indian air bases in Jammu and Kashmir near the LoC as well as further South in Punjab, Haryana and Gujarat provinces, to include Beas near Amritsar, Adampur (VIAX/AIP), Suratgarh (VI43), Sirsa (VISX), Srinagar (VISR/SXR), Jammu (VIJU/IXJ), Udhampur (VIUM) as well as Pathankot (VIPK/IXP) and Indian air defences were activated in response. In addition, on 10 May, Pakistan reportedly launched drones at areas of Jammu and Kashmir along the LoC as well as further South in Amritsar, Rajasthan and Gujarat provinces and Indian air defences were activated in response.

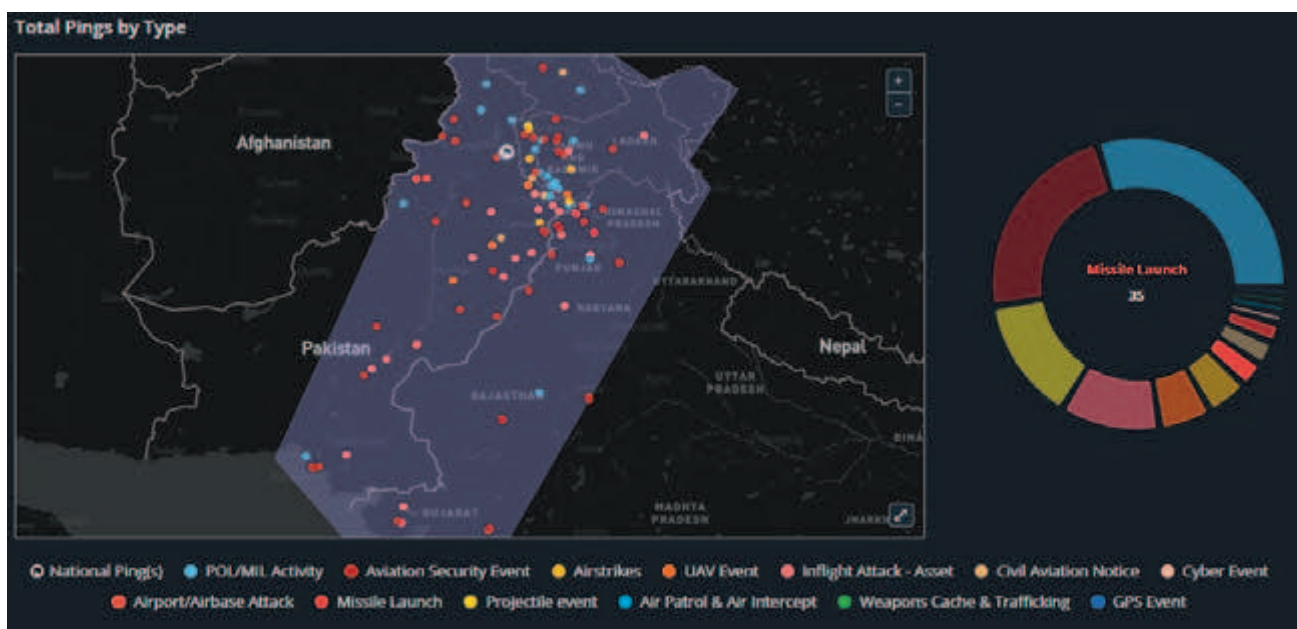
On 9 May, the Indian military reportedly targeted PAF Base Nur Khan (OPRN/RWP) in Rawalpindi, PAF Base Rafiqui (OPRQ) in Shorkot and PAF Base Murid in Chakwal with cruise missiles and air-defences were

activated in response. In addition, on 9 May, Pakistani air defences were reportedly activated in response to Indian drones over Lahore. On 9 May, India announced Pakistani military drone sightings at 26 locations along the entire Western border from Jammu and Kashmir along the LoC down to Gujarat province, with air defences activated in response. On 9 May, Pakistani air defence reportedly were activated in response to Indian military drones over several areas of Pakistani-administered Kashmir along the LoC as well as over several areas in Punjab province.

A FULL RESUMPTION OF ARMED CLASHES BETWEEN THE TWO COUNTRIES REMAINS UNLIKELY

Previously, on 8 May, the US State Department issued a security alert to its nationals in Pakistan stating the following: "Due to reports of drone explosions, downed drones and possible airspace incursions in and near Lahore, the US Consulate General in Lahore has directed all consulate personnel to shelter-in-place" and the: "Consulate has also received initial reports that authorities may be evacuating some areas adjacent to Lahore's main airport [(OPLA/LHE)]". Overnight on 8-9 May, India stated that Pakistan attempted to conduct around 50 missile and drone attacks on military targets along the entire Western border and that it had employed air defence systems in response to the incoming strikes. This activity reportedly occurred in areas stretching from Jammu and Kashmir near the LoC to Southern Rajasthan province.

India previously stated that overnight on 7-8 May, Pakistan attempted to conduct missile and drone attacks on military targets stretching from along the LoC to Gujarat province and that it had employed air defence systems in response to the incoming strikes. Also on 8 May, India claimed it has conducted strikes targeting Pakistani military air defence systems at a number of locations in Pakistan, to include Lahore. On



8 May, Pakistani air and/or air defences reportedly shot down around 25 Indian military drones over an area stretching from Jammu and Kashmir near the LoC to Sindh and Punjab provinces.

Previously, on overnight on 6-7 May, the Indian military confirmed conducting strikes on the following nine locations in Pakistan from near the LoC to areas well further south in Punjab province. Pakistan has claimed that its air and air-defences shot down five Indian military combat aircraft, including four over areas near the LoC as well as India's Punjab province well further south on 6-7 May. Pakistani air and defences also reportedly shot down two Indian military drones in areas along the LoC while Indian media reports claimed that one Pakistani combat aircraft was been shot down over Jammu and Kashmir on 6-7 May.

WHAT WOULD BE THE MOST LIKELY OUTCOME?

The security situation along the entirety of the India-Pakistan border remains fluid and subject to rapid change. The ceasefire holding thus far with no violations reported on 13-22 May is viewed by Osprey as an indicator of de-escalation. Osprey assesses that amid the ceasefire, allegations of further limited-scale violations are possible in the near term.

Osprey assesses that a full resumption of armed clashes – including unguided rocket/artillery fire, guided missile launches and airstrikes – along the LoC between Indian and Pakistani military forces are unlikely in the near term amid the ceasefire.

Osprey assesses that additional strikes by India and Pakistan in areas near the shared border in the countries' respective areas of the Punjab region, as well as in India's Rajasthan and Gujarat states and Pakistan's Sindh provinces, via guided missile launches and airstrikes are unlikely in the near amid the ceasefire.

Both India and Pakistan have military airbases with combat aircraft and air-defence units with conventional surface-to-air missile (SAM) systems operationally stationed in areas near the LoC and along the shared border. The conventional SAM systems and combat aircraft are capable of engaging targets at all altitudes. While unlikely, Osprey assesses that additional shoot-downs of military-grade air assets by both Indian and Pakistan air and air defences

INDICATIONS & WARNINGS

INDICATORS OF ESCALATION

- Ceasefire violations alleged by India and/or Pakistan
- Terror attacks by Pakistani-linked militant groups in Jammu and Kashmir region
- Terror attacks by Pakistani-linked militant groups in main urban centres of India
- Declaration of an end to the ceasefire by India and/or Pakistan
- Indian and/or Pakistani military forces announcing an increased alert posture
- Increased military aircraft and/or naval movements within India and/or Pakistan
- Increased GPS interference (jamming and/or spoofing) within India and/or Pakistan
- Airspace and/or airport closures in India and/or Pakistan

INDICATORS OF DE-ESCALATION

- Declaration of commitment to the ceasefire by India and/or Pakistan
- Direct and/or indirect diplomatic talks between India and Pakistan
- Airspace and/or airports reopening in India and/or Pakistan
- Decreased military aircraft and/or naval movements within India and/or Pakistan
- Decreased GPS interference (jamming and/or spoofing) within India and/or Pakistan
- Indian and/or Pakistani military forces announcing an decreed or normal alert posture
- India re-committing to the Indus Waters Treaty with Pakistan
- India re-opening the Wagah-Attari Border area with Pakistan
- Statements by Pakistani-linked militant groups that they will halt attacks in Jammu and Kashmir region
- Statements by Pakistani-linked militant groups that they will refrain from attacks in main urban centres of India.

– including via conventional SAM systems capable at all altitudes – in areas along the entire shared border are unlikely in the near term amid the ceasefire.

WHAT WOULD BE THE MOST DANGEROUS OUTCOME?

While unlikely, Osprey assesses that a conflict between India and Pakistan could extend beyond the LoC and encompass the entire border area through the medium term, should the current ceasefire fail to hold and should armed clashes between the countries return to 6-10 May levels.

Though unlikely, should the above occur, main urban centres in India's Punjab and Rajasthan provinces would be exposed to conventional military activity and Karachi, Islamabad and Lahore in Pakistan would be inside the conflict zone for an extended period of time in the medium term ●

Matthew Borie

is Osprey's Chief Intelligence Officer.

Osprey assesses that additional strikes by India and Pakistan in areas near the shared border are unlikely in the near future



MESA 2.0 Advanced WiFi Detection Just Got Better!

Detect, analyze and locate WiFi devices.

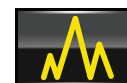
New
Firmware
Update
Delivers New
Capability.



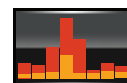
MESA^{2.0}
Portable Spectrum Analyzer

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

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



Spectrum View



SmartBars[™] (Patented)



Mobile Bands



WiFi



Bluetooth

FOR MORE INFORMATION CONTACT:

International Procurement Services (Overseas) Ltd

118 Piccadilly London W1J7NW

Phone: +44 (0)207 258 3771

Email: sales@intpro.co.uk

MESA[®] 2.0 hand-held Spectrum Analyzer

HEALD®

DESIGNERS, MANUFACTURERS AND INSTALLERS OF AWARD WINNING PERIMETER SECURITY PRODUCTS



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

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



@healduk



Heald Ltd



Heald Ltd



HealdLtd

FRONTIER PITTS

PROTECTING YOUR WORLD



WWW.FRONTIERPITTS.COM

+44 (0) 1293 422800

GATES » BARRIERS » BLOCKERS » BOLLARDS » PEDESTRIAN



HVM



«HOSTILE VEHICLE MITIGATION»

LPS I 175 - FORCED ENTRY

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

100 DAYS THAT SHOOK THE WORLD



Barry Zellen, PhD, reports on *President Trump's grand strategy for a new American empire*

Since triumphantly returning to the White House in January, Trump 2.0 has been a whirlwind of creative, innovative, paradigm-shifting American defence and security policy. Staggering in its vigour and bold in its willingness to take risks for what is hoped will be transformative gains. It's been one of the most exciting starts to a new presidential term since Gorbachev ascended to the pinnacle of the Soviet system and kept the West on its toes as Russia underwent its revolutionary transformation. It's been a wild ride in these first 100 days, with more turbulence expected in the weeks and months to come.

Indeed, the bold risks Gorbachev took in the end caused the entire Soviet system not to reform, but to collapse, both at home and abroad. Could we see the same happen to America? With Trump's 'Liberation Day' trade war starting off with a bang, world markets teetered on the brink of collapse with China briefly emerging (oddly enough) as a safe haven for much of the world, forcing a rethink and a slowdown of its rollout – suggesting a collapse of global order is

unlikely, and while a deceleration in its frenetic pace, hopefully not an end to this fascinating and courageous restructuring of the world economy and an historic and just rebalancing of trade with America.

As an old Arctic hand, it was both surprising and heart-warming for me to see the Arctic feature so prominently and centrally in American policy. This is both smart geopolitics for a warming world, and an ironic recognition of the deep, strategic impacts of climate change on world politics. But there is risk in hyping the wrong things in the Arctic, such as overstating the threat posed by China, which is not an Arctic state, or Russia, which is the largest Arctic state but one that is inherently defensive in its utilisation, development and ultimately its defence of its Arctic territories and waters – with the largest Arctic population, economy and territory, Russia has much more skin in the game and much more to lose in the event the region becomes destabilised.

The real and present danger to the Arctic is not posed by either China or Russia, but rather by internal gaps



Trump 1.0's approach to peace in Afghanistan is a guide for what we can expect next in foreign policy

in wealth, human development, cultural stress and marginalisation of its native peoples who have made great strides but who still find themselves to a large degree second-class citizens in their own homelands, whose powers while greatly expanded remain subordinated to the still largely colonial states that govern over them and their traditional territories. I've been writing about this fundamental risk to the Arctic's human terrain for decades, and to the importance of rebalancing state-tribe relations across the region and the world. President Trump, with his and Vice President Vance's direct appeal to Greenlandic Inuit to join America and leave their colonial existence behind them, understands that this internal fault line that runs across the entirety of the circumpolar Arctic is not only salient to the region's order, but increasingly essential to American and global security.

Looking ahead, we can be prepared for many more innovations to come. We can look forward to an end to America's own 'green colonialism' (a phrase I first heard from Greenlanders who have long opposed the EU's ban on seal products central to their local Arctic economies), and a more robust integration of Alaska's petroleum resources into America's growing energy independence, with more federal support for oil and gas development both on and off shore, and new mining ventures both in Alaska and perhaps, if Trump succeeds in his goal to integrate Greenland into America's constitutional polity, Greenland as well — joining Russia and the other Arctic states in their continuing efforts to develop their vast repositories of energy resources to meet their needs, enriching Arctic communities along the way. As for Greenland, we can anticipate continued creative and dynamic diplomatic engagement, with President Trump's instincts for strategic and economic opportunity aligning with the continuing polar thaw and converging with Greenland's own aspirations for continuing decolonisation culminating in, Greenlanders hope, their sovereign restoration and independence, and we Americans hope in their eventual constitutional union with America.

HOW MIGHT THIS PLAY OUT?

The conversation with Trump started with his territorial acquisition/statehood vision, and has been evolving from there toward support for Greenland's independence as his administration's relationship with Greenlanders grows, along with his desire to extend more robust American protection to Greenland — this is somewhat akin to how Trump 1.0 de facto evolved its views on Afghanistan, whose forever war Trump inherited and which despite two decades of mission creep and institutional momentum within the pro-war military-industrial-academic complex, he brought to an end. Trump found through peace negotiations with the Taliban that his administration and his political base (rooted in the MAGA movement) had ultimately more in common with their military opponent (the Taliban), as people of faith, than they did with America's own military ally, its very own (and very corrupt) client state that it had installed in Kabul 18 years prior.

As a change-making president with a mandate to "drain the swamp," Trump 1.0 internationalised this mandate and extended it not only to the forever war in Afghanistan where in the end it chose its opponent over its own client state much that way America did

after its long peace talks with the North Vietnamese in the Seventies. Trump 2.0 has taken its "drain the swamp" mission even further in both domestic politics and foreign policy, with the new Department of Government Efficiency (DOGE) purging federal payrolls by the tens of thousands while shuttering wasteful foreign aid programmes that propped up governments around the world as American taxpayers footed the bill for social and health programmes they are often denied, or couldn't afford, at home.

CHINA MAY BE UNWILLING TO ALLOW FOR SUCH A KINETIC REVISION TO THE WORLD'S BORDERS

Trump 1.0's approach to peace in Afghanistan is a guide for what we can expect next in foreign policy. Look no further than the new forever war in Ukraine, where a rapid and decisive peace favouring the Russian invader has become prioritised over a restoration of the territorial integrity of allied Ukraine. Indeed, finding common cause with Russia, perceived as a state that shares a commitment to traditional values, will allow for the restoration of global stability from Europe to Asia with Russia serving as a bridge of stability across the Eurasian heartland. And demanding a stake in Ukraine's mineral wealth promises to return to the American taxpayer some of the funds that were spent in Ukraine under the Biden administration, bringing economic justice to the American heartland. Moreover, Trump likes to test and provoke America's allies, and in his peace overture to Russia we see more of this.

And while China remains in many ways the American "bogeyman," with the heartland of America still recovering from the economic collapse that resulted from China's industrial rise and the intergenerational pain still fresh (having itself fuelled the rise to prominence of Vice President JD Vance), China and America share being two hard-working and innovative nations that have tamed much of their respective continents, stabilising their respective hemispheres to a large degree. In time, forging a lasting peace with China and ending the new cold war before it starts, and reintegrating our economies more equally and fairly, could cement Trump's legacy not only as one of the greatest dealmakers in history, but one of the greatest presidents as well. This will have to wait, of course, until the American heartland is ready to mend ties with Beijing, but Trump can show the way. Then, it won't be only Nixon who could go to China, but Trump as well. But that remains for later in the term.

IT'S NOT ALL PEACE AND HARMONY

As we see with Ukraine, a major world power (Russia) has changed the map of Europe and the price has been high in Ukrainian blood and American treasure. This may be just the beginning. Next, Greenland could become part of America, for a second redrawing of the world map. And, if America

wants to secure the Arctic and protect its own flanks, it may then have to expand its new Arctic territory in Greenland to also include parts of Canada's Nunavut territory sitting astride the Northwest Passage. This would be the third revision of the world map. And by the same logic that propels Trump's geopolitical interest in Greenland, we may see Russia emulate America's actions by taking Svalbard, Norway's remote, offshore archipelago that threatens Moscow's ability to project naval power beyond the Barents. But Norway, like Denmark/Greenland, is an integral part (and founding member) of NATO.

FORGING PEACE WITH CHINA AND ENDING THE NEW COLD WAR COULD CEMENT TRUMP'S LEGACY

Can the alliance survive both Denmark's loss of sovereignty over Greenland and Norway's loss of sovereignty over Svalbard? Perhaps so, as these islands are remote offshore possessions and not core constitutional parts of either Denmark's or Norway's traditional home territories, and the same can be said for the Northernmost parts of Canada's Nunavut, which were only settled in the mid-20th century as part of a Cold War relocation of Quebec Inuit to the High Arctic. Thus revising national boundaries to exclude these newly contested offshore island territories may well be achievable

without major war, as few Europeans will be willing to die to defend their nations' remote, colonial territories home to few residents and very limited industrial or strategic infrastructure.

China, for its part, may be unwilling to allow for such a kinetic revision to the world's borders without being part of this new wave of expansion – and this means ultimately that Taiwan will have to accept Beijing's sovereign control much the way that eastern Ukraine and Crimea will soon have to accept Russian control, and Greenland (and possibly Northern Nunavut) may soon choose to accept American control. More worrisome is if China and Russia agree to jointly take Hokkaido to protect essential sea lanes linking Chinese ports via the Northern Sea Route to European markets; it, too, is a remote island territory with a much briefer constitutional union with its sovereign partner, and thus not unlike Taiwan, and may thus find itself similarly contested. Being remote island territories with relatively small populations and limited infrastructure, major war seems unlikely and protracted or global war exceedingly so.

In one swift surge of territorial expansion, we may thus witness the formation of a new foundation for generations of stability to come, all precipitated by Trump's bold and innovative imagination and strategic prescience. Further down the pike, we could see these same re-expanding great powers finding common cause in dividing Antarctica into territorial concessions, thereby retiring the Antarctic Treaty with its multilateral, demilitarised vision of the world. But that's for another day ●

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

Unsurprisingly, Trump's presidency hasn't been popular with everyone...



Picture credit: Ted Eytan

MCQUEEN TARGETS

LIVE FIREARMS TRAINING TARGETRY

**AIM
FOR
THE
BEST.**



**CIVILAIN
TARGETS**



**MILITARY
TARGETS**



**POLICE
TARGETS**



**THREAT
ASSESSMENT**



**3-D FOAM
TARGETS**



**3-D FOAM
ACCESSORIES**

Hit the mark every time with

MCQUEEN TARGETS

GALASHIELS, SCOTLAND



targets.ukgal@sykes.com

+44 (0)1896 664269

mcqueentargets.com



ELECTRONIC COUNTERMEASURES

IPS EQUIPMENT & SWEEP TEAM SERVICES



**NEW REI MESA MOBILITY
ENHANCED SPECTRUM ANALYZER**



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



**VIDEO POLE CAMERA
2.0 INSPECTION TOOL**



**EDD-24T NON LINEAR
JUNCTION DETECTOR (HANDHELD)**



**TSCM TRAINING
COURSES &
CERTIFICATION
UK/US/GLOBAL**

Looking for a

For details, demonstrations, sales and 24/7 response, contact:
International Procurement Services (Overseas) Ltd,
118 Piccadilly, London, W1J 7NW Email: sales@intpro.com
Phone +44 (0)207 258 3771 FAX +44 (0)207 724 7925

Rapid Quote:

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



needle in a haystack?

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

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

TALAN 3.0 DIGITAL
PHONE ANALYSER

RAKSA IDET
SELECTIVE RF
DETECTOR (MICRO
TSCM DEVICE)

ORION 2.4 HX NON
LINEAR JUNCTION
DETECTOR



TSCM Equipment supply, training and de-bugging services

*The preferred choice of Government & Law Enforcement
Agencies worldwide.*



Web: www.intpro.com



SILENT POWER

Mark Findlay *discusses the electrified future of the defence sector and how the industry can prepare for electric and hybrid vehicles.*

For defence, electrification goes beyond sustainability – it's a catalyst for battlefield transformation. In an era defined by multi-domain warfare and dispersed operations, energy resilience, stealth and mobility are vital. The defence sector is undergoing rapid technological change. In the UK Government's 2025 Spring Statement, at least 10 percent of the Ministry of Defence's equipment budget was earmarked for emerging technologies – a clear signal of intent to modernise across all operational domains. While the spotlight falls on AI-enabled command systems, drones and advanced surveillance tools, one equally vital innovation is the electrification of land systems

Hybrid and electric platforms can reduce energy use on the battlefield. This means platforms can be present in theatre for longer, enabling greater survivability, enhanced manoeuvrability and logistical independence in complex and contested environments. By reducing reliance on fuel convoys, lowering acoustic and thermal signatures and supporting flexible mission profiles, electrified vehicles are set to redefine how military operations are conducted,

unlocking a new level of capability for modern forces. So, how can electrified vehicles support the defence sector?

STEALTH AND SIGNATURE REDUCTION

Electrified vehicles bring a critical tactical edge: stealth. Traditional military vehicles powered by internal combustion engines are noisy and produce heat signatures detectable by infrared and thermal imaging. Electrified drivetrains, on the other hand, can be much quieter and emit considerably less heat when required.

This directly enhances silent watch capabilities, which are critical for reconnaissance, surveillance, and covert insertion missions. Forces can remain stationary or move slowly without compromising their position. Electric powertrains allow troops to approach enemy positions with a significantly lower risk of detection, increasing the probability of mission success and survivability in hostile environments.

While this advantage is most obvious in special operations, it applies equally to armoured vehicle patrols, logistics resupply and combat vehicle manoeuvres, especially in the context of modern asymmetric warfare where surprise and stealth often determine outcomes.



Mark Findlay is CEO at Drive System Design.

An all Terrain Electric Mission Module (ATeMM) trailer pushing along a squad carrying vehicle

FLEXIBILITY AND POWER EFFICIENCY

Electrified propulsion systems provide an unprecedented level of tactical adaptability. Hybrid vehicles can intelligently switch between propulsion modes (internal combustion or electric) based on mission needs, terrain and energy availability. This ensures optimal energy usage, enabling vehicles to operate more efficiently and for longer durations, even in fuel-limited conditions.

This dual energy offers commanders greater choice in how and when energy is used during missions. For instance, a hybrid vehicle can rely on its combustion engine during high-demand activities or long-range transit, while switching the combustion engine off for silent watch and stealth manoeuvres.

Advanced hybrid architectures may also incorporate integrated starter/generator (ISG) systems, enabling a seamless and near-instant transition from a stationary electric state to internal combustion power. This is particularly advantageous when quick repositioning or rapid engine activation is required.

PERFORMANCE ON DEMAND

In some configurations, particularly parallel hybrid systems, a 'boost power' mode allows the electric motor and internal combustion engine to operate simultaneously. This delivers instant torque, which is especially valuable for rapid acceleration or climbing steep terrain. In dynamic combat scenarios, this capability provides a vital performance edge, supporting fast tactical movements and responsiveness under load.

MOBILE POWER SUPPLY FOR THE BATTLEFIELD

Modern defence vehicles must power more than just their own movement. Communications gear, advanced sensor suites and even directed energy systems need significant onboard energy. This capability helps detach tactical units from fixed power infrastructure, enabling more agile operations. Electrified fleets become decentralised power sources, crucial in modern warfare where rapid movement and dispersed operations are the norm.

ENHANCING FUEL RESILIENCE

One of the biggest vulnerabilities on the battlefield is fuel supply. Traditionally, a sizeable portion of military logistics is dedicated to transporting and protecting fuel and ammunition convoys, a critical but exposed element of support operations. Electrified vehicles reduce this dependency.

Hybridisation enhances operational endurance and effectiveness by eliminating the need for idling engines, while providing electrical power at inefficient operating points of the combustion engine. This energy autonomy maximises time in theatre, increasing resilience if supply lines are disrupted and reducing exposure to enemy attacks on fuel infrastructure.

Successfully integrating electrified vehicles into the defence landscape will require a broad shift in thinking and planning. The benefits are significant, but they come with challenges that must be addressed across multiple fronts.

SYSTEM-LEVEL OPTIMISATION

Electrification is not a static upgrade, it's a dynamic, evolving system. As new battery technologies, power electronics and thermal management solutions emerge, defence vehicle designers must constantly re-balance

key system attributes such as weight, endurance, power output and survivability and keep in mind the requirement for proven trustworthy technologies.

Fuel cells also represent a promising addition to hybrid architectures, either complementing or replacing traditional battery systems. They offer the potential for extended range, rapid refuelling, and low acoustic and thermal signatures, making them especially valuable for missions where endurance and stealth are critical.

ADVANCED SIMULATION TECHNIQUES

Advanced simulation techniques like digital twins, virtual models of physical systems that replicate performance in real-time, can help evaluate and optimise these trade-offs. So, it ensures vehicles are configured for the demands of each mission type while maximising efficiency.

CROSS-SECTOR COLLABORATION

Realising this transformation will also demand deep collaboration across the defence ecosystem. OEMs, system integrators, technology startups, energy providers, and armed forces must work together. Not only to develop electrified vehicles, but also to create the standards, cybersecurity frameworks, and interfaces needed to make electrification scalable and secure.

This collaboration must go beyond just infrastructure. It should involve shared R&D initiatives, upgrades and maintenance, dual-use technology programmes and co-investment strategies that accelerate the adaptation of proven commercial technologies for military use.

STRATEGIC INVESTMENT

Government investment is a powerful enabler, but the industry must take the lead in embedding electrification into the very foundation of defence planning. Electrification is not just about acquiring new vehicles. It's about rethinking how defence forces move, fight and sustain operations.

It should be viewed as a core part of long-term force modernisation, rather than an optional or experimental programme. That includes prioritising technology transfer from the civilian EV sector, leveraging experience in battery systems, thermal management and drivetrain control architectures that can be hardened and adapted for defence conditions.

The transition to electrified defence vehicles is both a strategic imperative and an operational upgrade. From enhanced stealth and mobility to decentralised power and reduced logistical burden, electrification unlocks new capabilities for 21st-century warfare.

Tomorrow's battlefield will demand greater agility, resilience, and autonomy. Electrified platforms will form the backbone of this transformation, enabling silent manoeuvres, energy independence and seamless tech integration.

Our challenge will be to repower our existing fleet of platforms, which have internal combustion engines that have not been designed to accommodate hybridisation. We anticipate that there needs to be significant advances in the development of internal combustion engines, to allow package space for hybrid components. The time to act is now. With the right investment and collaboration, the UK can lead this global shift - building a defence force that is smarter, stronger and more sustainable. The future of defence mobility is electrified ●

RETAIL RANSOMWARE

Jon Bance *urges CIOs to take control of their security awareness within their business and review their cyber controls before it's too late*

Recent headlines have put the spotlight on an escalating cyber trend targeting the retail sector and UK companies are being reminded that vulnerabilities can have a tangible impact on day-to-day operations. Harrods recently confirmed it had: “experienced attempts to gain unauthorised access” to its systems, prompting its IT security team to take immediate action. This follows the attack on Co-op’s IT system and disruption at Marks & Spencer.

From human error to the security policies of organisations’ service providers, these cyber incidents not only highlight the growing sophistication of threats targeting major retailers, but also expose the web of risk that can be prevalent in every business’ IT ecosystems.

Marks & Spencer estimates the cyber attack will cost it around £300-million and the IT shutdown of Co-Op has left empty shelves that will affect revenue. No matter how prestigious brands are, none are immune to digital threats.

As cyber attacks become more common, CIOs need to pump even more time and effort into reviewing their plans and ensuring their systems are as robust as possible. Safeguarding against cyber attacks must be a continuous, forefront goal that the National Cyber Security Centre and Cabinet officials are now emphasising as a business priority.

Coordinated with C-suite functions, business leaders should prepare for the eventuality with cyber strategy and tool adoption. The temptation may be to pull all resources towards recovery, but it’s paramount for CIOs to take a strategic leadership role in guiding the business to invest where it matters – cyber security. This involves patch cycles and strengthening their reporting procedures and awareness training to prevent any security fallout.

In these fast-evolving times, the benefits of staying informed – whether it’s fixing vulnerabilities or updating business cyber hygiene practices – are huge. A brief check-up on your systems can go a long way in strengthening digital defences. The best approach is a proactive one involving regular audits including increased vulnerability scans, review of firewall logs and rules, internal systems scan, updated software and patch testing to ensure all crisis management strategies are supported. It’s not enough to only have layers of firewall and unbreakable software – the best defence is educating the people in the business.

Cyber groups often exploit human error rather than technical flaws, using tactics like phishing and impersonating IT staff to gain access. Remote and hybrid workers are prime targets as they often operate without the protections of on-premise security controls; therefore, retailers must invest in training employees, from the supply chain to both on-site and off-site workers.

The training that is delivered must be relevant to the risks these employees may face specifically, with continuous refreshers to address new threats. Accompanied by business measures such as mandatory password changes and using two-factor authentication, this targeted training can help



employees recognise these tactics and create meaningful behavioural change.

Retailers may also rely on third-party vendors for services, but CIOs in the retail sector need to implement comprehensive risk management frameworks for these third-party services to mitigate threats. The retail industry is one of the sectors that is highly dependent on suppliers for payment processing, customer support, raw material sourcing and much more, but are CIOs prepared to meet that risk with a business strategy across vendor ecosystems?

The attack on M&S is a clear example of hackers exploiting third-party relations to reset passwords, granting unauthorised access to internal systems. This incident highlights how vulnerabilities within third-party systems can serve as entry points for cyber criminals thus, a third-party due diligence programme needs to be in place to meet regulatory challenges and increase transparency.

Regularly evaluating the security posture of third-party vendors through audits, performance reviews and monitoring tools can identify any potential vulnerabilities and collaborating with vendors to develop joint incident response plans can ensure swift, coordinated actions in the event of a breach. Better visibility into all these areas helps CIOs proactively handle risks that are otherwise overlooked due to complicated supply chain networks.

Recent incidents underline the importance of readiness, and we can’t treat cyber security as a commodity. Brands must keep their finger on the changing pulse of the threat environment by embedding cyber practices into the business. Just take a look at your firewall(s) and email security logs to realise cyber criminals are constantly targeting all businesses.

Cyber and business risk should be high on a board agenda, all C suite representatives should have responsibility. CIOs must drive change within businesses from reactive patchwork to proactive resilience through ongoing employee training and continuous investment in technology and people to come out stronger, both in operations and reputation ●

The attack on M&S is a clear example of hackers exploiting third-party relations to reset passwords

Jon Bance is Chief Operating Officer at Leading Resolutions



ELF

Electronic Lens Finder



Electronic Lens Finder & Delivery Set

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

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

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



LONDON

T: +44 207 205 2100

E: contact@qccglobal.com

SINGAPORE

T: +65 3163 7100

W: www.qccglobal.com



Keeping your business, **your** business !



MILITARY MINDSET

Tom Exelby *reveals why SMBs need to change their thinking to combat the menace of ransomware*

Small and medium-sized businesses (SMBs) in the UK are high-profile targets for cyber criminals – and the constant evolution of ransomware is one of the severest challenges. A survey of 2,000 SMBs in the UK and US by Microsoft in September last year, for example, found cyber criminals have attacked one in three firms. The average cost of investigation and recovery after an attack was anything between £60,000 (\$78,000) and £3.1-million (\$4-million), with an average of £191,000 (\$250,000).

Although ransomware is just one type of malware, it is the intended threat of extortion, system down time and data theft that packs the biggest punch, capable of inflicting fatal damage. To defend themselves, SMBs need a reinvigorated approach, going back to the cyber basics and extending their effectiveness through methodologies borrowed from the military.

While SMBs have been paying close attention to data protection and strengthening their ability to detect phishing attacks, they should ensure they have no blind spots in relation to ransomware because the consequences of failure are so severe.

The costs of ransom payments to have data decrypted followed by remediation and recovery are mounting all the time. The loss of reputation among customers, partners and suppliers is a significant cost on its own. Irrespective of whether SMBs pay ransoms to have data restored, prolonged downtime caused by an attack can be enough to destroy a business. The haulier KNP Logistics, for example, was put out of business by Russian ransomware attackers in 2023 with the loss of hundreds of jobs because its data remained encrypted.

The danger for SMBs is underestimating the deviousness of ransomware criminals. While almost all the SMBs surveyed by Microsoft agreed cyber security is critical, 72 percent saw data protection as a challenge compared with only 42 percent identifying ransomware.

SMBs need to revitalise their approaches to ransomware because they lack in-house time and expertise, which puts them at a substantial disadvantage when up against ransomware gangs employing many new techniques including generative AI to increase speed and accuracy.

IBM's 2024 X-Force Threat Intelligence Report highlights how credential and identity-based threats are growing. Phishing, using stolen and valid credentials is

more sophisticated while social engineering, password-breaking software or keystroke logging are all methods that gangs continue to employ. Many of these tactics are precursors to ransomware attacks.

This year's CrowdStrike Global Threat Report confirms that 2024 saw the evolution of threats employing "high-tempo social engineering, legitimate remote tools and cloud-hosted payloads" to bypass defences. CrowdStrike found these techniques, including phoney help desk calls, are in use by groups including the outfit behind Black Basta ransomware. The report highlights how the time it takes attackers to move through a target's network once they have gained entry has crashed from 48 minutes to 51 seconds – a huge drop.

These developments accompany changes in the ransomware underworld, where the barriers to entry have been lowered through ransomware-as-a-service and a system of sub-contracting and specialisation. Ransomware is extremely attractive because it has low investment compared with other forms of organised crime and carries far less risk of being caught. The FBI estimates the Akira gang that targeted KNP Logistics raked in \$42-million from just 250 attacks.

SMBs may feel they are too small to be of interest to ransomware gangs. But this is where the criminals are clever. They use a formula to calibrate their demands according to the size of the business' revenue and they have malware that can access a company's insurance policy to work out the maximum level of extortion likely to trigger a pay-off.

To deal with such cunning adversaries, SMBs need to adapt their cyber security posture so they can constantly adapt to the new or updated techniques that criminals deploy. Rolling out a single solution and then relying on it to provide all-round protection is not effective in today's adversarial environments. Ransomware gangs are always tunnelling under or finding new paths through static, perimeter defences.

The experience of UK cyber security companies shows many SMBs still practise poor cyber hygiene, failing to do the basics such as regularly changing passwords, implementing multi-factor authentication and consistently applying security patches to software to remove vulnerabilities. Even security awareness training is frequently neglected, which is extremely dangerous given that the human factor is so prevalent in cyber breaches. Last year's Verizon Data Breach Investigation Report, for example, found a human element in 68 percent of breaches. The success of phishing campaigns is often a result of staff being unaware of what to spot in an email that indicates it contains malicious content. Firms that are still struggling with the essentials in this way should make a concerted effort to comply with the NCSC's Cyber Essentials programme, which is a major step in the right direction without significant cost.

An important element in the basics of cyber defence is resilience. Organisations must gain a greater understanding of resilience and use external expertise so they can not only defend, but also respond and recover from an attack as quickly as possible. Achieving effective resilience requires military precision, with a detailed and rehearsed incident response plan which addresses the key tenants of containment, eradication and recovery.

Planning for a ransomware attack must include mapping of data and a thorough understanding of its sensitivity. In other words, whose data it is and who may have to be informed – such as customers and third parties. This is important for regulatory compliance, but also to avoid long delays and indecision in the event of a ransomware attack. Any failure to inform affected individuals or companies is likely to incur reprimands and possibly, penalties from the Information Commissioner's Office or regulators.

For business continuity, organisations must regularly review their backup policies. Securing backups is essential as ransomware attacks frequently commence with encryption of backups before the criminals move on to their main targets.

ONE IMPORTANT LESSON FROM THE MILITARY SPHERE IS REGULAR DRILLS AND EXERCISES

The three watchwords here are defend, respond and recover, requiring a multi-layered ecosystem of tools that will kick in at different stages of an attack. This is where SMBs should learn from the military sector and adopt a layered defence in-depth approach.

Unfortunately, many SMBs put almost total faith in their endpoint protection. Even when they have integrated solutions behind them, nobody is monitoring, which significantly reduces their efficacy. Monitoring of endpoints is a necessity, but it must be in line with risk-management protocols that fit the business and its requirements. This requires expertise to know which alerts matter and how to act on them.

Fortunately, there is an optimal approach which utilises behavioural analysis to identify the telltale signs of a ransomware intrusion and stop it in its tracks. Spotting this behaviour is possible due to the nature of a ransomware attack and the predictable pathway it needs to take through a digital system to achieve its aim. If ransomware has been undetected and successfully starts to encrypt data, more advanced tools will recognise this, stop the process and be able to decrypt the small amount of encrypted data. This removes the necessity for negotiations, payments and prolonged downtime while backups are restored.

Given the speed with which ransomware can move through systems, SMBs must also segment their networks through user permissions. This will slow down lateral movement and increase the likelihood of detection. Multi-factor authentication is not difficult to implement and creates a significant barrier for attackers attempting to use compromised credentials. It is a simple but effective step.

SMBs need to act now because although the threat from AI is easily overstated, it is improving the effectiveness of ransomware, especially in the initial techniques that precede an attack. All the evidence shows AI is gradually making phishing campaigns faster and better targeted. With large language models, criminals can scan through masses of data

SMBs should ensure they have no blind spots in relation to ransomware because the consequences of failure are so severe.

– including stolen data – for the target details most relevant to their phishing campaign. Then they can prompt the technology to use these details to devise better-worded, more convincing emails that act as lures.

THE DANGER FOR SMBs IS UNDERESTIMATING THE DEVIOUSNESS OF RANSOMWARE CRIMINALS

This is not where the use of AI ends, however. AI will help criminals identify organisations that have been lax about patching a particular vulnerability and can point to the open doors in a network. If a vulnerability is patched, adapting the malware to find another vulnerability is relatively straightforward for practised operators. This is why regular patching is now so important.

Criminals are deploying AI to accelerate scanning for weaknesses once they are in an organisation's environments. They scan data to work out what is most important to a firm, examine the insurance certificate to gauge its size and coverage, and determine the likelihood and size of a payout. The speed of these operations, followed by encryption, makes it harder for businesses to detect without specialist tools and external expertise.

There are lessons here for businesses from the military approach to risk-management, tying together people, processes and technology. SMBs need intelligence about what their enemies are doing – in this case it is the ransomware gangs. This intelligence should include information about

how other organisations have been breached and what happened – what was successful and what was not. The business must use this intelligence to inform their defence, making an attack as difficult as possible by, for example, patching vulnerabilities as soon as possible. It is important not just to monitor for new threats, but to act on them, following the military concept of intelligence integration.

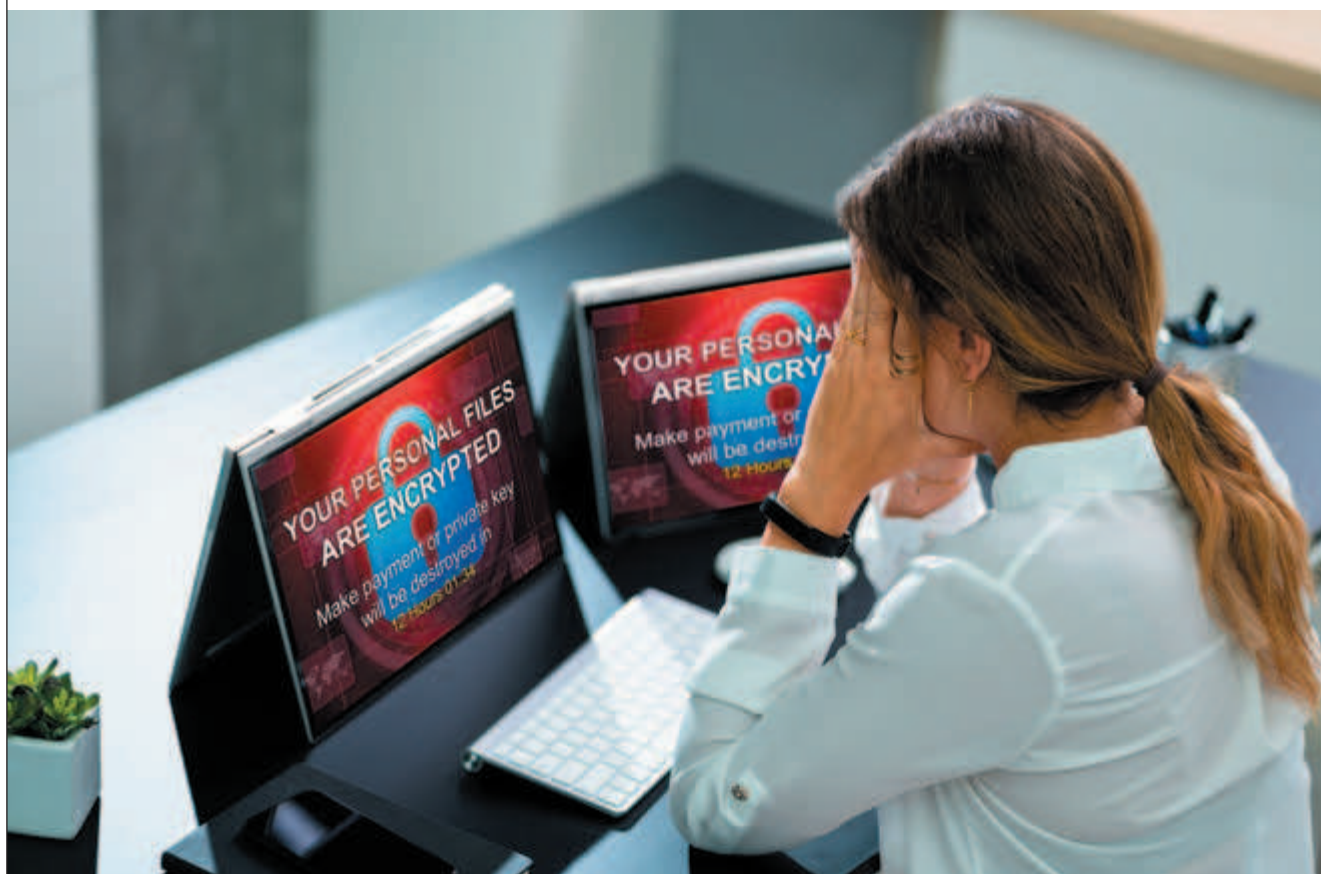
Allied to this is resource prioritisation – the process of focusing potentially limited resources on the most important, most lethal threats. This demands experience to avoid creating new threats through undue focus on one area. Concentrating on ransomware should not rob an organisation of effective defences against other types of threats.

Another important lesson from the military sphere is the necessity for regular drills and exercises. The ability to react decisively and recover quickly from a ransomware attack depends in large measure on preparation and the development of well-rehearsed, documented processes that people know how to follow should a breach occur. Making these drills effective demands thorough analysis of their effectiveness, followed by fast adaptation to ensure continuous improvement.

The dangers of ransomware are unlikely to recede for the UK's SMBs, given the profitability of this area of cyber crime, the increased sophistication and specialisation of the gangs involved and the low likelihood of them being caught. Yet, as we have seen, there are steps that SMBs can take that involve basic cyber hygiene and adoption of a multi-layered defence. With the assistance of third-party expertise, there are many reasons why SMBs should feel able to protect themselves against the menace of ransomware ●

Tom Exelby is Head of Cyber Security at Red Helix.

The time it takes attackers to move through a target's network once they have gained entry has crashed from 48 minutes to just 51 seconds





THE SECURITY EVENT



SAVE THE DATE

28-30 APRIL 2026
NEC BIRMINGHAM, UK

EUROPE'S LEADING COMMERCIAL,
ENTERPRISE & DOMESTIC SECURITY EVENT



ORGANISED BY

Nineteen

WWW.THESECURITYEVENT.CO.UK



NETWORK PROTECTION

Tyler Gannon *explains why securing hugely complex OT and IoT networks puts PAM technology centre-stage*

Amid the massive growth in IoT networks, machine identity is fast becoming a major security challenge. The number of IoT devices worldwide is expected to more than double from 16-billion in 2023 to over 32-billion in 2030. Many devices will be in the consumer market, but the industrial, automotive and healthcare sectors are also destined to see major expansion of IoT connections, with Statista forecasting 16 percent compound annual growth in Industry 4.0 technologies up to 2028.

The challenge is to secure data generated and handled by these devices, and to prevent them from becoming botnets or acting as points of entry to connected IT systems where criminals can exfiltrate or ransom valuable data. The

CyberArk 2024 Identity Security Threat Landscape Report revealed that more than two-thirds of surveyed security professionals believe as many as half of all the machine identities in their organisation have access to sensitive data.

Across sectors such as manufacturing, energy and logistics, the rapid proliferation of devices introduces new vulnerabilities that traditional identity and access management (IAM) systems were not designed to address. Organisations must therefore rethink their strategies to protect this expanding digital frontier by securing devices, automating identity processes, and implementing effective lifecycle management for a diverse range of devices.

In the manufacturing sector especially, organisations need to take best-in-class privileged access management (PAM) approaches and integrate them fully, extending



Cyber attacks using valid credentials shot up 71 percent last year

them across the shopfloor. In effect, this is extending the principles of zero trust access to encompass almost all the devices in an operational technology (OT) network. A zero-trust framework that extends throughout the lifecycle of both human and non-human identities ensures each identity, whether it belongs to a person, device, or process, is verified, authenticated and granted only the minimum level of access required for its role.

Thousands of organisations already apply PAM to the monitoring and protection of privileged accounts, to give staff and authorised partners and suppliers special access to maintain efficiency and security in IT. This covers the principle of least privilege – giving no more access than is strictly required. It also includes session management, password management and multi-factor authentication.

PAM therefore provides the necessary control and oversight when systems access is required by people inside or outside the organisation. These are the protocols that should be extended across OT and IoT networks to cover machine identities and credentials, so that devices are not hacked or logged into by criminals, state-sponsored hackers or malign insiders.

Managing the identity lifecycle of vast arrays of connected devices is critical to prevent serious harm. In poorly secured industrial IoT (IIoT) hackers are not only able to use stolen or unprotected device identities to gain access to sensitive data, but they can also threaten the health or wellbeing of large numbers of people. Causing healthcare devices, water treatment plants or connected vehicles to malfunction is potentially extremely serious.

The identity-related threats are real enough. Cyber attacks using valid credentials shot up 71 percent, according to IBM in its X-Force Threat Intelligence Index last year. As the report's introduction says: "In this era the focus has shifted towards logging in rather than hacking in." Through social engineering, phishing or inadequate or out-of-date device security, criminals can acquire the credentials they need to gain access.

For many organisations, the biggest risk lies in machine identities in OT accounts or IoT devices that allow attackers to operate unnoticed. The 2024 Waterfall ICS STRIVE report found a 19 percent year-on-year rise in OT security incidents with physical consequences, demonstrating that threats are far from theoretical and the repercussions are very real.

Managing identities in OT and IoT environments presents a very different set of difficulties compared with traditional IT however. In typical IT environments, the focus is primarily on human identities – employees, administrators and other personnel. However, in OT and IoT environments, devices can outnumber human users by as much as 45-to-one.

Every device in these environments requires a unique machine identity, sometimes several per device, complete with authentication credentials and specific access controls, so it can interact securely within the network. This complicates the security framework, as each device must be meticulously managed to prevent unauthorised access and potential breaches.

Compounding the complexity is the fact that many devices were designed to function in isolated, air-gapped setups. Many OT devices have little or no in-built security and were never intended for remote access through internet connectivity. Yet these devices must interact with multiple systems in today's IoT/OT networks. Alongside the surge in internet connectivity, IoT networks

are also managed from the cloud, 5G and satellite, bringing with them significant security challenges when managing the identity lifecycle of a vast array of connected and diverse devices.

The sprawling and uncharted nature of many networks, which may have been built up over decades, is another major obstacle. Many organisations' IT teams are not fully aware of all the devices for which they are responsible, let alone the state of the security in each of them. As organisations integrate their IoT and OT with broader IT systems, they create extensive attack surfaces vulnerable to malicious actors. But if organisations are unaware of all the devices they own, the task of defending a network is that much harder.

AUTOMATION ELIMINATES MUCH OF THE HUMAN ERROR THAT CAN LEAD TO SECURITY BREACHES

Lifecycle management across these devices introduces an additional layer of difficulty. From deployment to decommissioning, each device's access must be carefully managed, especially as they connect with various systems and even change ownership over time. Traditional manual IAM processes fall short in these contexts, as they cannot keep pace with the rapid evolution and proliferation of devices, each requiring distinct and ever-changing credentials.

The volume of work necessary to maintain protection in industrial IoT is beyond human capacity. Machine identities are complex. Each comes with its own set of digital encryption keys and requires a password which must be rotated. Every access request must be approved and then each device must recognise the approved credentials. When humans are burdened with all this, errors are inevitable, presenting major opportunities for hackers, ransomware gangs and employees or contractors with grudges.

To effectively manage identities in OT and IoT settings, organisations must adopt a comprehensive, automated approach. They need to start by mapping all the devices on their networks. Then they must bring PAM into management of the entire lifecycle of a device's identity.

Integration of PAM solutions safeguards high-risk identities and sensitive systems, extending strategies traditionally used for human identities to encompass device identities as well. Through centralised control and policy enforcement, PAM systems ensure secure access to critical devices and systems while maintaining operational efficiency, seamlessly weaving security into daily operations.

Extending zero trust across a network means benefiting from automation that deploys tested PKI (public key infrastructure), zero trust technology at scale and IAM provisioning. In addition, there is a need for policy-driven data encryption and continuous, automated monitoring of ecosystems. To be effective, that requires AI.

PKI security is vital. It is based on certificate assurance – an approach that has evolved to resolve problems of identity, authentication, integrity and privacy. It has now overcome the difficulties of scaling

for IoT, especially for devices with no UI or associated user. Policy-driven automation ensures IoT device certificates are securely generated, signed and managed. Automation is obviously essential for greater efficiency and removal of human errors, and to enforce uniform security standards across every device and identity within the network.

The benefits of automating identity lifecycle management for OT and IoT devices are substantial, particularly in terms of speed, security, and scalability. Automation eliminates much of the human error that has historically led to security breaches.

This not only improves the accuracy of identity management, but also significantly boosts response times to potential security incidents. Events and alarms from a PAM platform should be fed into SIEM (security information and event management) and SOAR (security orchestration, automation and response) systems to increase speed and effectiveness. Even if a device's credentials are compromised, the damage can be contained to prevent it from spreading across the network.

Security teams can act swiftly to mitigate risks before they escalate, ensuring that vulnerabilities are addressed promptly and efficiently. Such advanced PAM solutions enable organisations to uphold stringent security standards while ensuring smooth, interconnected operations.

Alongside automation, detection and faster incident-response, implementing a comprehensive identity lifecycle management solution simplifies regulatory compliance. This must be a critical consideration for organisations operating in industries where regulation is substantial and the stakes extend beyond financial losses – such as energy, manufacturing and healthcare.

Compliance with strict security regulations is essential and the integration of automated identity management to cover IoT and OT networks provides demonstrable control of access and the constant

upgrading of security measures across the lifecycle of each device and system. This consistency not only aids compliance, but also overhauls any organisation's entire security posture, providing peace of mind.

Looking ahead, as the volume and complexity of connected devices grow, identity lifecycle management solutions will need to evolve to keep pace. Emerging technologies, such as AI-driven analytics, offer promising enhancements in real-time threat detection and automated responses, which will be pivotal to future identity management frameworks.

The implementation of smart city concepts and significant initiatives to reindustrialise Europe and the USA to protect supply chains are only likely to further increase the importance of enhanced IoT/OT security based on automation of privileged access management. A survey of 1,300 executives at large companies conducted for the Capgemini Research Institute, found 48 percent of organisations engaging in reindustrialisation plan extensive use (for more than 50 percent of processes and activities) of IoT and industrial IoT technologies.

This is the context in which major companies must plan for scalability, ensuring that their identity management solutions can adapt as their OT and IoT ecosystems expand. Future developments are likely to emphasise even greater automation, more refined real-time monitoring capabilities, and enhanced interoperability across diverse environments in an increasingly interconnected world.

Securing identities in proliferating OT and IoT environments is a multi-faceted challenge that requires a strategic, automated approach. As connected devices perform ever more complex tasks, organisations that take security seriously will need more robust identity lifecycle management to safeguard their digital infrastructure.

By adopting comprehensive, automated solutions rooted in zero-trust frameworks and PAM systems, businesses can effectively mitigate the identity and credentials-based threats they face and ensure the security and integrity of their operations into the future ●

Tyler Gannon is VP North American Ops at Device Authority.

Every device requires a unique machine identity, sometimes several per device, complete with authentication credentials and specific access controls, so it can interact securely within the network



MCQUEEN TARGETS

LIVE FIREARMS TRAINING TARGETRY

**AIM
FOR
THE
BEST.**



**CIVILIAN
TARGETS**



**MILITARY
TARGETS**



**POLICE
TARGETS**



**THREAT
ASSESSMENT**



**3-D FOAM
TARGETS**



**3-D FOAM
ACCESSORIES**

Hit the mark every time with

MCQUEEN TARGETS

GALASHIELS, SCOTLAND



info@mcqueentargets.com

+44 (0)1896 664269

mcqueentargets.com

INCIDENT BRIEF



Europe

1 May, London – England

Just days after Marks & Spencer and the Co-op were targeted, Harrods was hit by a cyber attack understood to have forced the shop to shut down some systems.

2 May, Kaçanik – Austria

The Austrian Explosive Ordnance Disposal team carried out the controlled detonation of a WWII bomb found near a river.

3 May, Rochdale – England

A man was arrested on suspicion of murder and later charged for preparation of a terrorist act after collisions involving a car and four pedestrians.

4 May, London – England

Police arrested five suspects as part of a plan to target “specific premises” in an alleged imminent terror plot.

4 May, Madrid-Seville – Spain

Spain’s rail network suffered “an act of serious sabotage” after vital signalling cable was stolen, bringing severe delays to high-speed services affecting more than 10,000 travellers.

7 May, Paris – France

A violent confrontation erupted after a car rammed into a crowd of Paris Saint-Germain supporters. The vehicle was later chased down by a group of youths and set on fire.

8 May, Chedworth – England

Four controlled explosions were carried out at a farm in the Cotswolds by an Explosive Ordnance Disposal team after 140 sticks of dynamite were discovered in an outbuilding.



Americas

1 May, Tampa – USA

A suspicious suitcase found at the loading dock of the St. Petersburg Police Department led to an evacuation and the response of the Tampa Bomb Squad. Authorities later confirmed the suitcase was empty and arrested a suspect in connection.

1 May, Mendocino County – USA

A 49-year-old man was taken into custody after a couple of explosive devices left in the city were linked to him. Police found a third device in his home.

2 May, New Jersey – USA

A Passaic County man admitted to setting off an explosive at an ATM at a Chase Bank in Prospect Park, officials with the US Attorney’s Office said.

2 May, Washington – USA

The United States labelled the Viv Ansanm and Gran Grif gangs in Haiti as “foreign terrorist organisations”.

2 May, Ventura – USA

Two students were arrested after threats of a bomb and shooting locked down the Californian high-school campus.

5 May, Rio de Janeiro – Brazil

Two people were arrested in connection with an alleged plot to detonate explosives at a free Lady Gaga concert, in an attack authorities believe was targeting Brazil’s LGBTQ community.

7 May, Springfield – USA

A Virginia, man was sentenced to 364 months in prison for his efforts to provide material support believed to have been upwards of \$185,000 to Isis.



Asia

1 May, Guwahati – India

Three men linked to insurgent group extortion activities were arrested by police following extensive intelligence reports.

1 May, Osaka – Japan

Police arrested a man on suspicion of attempted murder after he drove his car into seven schoolchildren walking home from school. A girl suffered a broken jaw and the other children are reported to have relatively light injuries.

2 May, Deir ez-Zor – Syria

The Syrian Democratic Forces arrested Isis leader Hamoud Abdullah al-Khatib, aka Abu Zakaria.

4 May, Tel Aviv – Israel

Israeli and US defence systems failed to down a missile fired at Gurion airport by Houthi militants from Yemen.

4 May, Tira – Israel

Police arrested a 16-year-old minor on suspicion that he planned to carry out a terror attack after he entered the parking lot of a police station armed with a knife and shouting: "Allahu Akbar".

5 May, Hodeida – Yemen

Israel's military carried out airstrikes against Houthi rebels in the Red Sea city after the Iranian-backed rebels missile launch yesterday.

6 May, Yemen

The US agreed a ceasefire with the Houthis in Yemen after the Iran-aligned group agreed to stop targeting shipping in the Red Sea.

7 May, Bahawalpur, – Pakistan

Abdul Rauf Azhar, the younger brother of Jaish-e-Mohammed chief Masood Azhar was killed during a series of "precision airstrikes" as India struck infrastructure in Pakistan and Pakistan-occupied Kashmir.

8 May, Kafr Qasim – Israel

Israeli security forces arrested a resident of the central Arab-Israeli city on suspicion of attempting to join the Islamic State terrorist organisation in Syria.



Africa

1 May, Maiduguri – Nigeria

Residents of the capital of Borno State were thrown into panic in the early hours as multiple explosions occurred at the Giwa Barracks.

2 May, Buni Gari – Nigeria

Militant insurgents killed at least 11 soldiers in an attack on their base in Yobe state.

2 May, Nigeria–Niger Republic border

As many 18 fishermen were gruesomely killed and several others declared missing following a deadly attack by Boko Haram terrorists in the Mobbar Local Government Area.

3 May, South Africa

South African Airways announced that it has been impacted by a significant cyber incident, temporarily disrupting access to its website, mobile app and several internal operational systems.

4 May, Port Sudan – Sudan

The paramilitary Rapid Support Forces (RSF) carried out a series of drone attacks on the Northern port in the city.

5 May, Kosti – Sudan

RSF drone attacks targeted fuel depots in the Southern White Nile state, leading to a number of power black-outs across the country.

5 May, Doso – Niger

About 10 soldiers were killed, seven injured and 18 left unaccounted for following an ambush in the country's South.

5 May, Tunis – Tunisia

A court sentenced former Prime Minister Ali Laarayedh to 34 years in prison on a raft of terrorism charges.

6 May, Port Sudan – Sudan

Air traffic was disrupted as RSF drones struck the airport and targeted an army base. No one was hurt in the attack, but a number of flights were cancelled.

6 May, Niassa – Mozambique

An attack claimed by jihadists linked to the Islamic State group in a remote tourist town in the North killed two rangers.



NEWS

Europe

UK denied access to EU crime and illegal migration data

A request for access to shared European Union crime and illegal migration data from the UK was reportedly rejected in early May, in a blow to Keir Starmer's hopes of a post-Brexit relations "reset". British negotiators had been hoping to reach a deal on gaining access to the Schengen Information System (SIS) – a vital tool for sharing police alerts across borders within the area where 29 countries have abolished passport controls. However, European officials were reported by *The Times* to have ruled out allowing access to it and to the bloc's centralised fingerprinting system, Eurodac, which stores information on illegal migrants. The prime minister suggested last year at an Interpol annual general assembly in Glasgow that EU leaders had shown an interest in giving the UK access to the intelligence database used to identify people seeking asylum. Asked whether he could detect enthusiasm from EU leaders about giving the UK access to Eurodac data as part of a new security deal, he told journalists: "Yes, there is an appetite to work more closely with us on this. Because look, these are shared challenges."

Security agencies support for personal data to stop terrorism

As many as 79 percent of UK adults support national security agencies collecting and processing personal data to investigate terrorism and serious crime, according to new research by the Centre for Emerging Technology and Security (CETaS) at The Alan Turing Institute, in collaboration with Savanta and Hopkins Van Mil. The new study, which featured a representative survey of over 3,000 UK adults alongside a citizens' panel, measured public attitudes to national security agencies processing personal data. The research measured public support for data processing across several different purposes, ranging from investigating

individuals suspected of terrorism and serious crime to creating automated tools for predicting future behaviour. Public support ranged across these contexts and was not universal; for example three in 10 (28 percent) are opposed to personal data being used to train a new automated tool for predicting future behaviour. Three in four (75 percent) support national security agencies collecting and processing personal data to detect foreign government spies and four in 10 (42 percent) support its use to create automated tools to predict future behaviour.

UK warns companies cyber security must be "priority"

In mid-May the British government warned all UK companies to treat cyber security as an "absolute priority" in the wake of attacks on retailers Marks & Spencer, the Co-op and Harrods. Cabinet office minister Pat McFadden led a briefing with national security officials and Richard Horne, the CEO of the National Cyber Security Centre, about support being provided to the affected retailers. Speaking at the CyberUK conference in Manchester, McFadden warned the recent attacks are a: "wake up call" for all businesses before highlighting moves to: "bolster our national defences" including new legislation – the Cyber Security Bill. "In a world where the cyber criminals targeting us are relentless in their pursuit of profit – with attempts being made every hour of every day – companies must treat cyber security as an absolute priority," McFadden advised.

German spy agency labels AfD "right-wing extremist" force

Germany's domestic intelligence service has designated the far-right Alternative für Deutschland (AfD), the biggest opposition party, as a "confirmed right-wing extremist" force, meaning authorities can step up their surveillance as critics call for it to be legally banned. The Federal Office

for the Protection of the Constitution (BfV) previously considered the anti-immigrant, pro-Kremlin party a "suspected" threat to Germany's democratic order, with three of the AfD's regional chapters in Eastern states and its youth wing classed as confirmed extremist. The AfD, which came second in the February general election with just over 20 percent of the vote, said it would challenge the BfV's decision in court. The BfV said it had concluded that racist and anti-Muslim stances advanced by the AfD, based on an: "ethnic-ancestry-based understanding" of German identity, were: "incompatible with the free democratic basic order" set out in the country's constitution. The decision will clear the way for tougher measures to monitor the party for suspected illegal activity, including tapping telephone communications, observing its meetings and recruiting secret informants.

PKK militants to disarm after decades against Turkey

The Kurdistan Workers' party (PKK) – whose insurgency against Turkey has spanned more than four decades – has declared it will disarm and disband, after a call from its jailed leader earlier this year. The PKK announced the decision to dissolve its guerrilla forces, heeding a watershed announcement from Abdullah Öcalan three months ago. Leaders of the militia group, which is regarded as a terrorist organisation in Turkey, the UK and US, said their armed insurgency had: "brought the Kurdish issue to the point of resolution through democratic politics, and in this regard the PKK has completed its historical mission." The announcement will affect forces based near Turkey's borders with Iraq and Iran, as well as allied or splinter groups in North-East Syria. Despite the PKK announcement of a: "new phase", the decision to dissolve appears to be unilateral, with few indications about authorities in Ankara offering dialogue.



Americas

NEWS

Trump to reopen Alcatraz prison for "most ruthless offenders"

US president Donald Trump has said he is directing the administration to reopen and expand Alcatraz, the notorious former prison on an island off San Francisco that has been closed for more than 60 years. In a post on his Truth Social site in early May, Trump wrote: "For too long, America has been plagued by vicious, violent, and repeat Criminal Offenders, the dregs of society, who will never contribute anything other than Misery and Suffering. When we were a more serious Nation, in times past, we did not hesitate to lock up the most dangerous criminals, and keep them far away from anyone they could harm. That's the way it's supposed to be." He added: "That is why, today, I am directing the Bureau of Prisons, together with the Department of Justice, FBI and Homeland Security, to reopen a substantially enlarged and rebuilt ALCATRAZ, to house America's most ruthless and violent Offenders." The directive received a scathing reception from critics, especially California Democrats. Scott Wiener, a Democratic state senator representing San Francisco, posted that Trump: "wants to turn Alcatraz into a domestic gulag right in the middle of San Francisco Bay".

Trump administration to cut thousands of jobs from CIA

The White House plans to cut staffing at the Central Intelligence Agency by 1,200 positions while other intelligence agencies including the National Security Agency will also shed thousands of jobs, *The Washington Post* reported in early May. The Trump administration has told members of Congress about the planned cuts at the CIA, which will take place over several years and be accomplished in part through reduced hiring as opposed to layoffs, the *Post* reported. The cuts include several hundred people who had already opted for early retirement,

it claimed. In response to questions about the reductions, the CIA issued a statement saying its director, John Ratcliffe, was working to align the agency with Donald Trump's national security priorities. "These moves are part of a holistic strategy to infuse the agency with renewed energy, provide opportunities for rising leaders to emerge and better position CIA to deliver on its mission," the agency said in the statement. Earlier this year the CIA became the first US intelligence agency to join a voluntary redundancy programme initiated by the president, who has vowed to radically downsize the federal workforce in the name of efficiency and frugality. The NSA has already offered voluntary resignations to some employees and the CIA has said it plans to lay off an unknown number of recently hired employees.

CISA & FBI: hackers are targeting industrial systems

In early May, the FBI and Cybersecurity and Infrastructure Security Agency (CISA) warned of unsophisticated threat actors targeting industrial control systems and operational technology environments in key critical infrastructure sectors. The guidance, co-authored by the US Department of Energy and the Environmental Protection Agency, said the threat activity targeted critical infrastructure in the oil and gas industry and involved the energy and transportation sectors. The agencies urged security leaders to use better cyber hygiene and protect assets exposed to the internet. While it is not clear what specific incidents led to the advisory, the guidance is similar to prior warnings about threat actors targeting drinking and wastewater treatment providers and small power companies. The agencies advised three major security improvements: removing OT connections from the public internet, as exposed OT devices can easily be discovered through search engines that track open ports. Immediately changing default passwords with

strong passwords that are hard to guess and securing remote access to OT networks, with users upgrading to a private IP network and adopting VPNs with strong passwords and phishing-resistant multifactor authentication.

US creates second military zone along Southern border

The Pentagon is creating a second expanded military zone at its South-Western border, to be patrolled by US soldiers, in the Trump administration's latest step to militarise the boundary with Mexico to help stem the flow of migrants. The military's Northern Command said in a statement in early May that it was establishing a narrow strip of land along the Southern border of Texas that will become part of Fort Bliss, near El Paso. The strip will be about 63 miles long. In April the Pentagon created a 60-foot-wide strip of land along 200 miles of the border between New Mexico and Mexico, effectively turning it into part of a military base there. Any migrants entering the newly designated military installations, or national defence areas, will be considered to be trespassing and can be temporarily detained by troops until Border Patrol agents arrive, military officials said.

Migrant crossings at US-Mexico border stay historically low

The number of migrants crossing the US Southern border unlawfully continued to be at a historically low level in April as Border Patrol agents recorded 8,400 apprehensions of those crossing the US-Mexico border without authorisation. April's preliminary tally, which could be adjusted once the data is published, is a slight increase from March, when Border Patrol recorded 7,200 apprehensions. And it is nearly identical to the 8,300 apprehensions the agency recorded in February. The number of illegal crossings during Trump's first three months in office represents a seismic change.



Asia

Pakistan intel may seek details on India's military trains

India's Railway Ministry has cautioned its employees against the Pakistan intelligence agencies' attempt to seek details of the movement of military trains and asserted that the confidential information should not be shared with any unauthorised person. In its advisory released on 6 May, a day before Indian armed forces carried out missile strikes on nine terror targets in Pakistan and Pakistan-Occupied Kashmir in retaliation for the Pahalgam attack, the ministry said divulging such information will be a grave threat to national security. "Pakistan intelligence operatives may call railway officials and seek confidential information regarding military special train movements," a message from the Railway Board to all Principal Chief Operation Managers of all railway zones, said. "Disclosing of such information to any unauthorised person other than Mil Rail staff (Military Wing of Railways) by railway officials will be considered as a breach of security and will amount to grave threat to national security," it said. Mil Rail is a specialised wing of the Indian Railways that provides logistical support to defence forces. "Therefore, it is desired that the railway officers and staff may be instructed to be sensitised to the critical nature of information regarding the movement of military special trains and the gravity of the issue," it said. The ministry has urged senior officials to instruct all staff that "in case any individual seeks information about military movement, no information should be divulged to unauthorised persons".

Billbug expands cyber espionage campaign in South-East Asia

A China-linked cyber-espionage group using custom malware had "significant success" infecting government organisations and critical private-sector industries in much of South-East Asia in late 2024 and early 2025, according to intelligence

reports released in early May. The group has targeted the government, manufacturing, telecommunications and media sectors in several South-East Asian countries and regions, including the Philippines, Hong Kong, Taiwan and Vietnam, according to a report released by the Symantec threat hunting team at Broadcom, which calls the group Billbug (although it's better known as Lotus Panda or Lotus Blossom). It has used legitimate but out-of-date binaries from security firms to load malicious software components onto targeted systems in order to compromise them, according to the Symantec threat analysis. While the group has expanded its focus beyond government and military organisations to include private industry, it focuses almost exclusively in the South-East Asia region, says Dick O'Brien, principal threat intelligence analyst for the Symantec Threat Hunter Team. "They have quite a tight focus on South-East Asia, and it's rare to see them go further afield," he concluded.

Myanmar militia leader sanctioned by US

The US Treasury Department sanctioned a Myanmar militia group and its leader in early May for their alleged participation in the booming cyber fraud industry. The designation targets the Karen National Army (KNA) and Saw Chit Thu, a longtime power broker in the Myawaddy area of Karen State along the border with Thailand. The Treasury's Office of Foreign Assets Control also sanctioned his two sons, Htoo Eh Moo and Saw Chit Chit. The KNA, who until mid-2024 were known as the Karen Border Guard Force, control security in Shwe Kokko, an area home to industrial-size scamming compounds, where much of the workforce is made up of people who are lured into the industry on false premises and forced to carry out scams. The FBI reported Americans lost more than \$6.5-billion to crypto currency-related investment fraud

last year. Despite recent crackdowns backed by Thailand and China, the scamming industry has continued to metastasize throughout the region and within Myanmar, including in Myawaddy. Saw Chit Thu was sanctioned in 2023 by the UK and in 2024 by the European Union.

Malicious bots behind nearly half of web traffic in Singapore

Malicious bots aided by artificial intelligence tools now generate as much as 45 percent of all internet traffic in Singapore, a sharp rise from 35 percent a year ago, according to the 2025 Imperva Bad Bot Report, which compared traffic between 2023 and 2024, found bad bots to be most prevalent in the gambling, gaming, automotive and travel sectors. The 12th edition of the report drew from data collected from across the Imperva global network in 2024, including the blocking of 13-trillion bad bot requests across thousands of domains and industries. Singapore ranked fourth among places in the Asia-Pacific that were most targeted by bad bots in 2024, after Hong Kong, Indonesia and Australia. Globally, automated bot traffic surpassed the human-generated type for the first time in a decade, constituting 51 percent of all web traffic last year.

Syrian forces monitored armed civilians who killed Alawites

One of the men accused of taking part in sectarian violence against Syria's Alawite minority told the BBC that he and other armed civilians who travelled to the area were advised and monitored by government forces there. Abu Khalid said he had travelled as a civilian fighter to the Mediterranean coastal village of Sanobar on 7 March, to help battle former regime insurgents. "There were eight men with me, but it was a large group, and the General Security department was overseeing things so that no-one would vandalise the village or harm the residents," he said.



INTERNATIONAL SECURITY EXPO

30 SEPT - 1 OCT 2025 | OLYMPIA, LONDON

CONNECTING THE GLOBAL SECURITY COMMUNITY

10,000+

GLOBAL SECURITY
DECISION-MAKERS

300+

INTERNATIONAL
EXHIBITING BRANDS

HIGH-LEVEL

SUMMIT & CONFERENCE

EXCITING

LIVE DEMONSTRATIONS



SCAN TO REGISTER
FOR FREE



INTERNATIONALSECURITYEXPO.COM



CO-LOCATED WITH
INTERNATIONAL
CYBER
EXPO

30 SEPT - 1 OCT 2025 | OLYMPIA, LONDON



NEWS

Africa

Dossier of Sudan war crimes handed to Metropolitan police

Scotland Yard has received a dossier of evidence documenting myriad alleged war crimes committed by a paramilitary group during the conflict in Sudan. Lawyers have submitted a 142-page file of evidence to the war crimes unit of the Metropolitan police containing details of numerous atrocities perpetrated by the Rapid Support Forces (RSF). Compiled by a London-based team of barristers specialising in international law, it documents killings, torture and mass rape. It has been drawn up to support global efforts to hold perpetrators accountable and the lawyers have requested that the Met unit – part of the force's counter-terrorism command known as SO15 – reviews the dossier before passing it to the international criminal court (ICC) to assist investigations into RSF atrocities in Darfur, Sudan. Now into its third year, the catastrophic war between the RSF and the Sudanese military has prompted the world's biggest humanitarian crisis, killed at least 150,000 people and forced 12-million from their homes. The lawyers said the documents, given to the Met on Monday, offer evidence that the RSF's leadership are responsible for repeated war crimes, focusing on the legal principle of "command responsibility" – that commanders knew or ought to have known about the atrocities committed by their troops.

US puts \$10-million bounty on Manda Bay al-Shabaab fighter

The US government has placed a \$10-million bounty on Abdullahi Banati, a suspected al-Shabaab militant believed to be behind the Manda Bay terror attack of 2020. The attack saw 30-40 militants launch mortar rounds and fire rocket-propelled grenades and small arms as they took the lives of three US citizens and was the first major attack by militants on a US base in East Africa. Abdullahi is said to be a member of

the Jaysh al-Ayman group named after ethnic Somali Maalim Ayman. Banati is understood to be one of the individuals involved in the operational planning of the 2020 attack. The US Department of State designated al-Shabaab as both a Foreign Terrorist Organisation and a Specially Designated Global Terrorist in March 2008. The group is currently under sever attack in Kenya and Somalia.

Nigeria state leaders demand action against Islamist attacks

State governors from North-Eastern Nigeria called on the government to put forward a new strategy to tackle an upsurge in Islamist militant attacks at the start of May. The governors of Borno, Adamawa, Yobe, Gombe, Taraba and Bauchi took part in the 11th North-East Governors Forum (NEGF) amid renewed violence that left more than 100 people dead last month. Taraba state governor Agbu Kefas said in a closing statement, "The forum... calls for the armed forces, other security agencies and community leaders to reappraise their strategy in the counter-insurgency onslaught in the region." While the main militant group, Boko Haram, as well as its splinter group, Islamic State West Africa Province (ISWAP), has lost ground to the Nigerian military, a recent spate of attacks has sparked concerns that the violence could once again spread. The two former rivals have reportedly resolved some of their differences, allowing them to concentrate on fighting Nigeria's security forces. They've also updated their combat tactics, employing drones and explosive devices.

Cameroon insecurity getting worse in Far North region

Cameroon is continuing to be attacked by Boko Haram and the situation is getting worse, according to a local bishop. Bishop Barthélemy Yaouda Hourgo of the Yagoua Diocese in Cameroon's Far North warned that the security situation is deteriorating

rapidly and that: "Boko Haram now has access to drones". "Unfortunately, we are losing soldiers and the toll on civilians is even more devastating. Civilians who have their cattle in the bush are killed. It's become part of our daily lives," he noted. Added to the attacks are the kidnapping of people for ransom. "Once kidnappers believe you have a little money, they will either come for you, your kids or your wife. They take all these people and they can only be released upon the payment of a ransom," Yaouda Hourgo explained.

Infosec Africa to commission AI-driven security operations

Indigenous Ghanaian firm Virtual Infosec Africa Limited (VIA) launched Africa's largest and most advanced managed security and digital forensic services centre in Accra in mid-May. The centre will serve as a one-stop shop for companies seeking quality cyber security solutions. The state-of-the-art facility promises to transform how organisations across Ghana and the continent approach cyber security challenges by dramatically reducing costs while enhancing protection capabilities. The company said in a press statement that the new centre will slash cyber security expenditures for organisations by over 90 percent by eliminating one-off capital investments. It will also reduce companies' operational costs by more than 60 percent, the statement said, adding that the facility will be a significant leap forward for Ghana's digital security infrastructure. The launch of the managed security service comes at a time when critical information infrastructure and businesses across Ghana and Africa are under increasing threat from sophisticated cyber attacks. As recently as late April, thousands of MTN Ghana customers suffered a security breach after it suffered a cyber attack that the company said might have compromised some data.

DIARY DATES

2025/6 Conference and Exhibition planner

31 July - 1 August India Homeland Security Expo 2025

New Delhi, India
Organiser: Nexgen Exhibitions
Tel: +91-7533018555
Email: info@internationalpoliceexpo.com
www.homelandsecurityexpo.in

26-27 August ISEC International Security Conference 2025

Seoul, South Korea
TEL | FAX +82-2-715-8245 | E-MAIL : isec@boannews.com
Organiser: theBN Company
Tel: +82-2-719-6933(ARS. 4)
Email: isec@boannews.com
www.isecconference.org/2025

9-12 September DSEI 2025

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

17-18 September The Emergency Services Show 2025

Birmingham, UK
Organiser: Nineteen Group
Tel: +44 (0)20 8947 9177
Email: info@emergencyuk.com
www.emergencyuk.com

22-23 September CLS EU Cyber Leader Summit 2025

Brussels, Belgium
Organiser: Clarion Events
Tel: +44 (0)20 7384 7700
Email: info@clarionevents.com
www.cyber-leaderssummit.com

29 September - 1 October Global Security Exchange 2025

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

30 September - 1 October International Security Expo 2025

London, UK
Organiser: 19 Events
Tel: +44 (0)20 8947 9177
Email: info@internationalsecurityexpo.com
www.internationalsecurityexpo.com

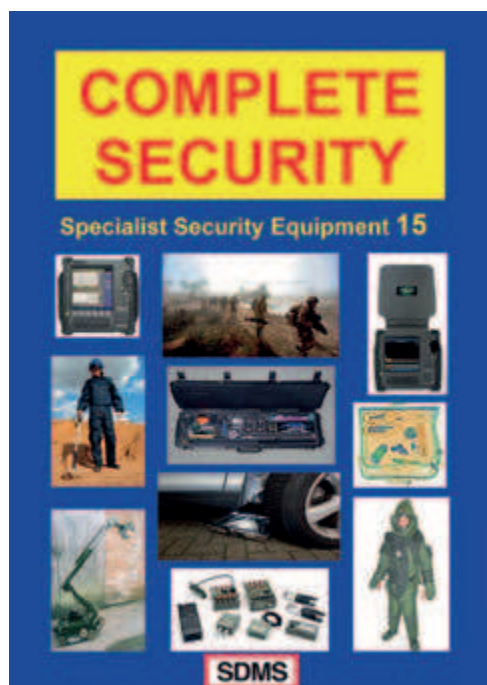
18-21 November Milipol Paris 2025

Paris, France
Organiser: Comexposium
Tel: +33 1 76 77 11 11
Email: info@comexposium.com
www.milipol.com

19-21 November Sicurezza International Security & Fire Exhibition 2025

Milan, Italy
Organiser: Fiera Milano
Tel: +39 02 4997 7134
Email: info@fieramilano.it
fieramilano.it

SUPPLIERS OF ANTI-TERRORIST EQUIPMENT



SDMS are suppliers of anti-terrorist and internal security equipment to the governments of over 130 countries worldwide, as well as to many large corporate clients. We supply top-quality equipment at highly competitive prices. Most equipment is also supplied on our "sale or return" basis whereby, if a client is not completely satisfied with equipment we have supplied, it can be returned to us for a complete refund.

SDMS also undertakes specialist training assignments, utilising some of the UK's most experienced and highly qualified ex-government instructors.

- * Anti-terrorist
- * Surveillance
- * Methods of entry
- * Search - explosives, weapons and drugs
- * Personal protection
- * Counter-surveillance
- * Property protection
- * Police & special forces
- * Training

SDMS Security Products UK Limited, Elysium House, 126-128 New Kings Road, Fulham
LONDON SW6 4LZ

Tel: +44 (0)20 7731 8417

Fax: +44 (0)20 7610 9927

Email: sales@sdms.co.uk

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.

*Tested mobility
solutions for
protection
up to VR10*



TSS International official distributor for:



YOUR MOBILITY SPECIALIST FOR AMOURED 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 BV ZUIDEINDE 30-34, 2991LK BARENDRECHT. THE NETHERLANDS.
PHONE: +31 (0)180-618 922 EMAIL: SALES@TSSH.COM **WWW.TSSH.COM**



NEW TECHNOLOGY SHOWCASE



Detection Technology unveils X-Cargo detector modules

Detection Technology has introduced X-Cargo, its advanced multirow detector family that's purpose built to set a new benchmark in high-speed, high-energy X-ray imaging performance. X-Cargo is tailored for cargo scanning and other demanding MeV-level applications, combining speed, resolution and sustainability in a single modular platform. It meets the demanding needs of modern cargo inspection in critical security environments such as ports, border crossings and customs checkpoints by enabling fast, non-intrusive scanning without manual inspections to ensure efficient control over goods moving through high-risk infrastructures. Primarily used for truck and train cargo scanning, X-Cargo also serves growing industrial applications like dense metal waste sorting and advanced non-destructive testing (NDT) of assembled automotive parts and battery systems. With support for scanning speeds up to 70km/h in single energy Linac systems and 36km/h in dual energy setups, X-Cargo's newly designed high-speed, optical 10Gbps control board is capable of managing up to 80 detectors with a single board. This opens the door to building larger system designs and multi-view configurations, crucial for high-throughput environments and more comprehensive inspections. This scalable, platform-based approach separates the sensor and data acquisition board, offering software-configurable flexibility and faster servicing – only necessary components need replacing, which reduces downtime and contributes to environmental sustainability.

i-PRO ISO/IEC 42001 AI certification first

i-PRO Co. obtained ISO/IEC 42001 certification for its Artificial Intelligence management systems from the British Standards Institution in early May. ISO/IEC 42001 is the first international standard for the design, development and operation of ethical, transparent, secure and accountable AI systems by organisations utilising AI technology. The standard was published by the International Organisation for Standardisation (ISO) and International Electrotechnical Commission (IEC) in December 2023. Businesses that obtain certification are required to implement comprehensive AI management, including management systems, risk assessment, internal controls, ethics policies, human resource training and information sharing with external parties, encompassing the entire lifecycle of AI systems. i-PRO has been at the forefront of AI research and development for many years, delivering innovative camera hardware that utilises cutting-edge AI technology in the security and public safety fields. This is the first certification in Japan, through a comprehensive independent audit conducted by BSI (British Standards Institute) Group Japan.

Verkada new dual-head camera

Verkada has unveiled its new dual head camera and enhanced alerting capabilities on its Command platform, along with a range of updates making it easier to keep people and places safe. The latest expansion to its multisensor line, the CY53-E Two-Camera Multisensor boasts two viewing angles from a single install point, an advanced onboard processor, and 2.55x optical zoom in each sensor. Verkada has also introduced enhanced alerting capabilities so security teams can receive an alert when a visitor arrives on-site. Additional features include deeper integration between alarms and access control with the addition of door event triggers; the ability to group persons of interest into lists and the expansion of History Player Search to include vehicles; new deterrence capabilities include a wireless siren and strobe that can be triggered by Verkada Alarms; and a refreshed UI and search experience.

Roke redefines electromagnetic warfare with portable module

UK company Roke has launched EM-Vis Deceive, its new portable electronic warfare system that brings electromagnetic attack capabilities directly to troops on the ground. The lightweight system can be carried by a soldier and helps detect, track and disrupt enemy communications, drones or other electronic signals. EM-Vis Deceive is the first fully integrated person-borne system of its kind to be designed and built to modular open standards – providing a flexible, upgradable and tailorable solution for different missions. The system can disrupt a wide range of enemy targets including drones, missiles and communication systems, and marks a major step as electronic warfare moves closer to the frontline, responding to the need for faster, more flexible responses to threats on the modern battlefield.

GA-ASI's uncrewed Protector gains UK certification

The UK's Military Aviation Authority has issued a Military Type Certificate to the Royal Air Force's Protector RG Mk1 uncrewed aircraft, also designated the MQ-9B, certifying that it has passed a rigorous airworthiness assessment and verifying it's safe to operate without geographic restrictions, including over populous areas. The decision was a first-of-its-kind milestone for a large, unmanned aircraft system and marks something of a technological watershed for unmanned aircraft systems. GA-ASI is the first manufacturer of large, unmanned aircraft to receive an MTC based on rigorous compliance with STANAG 4671, the NATO standard for unmanned aircraft system airworthiness.



3DX-RAY

An **IMAGE SCAN** company

INSIGHT WHERE IT MATTERS

ThreatScan®-AS

PORTABLE X-RAY SYSTEMS

AS1 larger panel or AS2 smaller panel

120kV or 150kV generator & imaging station

High penetration with sub-millimetre resolution

Intuitive, user-friendly ThreatSpect software



FOR MORE INFORMATION CONTACT

sales@3dx-ray.com

www.3dx-ray.com

PROTECTING WHAT MATTERS

CRASH RATED HOSTILE VEHICLE MITIGATION SOLUTIONS

BOLLARDS, ROAD BLOCKERS, GATES & VEHICLE BARRIERS

ATG Access has been enhancing urban environments and creating spaces where people feel safe, living without fear of vehicle borne threats, since 1989.

With a vast range of crash rated hostile vehicle mitigation solutions including bollards, road blockers, gates and vehicle barriers, ATG Access offers a one-stop-shop solution for your perimeter and entrance security requirements.

