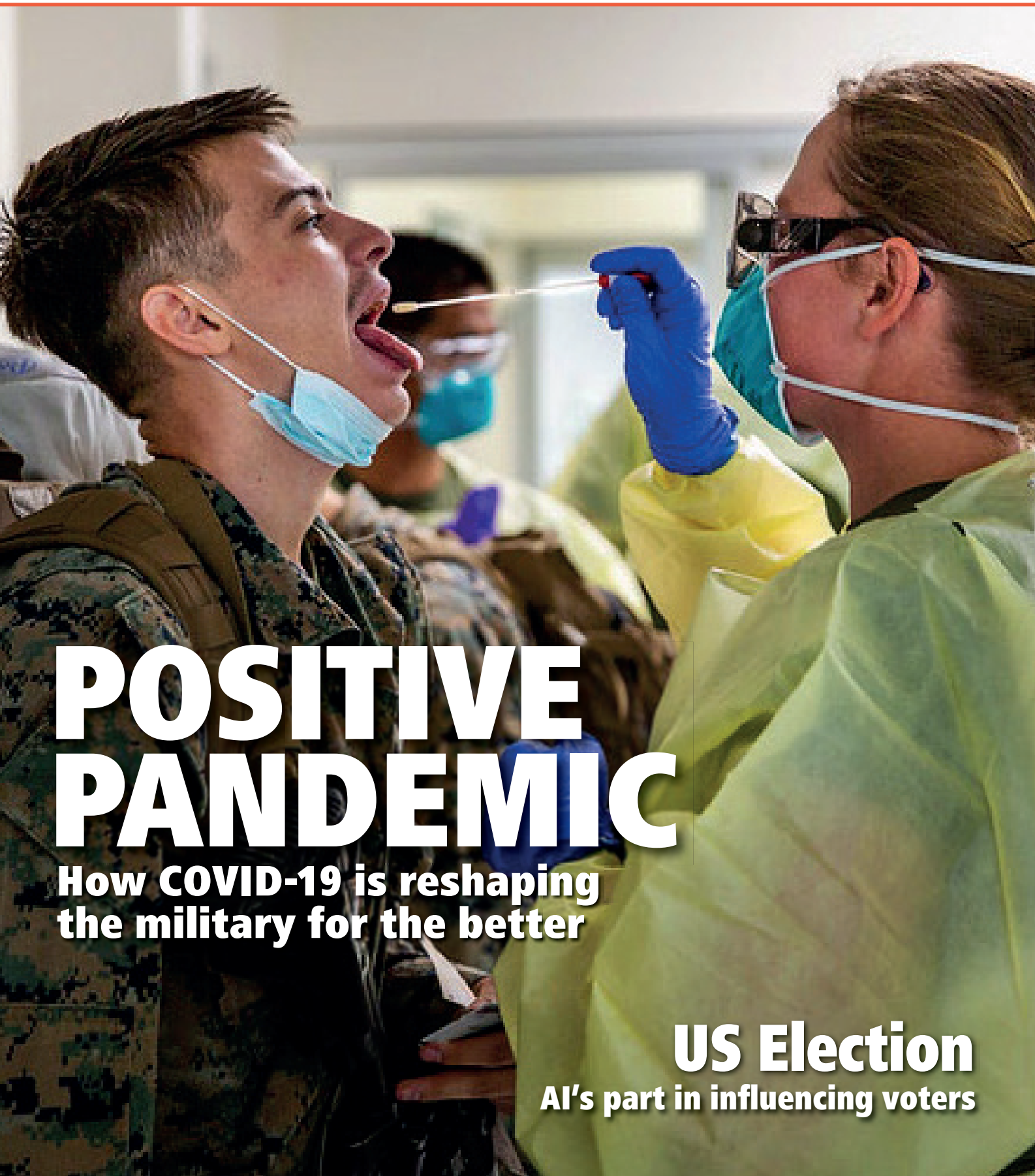
www.intersec.co.uk

intersec

The Journal of International Security

October 2020



POSITIVE PANDEMIC

How COVID-19 is reshaping the military for the better

US Election

AI's part in influencing voters

POLMIL®

ON-GROUND RELOCATABLE SECURITY FENCING

POLMIL® CPNI ASSESSED

POLMIL® PAS 68 RATED
(Test Reports on Request)

POLMIL® MOB ATTACK TESTED

POLMIL® TESTED AND PROVEN

POLMIL® HOT DIPPED GALVANISED FOR COASTAL ENVIRONMENTS

POLMIL® WITH WATER BALLAST

POLMIL® IS A DIVISION OF BLOK N MESH UK LIMITED

THE QUEEN'S AWARDS FOR ENTERPRISE: 2016

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

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

Tel: UK +44 (0) 151 545 3050

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

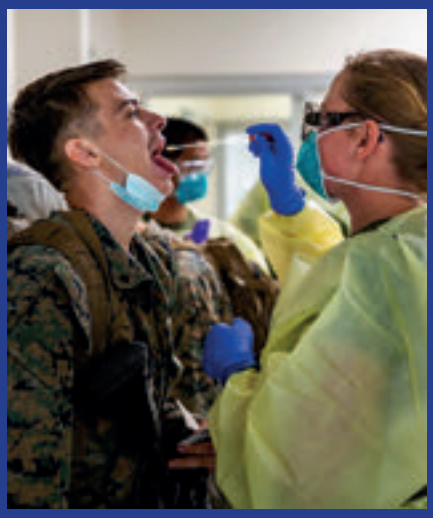
Tel: FR +33 (0) 3.20.02.00.28

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

Tel: Qatar +974 6652 1197

www.polmilfence.com

intersec
Volume 30 Issue 10
October 2020



Cover photograph: US Dept of Defense

Editor
Jacob Charles

Principal Consultant Editor
Maj. Gen.
Julian Thompson CB OBE

Design & Production
jellymediauk.com

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

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

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

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

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

EDITORIAL COMMENT

As we got to press it's been revealed that once again Russian military intelligence services have been caught attempting a major cyber attack, this time on the Olympics and Paralympics that were due to take place in Tokyo this summer. It is understood that the Russian cyber-reconnaissance work included the Games organisers, logistics services and sponsors, although the organising committee noted that there was: "no significant impact observed". Another focus for attacks was the agencies conducting inquiries into Russian sports doping, which comes as no great surprise considering Russian competitors have been excluded from taking part due to persistent state-sponsored doping offences.

Although not wishing to reveal the details of the countermeasures that had been put into place, organisers explained to *The Guardian* that cyber security has been high on its agenda and that it: "has been taking a range of measures and making thorough preparations" for just such an eventuality. Meanwhile, the Kyodo news agency noted that senior Japanese Government officials were also considering lodging a protest with Moscow if attacks were confirmed to have been carried out by Russian agents.

This is not the first time attacks have come from the region, with the UK Government being the first to confirm Russian attempts to disrupt the 2018 winter Olympics in Pyeongchang, South Korea, and it serves as a timely reminder that Russia is not limiting its cyber activities to purely destabilising governments.

Recriminations have been swift, with UK foreign secretary, Dominic Raab observing: "The GRU's actions against the Olympic and Paralympic Games are cynical and reckless. We condemn them in the strongest possible terms. The UK will continue to work with our allies to call out and counter future malicious cyber-attacks." Meanwhile, the US went a step further by indicting six Russian military intelligence officers for their alleged role in hacking attacks on the aforementioned Winter Olympics, and on targets of the NotPetya malware.

Commenting on the attacks, Hank Schless, Senior Manager Security Solutions at Lookout, told *Intersec*: "In the case of something like a large event, attackers will use social engineering to convince targets to download a malicious app under the guise of it being helpful to the mobile user. Sandworm used the PyeongChang Olympics as a platform to distribute mobile malware in the form of malicious apps. These apps can be used to spy on the device users, exfiltrate data on the device, and gain access to any other apps the user logs into on that device."

As Coronavirus restrictions means that vast swathes of the UK workforce continues to find themselves having to do their jobs remotely from home, the need to be vigilant to the threat of cyber attacks remains as high as ever. You can read our feature on how the pandemic has affected the situation on page 32.

Jacob Charles, editor

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

Subscriptions
Annual Subscription Rates: UK £150, Europe £180.
USA post paid US$350
Other Countries air-speeded £220. 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: October 2020

CONTENTS

October 2020 www.intersec.co.uk

intersec

Features

Regulars

FRONTIER PITTS
PROTECTING YOUR WORLD

IWA 14 IMPACT TESTED

HVM
TERRA BI-FOLD GATE

- **WORLD FIRST**
- Double Leaf HVM Bi-fold Speed Gate
- Successfully impact tested to stop a Hostile Vehicle travelling at 30mph
- Aperture up to 8m
- Security Rated
- Minimal Penetration
- Made to order

FOR A SITE VISIT OR QUOTATION
CONTACT TECHNICAL SALES ON
+441293422800 OR sales@frontierpitts.com

Is the UK ready to fight for its waters?

Major General Julian Thompson CB OBE Principal Consultant Editor

The UK media is still dominated by Coronavirus chatter featuring a mix of common sense, panic and nonsense, however the matter of the UK leaving the European Union Common Fisheries Policy at the end of 2020 is beginning to generate some column inches and minutes of air time. What has not attracted much attention is the question: how is the UK to protect its waters?

The UK's territorial waters are the 3 (Nautical) Mile Limit,the historical definition of maritime territorial waters; the 6 Mile Limit, inshore fisheries boundaries – UK vessels have exclusive rights to fish within this area; the 12 Mile Limit, covering a band of 6-12 nautical miles out – only UK vessels or those with historic rights may fish these waters; and the 200 Mile Limit: UK Exclusive Economic Zone (EEZ). The littoral state has the rights to resources in this area – typically fish, oil and gas. But otherwise these are international waters.

There are two further complications: the Median Line, which applies when there is insufficient sea between two states to impose one or any of the above limits, in which case jurisdiction runs up only to the midway point between them; and the Continental Shelf – within certain limits states can claim extra access rights to exploit natural resources beyond the EEZ if the seabed has not fully levelled off.

The core principles governing territorial waters are set out in United Nations treaties and, in particular, the UN Convention on the Law of the Sea (UNCLOS). The significance of the above detail lies in those UN terms providing legal safeguards under international law for the UK once it asserts its sovereign rights after Brexit. At which stage UK waters are not subject to EU agreement for the UK to retain access to its rigs and fish stocks. The EU, both as a body, and in the form of some of its members, is a direct threat to both.

We have already been given a foretaste of the trouble ahead. Recently a French trawler came into Lyme Bay, well within the 3 Mile Limit, towing a massive net and swept up a number of lobster pots, towing them out to sea; destroying the sea-bed and stealing those pots that did not fall off. The Dutch have been pulse fishing within the 6 Mile Limit off the north-east coast of the UK; a pulse trawl emits an electric field above the sea bed to shock the fish: a method that is in effect environmental vandalism.

This is only a foretaste of trouble to come when boats from France, Spain and Holland especially fish in UK waters. There is a historic precedent for the shape the trouble will take provided by the Cod Wars of the sixties when Iceland firmly put the UK in its place. Back then, the boot was on the other foot: the UK was attempting to fish in Icelandic waters, relying on the fact that the Royal Navy was several times bigger than it is now, and Iceland hardly had a navy. Using converted tugs and trawlers, the Icelanders rammed the relatively thin-skinned British warships, cut trawler nets, and barged the intruding trawlers. Eventually Iceland won the 'battle', by threatening to close key NATO facilities on the island. The UK no longer fished in Icelandic Waters.

The UK needs to do more to protect its waters from foreign fishing boats

The UK is not battle-ready and is woefully unprepared for the forthcoming fight. The UK Ministry of Defence should be adopting the three Ps policy. First Platforms: there is a shortage of the right platforms (vessels). Expensive high-tech frigates and destroyers are of little use in a barging free for all; except to launch helicopters, of which more later, and provide overall surveillance of UK waters. Cheap converted powerful tugs, equipped with rams and net cutters with grabs are required. These can be used to cut intruding trawlers' nets, followed by grabbing the net to prevent it sinking, thus killing all the fish and polluting the sea bed. Any attempt by the crew of the intruder to fight back can be dealt with by fast-roping armed Royal Marines down from helicopters launched by warships in attendance or boarding from fast, armed chase boats; the trained Royal Marines and boats already exist and are well practiced in the necessary techniques. It may be necessary to hire or buy suitable tugs, which can be converted.

Next, Planning: this involves review and if necessary updating the current rules of engagement and publicising them widely; especially to potential adversaries. The UK should liaise with the Norwegians, Canadians and Icelanders to learn lessons from their experience with EU nations who have attempted to poach their fish. Planning should include studying the Cod War records to glean any lessons contained therein. Finally, there is a need to conduct robust training and exercises with maximum publicity to ram home the message: "This is what will happen to you if you attempt to steal our fish".

Finally Publicity: as well as the publicity accorded to training and exercises discussed above, there is a need for a clear information campaign to both the UK fishermen and those of countries likely to transgress.

Picture credit: Getty

AI AND THE US ELECTION

Christopher Thissen *considers the part that artificial intelligence played in the recent race for the Presidency*

This Presidential election campaign has seen myriad stories and comments published online by supporters on both sides looking to influence voters. While many were written by humans, an increasing number were generated by AI. Advances in machine learning mean AI generated text is now almost indistinguishable from anything written by people.

While AI created content has many legitimate uses, such as helping overworked journalists write articles, there are instances where it can be used to promote fake news or a disinformation agenda. This can be through making up stories to influence public opinion, burying real news in a deluge of bogus reportage or increasing the number of comments a genuine article receives to make issues seem more popular than they actually are.

AI-generated text is used extensively by businesses to respond to customers that need help on their websites or via apps. Customers input a question into a chat box and the chatbot will respond with further questions to point them in the right direction, such as a specific page on the website or handing them over to a human operator.

Time will tell just how much of an impact AI-generated content had on the outcome of the election

Similar technology is now being used to create original content, such as news articles, blog posts and even creative writing. The latest advancement in AI language modeling technology is GPT-3, developed by OpenAI, which creates articles so realistic they are difficult to distinguish from those written by humans.

AI is now used regularly by big news outlets to write articles that are heavily based on statistical information, such as financial reports or data from sporting events. In fact, around a third of the content published by Bloomberg News is at least in part written by a machine learning program called Cyborg.

In the age of 24-hour, instant-access news, AI is an incredibly useful tool for generating reports quickly. In the world of finance, news outlets are often presented with lengthy company reports, sometimes hundreds of pages long, containing thousands of statistics. Going through this much information manually to find a good news angle can take days. On top of this, there is also the race against competitors to be the first to break the news. Instead, the reports can be uploaded into an AI program that extracts much of the relevant information and creates an article based on this data within minutes. The article is then checked by an editor to ensure the right story has been created from the extracted information. In this way, financial stories can be created at a much faster rate than using traditional methods. A similar process is used in sports journalism to rapidly produce match reports.

KEEPING IT REAL

The likes of GPT-3 are taking this a step further. With GPT-3, AI-generated articles are no longer limited to the structured, data rich formats common in sports and finance. Instead, these next-generation AIs can create realistic articles about nearly any topic, often without requiring additional human intervention or editing.

Troublingly, AI also excels at creating fake news. Such stories are very easy to create – seeded with only a title, subtitle and perhaps a political slant, the AI can generate the rest of the article. Of course, you don't need a sophisticated AI to generate false and outlandish stories that might impact an election – plenty of human-generated fiction went viral during the 2016 election. Rather, the concern is the sheer volume and rapidity of original, convincing content that the AI can create.

With the latest AI, it would be straightforward to devise a list of topics, quickly generate hundreds or thousands of articles with a specific political bent or conspiracy theory in mind, and automatically share the stories on social media or blogs. A study conducted by Oxford University found that roughly half of all news shared on Twitter in Michigan during the 2016 election came from untrustworthy sources. By generating realistic content that is difficult to distinguish from professional journalism, this percentage could rise much higher, burying true news stories in vast amounts of AI-generated fake articles.

The speed and scale at which realistic content may be generated is particularly concerning for issues surrounding election results. As recently as September, the FBI and the Department of Homeland Security issued a joint announcement warning that delays in final tallies may provide an opportunity for foreign actors and cybercriminals to "create or share corresponding social media content… in an attempt to discredit the electoral process and undermine confidence in US democratic institutions." AI's may facilitate rapid generation of articles about voter suppression, cyber attacks on election infrastructure, voter fraud and others in attempt to make the election results appear illegitimate.

Social media platforms – where users can post articles regardless of veracity – are a common target for disinformation campaigns and citizens that get their news from social media sites are especially vulnerable to disinformation. A study by the Pew Research Center found that one in five US citizens primarily get their daily political news from social media, while

THE CONCERN IS THE SHEER VOLUME OF ORIGINAL, CONVINCING CONTENT AI CAN CREATE

a quarter find out what is happening in the world via news websites. This means that a significant proportion of the US population are likely to have viewed news stories that have been partly or wholly generated by AI. In most cases, the consumers would have been unaware of this.

The research also found that those who used the likes of Facebook and Twitter as their main or only source of news were less knowledgeable about current events. This means that not only are these users more likely to be exposed to disinformation campaigns, but also they are less likely to doubt what they are reading or to find other sources to confirm or deny the news stories that appear in their streams.

AI may also be used to generate the appearance of a political movement, further influencing voters. A study by the Pew Research Center of the FCC's 2014 open comment period on net neutrality found that the vast majority of the 21.7-million online comments likely resulted from organised campaigns designed to influence the outcome of the FCC's decision by flooding the board with fake messages.

Most of these fake comments (which comprise 94 percent of all comments) were identified by being copies of other comments. The more realistic comments generated by AI would be more difficult to detect. Comment bots may already be leveraged on social media sites and forums to make specific opinions appear widely held. Rather than influence specific government organisations, these bots would seek to influence public opinion. Research demonstrates that an individual is more likely to adopt a viewpoint when it is held by others in their social network, even if the majority opinion is only an illusion.

Government bodies in the US were clearly concerned about the influence disinformation, including that generated by AI, might have on the election. Earlier this year, those departments and agencies responsible for protecting the nation, including the Departments of Defense, Justice and Homeland Security as well as the FBI and NSA, released a joint statement about disinformation in elections. They warned US citizens to be vigilant about information they consumed and that a well-informed public was the best defence against disinformation.

People power can potentially be a critical weapon in the fight against the spread of disinformation and fake news. Indeed, Facebook is using crowdsourcing in an attempt to remove fake news from its platform.

Yet spotting disinformation requires those that are reading it to have a decent grasp of current affairs, as well as a good understanding of the language in which it is written when it comes to

AI ARTICLES ARE NOW SO REALISTIC THEY ARE DIFFICULT TO DISTINGUISH FROM THOSE BY HUMANS

computer-generated content. OpenAI says that it is possible to tell that an article has been generated by GPT-3 through factual inaccuracies, repetition, non-sequiturs and unusual phrasings, but notes that these indicators may be rather subtle. Given the frequency with which many readers skim articles, such indicators are likely to be missed.

There are others who are taking the approach of fighting AI with AI. For instance, the US Defense Advanced Research Projects Agency (DARPA) is developing the Semantics Forensics (SemaFor) program. DARPA says the project aims to: "develop technologies to automatically detect, attribute and characterise falsified, multi-modal media assets (eg text, audio, image, video) to defend against large-scale, automated disinformation attacks". However, the project is not expected to be functional before 2024.

Denying access to the advanced AI used to generate text is another option for limiting the impact of the technology to produce disinformation. OpenAI has pledged to restrict the availability of the GPT-3 AI for ethical uses only, closely monitoring its API (currently in private beta). But API keys are sometimes shared or accidentally exposed in public repositories. Now that the power of these AI capabilities has been proven, no doubt other groups will try to replicate the results for both personal and political gain. Replication efforts are already underway. Whether threat actors ultimately adopt this type of technology depends on whether it improves their workflow, making it easier to achieve their goals.

Disinformation undermines the democratic process. Controlling the proliferation of fake news will only get harder as AI is used more extensively to create it. It is ultimately down to us as individuals to question what we read and find additional sources to back up any claims that seem far fetched or controversial. This applies to all news and commentary, whether written by humans or machines.

Though it is still too early to tell how influential machine generated disinformation has been on the result of this election, my hope is not very ●

Christopher Thissen is a senior data scientist at Vectra, harnessing the power of machine learning to detect malicious cyber behaviours. Before joining Vectra, Chris led DARPA-funded machine learning research projects at Boston Fusion Corporation.

Comment bots typically use social media to make specific opinions appear widely held

Kestrel TSCM ® Professional Software

Dynamic Trace Autonomous Platform (DTAP-GPS) ™ with Dimensional RF Geo-Location Propagation Modeling!

Signals Intelligence Support System ™

Developed in Canada, Kestrel TSCM ® is well Positioned to Hunt in a Complex Signal Environment!

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

Kestrel TSCM ® Professional Software

A New Powerful Disruptive Technology Combination for the Modern Spectrum Warrior...

The SM200C with Photonic Interoperability Brings Enhanced Probability of Intercept (POI) so you Don't Need Luck to See and Respond to Hostile Spectrum Threat Technology.

The SM200C hardware with SFP+ 10 GbE connectivity is supported by the Kestrel TSCM ® Professional Software for mission critical Technical Surveillance Countermeasures (TSCM) and Remote Spectrum Surveillance and Monitoring (RSSM) ™ roles as defined by the TSB 2000 (Technical) Standard ™ when deployed on a suitable laptop computer equipped with Thunderbolt ™ 3 technology.

The Kestrel TSCM ® Professional Software in Combination with the Signal Hound (BB60C) and (SM200C) has become the Deployment Standard of the Modern Spectrum Warrior within the Private Sector, Government, Law-Enforcement, Military and National Security Infrastructure for enhanced TSCM, RSSM ™, SIGINT and ELINT Roles Worldwide.

Actionable RF Intelligence at the Speed of Light!

Visit www.signalhound.com for Technical Specifications

Our Kestrel ® Certified Technical Operator (CTO) ™ Training is Available in Canada or Hosted at Your Facility!

100% Canadian Scientific Research and Software Engineering Development with Strictly Controlled Operator Centric Software Defined Radio (SDR) Source Code for Proven Radio-Frequency (RF) and Power Line (PL) Offensive and Defensive Monitoring and Surveillance Requirements.

Kestrel-net ™

Actionable **RF** Intelligence

Professional Development *TSCM* Group Inc.

"Innovation is Simply the Beginning..."

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

Telephone: ***1-647-293-7384*** *Email:* ***pdturner@pdtg.ca*** *Contact:* ***Paul D Turner,*** *TSS TSI*

THE PANDEMIC'S IMPACT ON DEFENCE

Picture credit: US Dept of Defense

Matt Medley *explains how the military has found the pandemic instrumental in bringing about efficient digital change*

Military organisations have responded to the global pandemic by cutting back on bureaucratic processes and investing more in technology to ensure that operations can continue while implementing social distance guidelines. Technology has helped organise military personnel across various critical operations, ranging from deployment overseas to assisting in emergency relief and remote access for personnel at home.

For example, the Royal Australian Navy has commissioned research from a combination of academia, military and industry experts to assist the Hunter Class Frigate Program with developing new manufacturing technologies. The innovative programme is targeted towards optimising anti-submarine warfare by providing new frigates to replace the Anzac-class. By providing valuable integrated data insights across the entire supply chain, the programme signifies a shift in the way shipyards could be planned and managed in the future. Additionally, the US Department of Defense is hoping to elevate military operations by trialling 5G technology to see if it can be used to assist digital infrastructure, such as augmented reality in MRO and training.

A recent interview with senior members of the UK military forces revealed that the recent investments in new technology have awarded great success, by allowing for an escalation of programmes in double time across the board. For the Royal Navy, the current pandemic has acted as a catalyst for digital transformation programmes without question. Naval leaders have described that the steps taken during Covid-19 have the potential to impact programmes relating to all areas of the force, from support systems for ships, to the estate and personnel. The Royal Air Force has also reported an increase in efficient operations as a result of its accelerated 3D Printing programme.

The recent restructuring of military operations, which has seen digital transformation take a crucial

Questions are now being raised about whether traditional processes have actually been hindering productivity

newfound role is not an anomaly, but rather a pattern that is being replicated within organisations across many industry sectors. While the economic concerns that have spawned from the Coronavirus pandemic may not be credited entirely for this recent trend, there is no denying that it has expedited the process. Recent IFS research reports that in response to the pandemic, over 50 percent of respondents across multiple industries are looking to increase expenditure on digital infrastructure.

The Coronavirus pandemic has not only accelerated technology adoption, but certainly for the global military organisations, it has allowed time for a reflection on traditional practices and a re-assessment of current operations. In turn, there is no doubt that Covid-19 will deliver numerous advances for the defence industry.

In particular, four key areas can be highlighted to demonstrate how the economic and business effects of the pandemic are acting as the driving force behind the technology transformation within military organisations.

EMBRACING MODERNITY

Prior to the pandemic, flexible and remote working options were, for the most part, an unexplored and dubious prospect. In addition to a long-standing tradition of strict practices within the defence sector, there has been a distinct reluctance from higher-ranking leaders to embrace remote working due to the deeply ingrained bureaucratic system of in-person, direct management and leadership.

However, challenges created from the Coronavirus pandemic have meant that a new working paradigm is now crucial for survival. With remote and flexible working proving to be efficient means of operating, questions are being raised about whether traditional processes and policies within defence organisations have been hindering productivity in the past.

With processes once deemed necessary now coming under scrutiny in a post-Covid world for being forces of habit – new efficiencies are being explored. For instance, electronic signatures generated by automated workflows are quickly replacing the traditional method of requiring physical signatures on formal documentation – allowing wait time between approval stages and total throughput time to be drastically reduced. Additionally, many organisations are finding that lengthy approval workflow processes tend to disempower their employees to act. By reducing the number of total approval steps and raising authority thresholds for lower-level managers, the new measures have incentivised employees to act, while also freeing up valuable executive time to focus on more pressing strategic matters.

If the defence sector continues to embrace change and realise the benefits of non-traditional working, it can learn valuable lessons from the pandemic. The defence industry has the opportunity to further streamline processes and increase efficiencies across organisations – all while empowering the workforce to focus on results.

WORKFORCE PRODUCTIVITY

The belief that digital transformation and automation would lead to a cutback on personnel was another reason why many leaders within military organisations were hesitant to embrace new technological changes. This has been delaying the progress of administration and headquarter reform for years.

In practice, digital transformation actually optimised workforce efficiency as opposed to the previously feared personnel cuts. This has two main benefits. Firstly, with additional pressure to reduce company expenditure being exacerbated by the Coronavirus crisis, companies want to hold onto the personnel they have so heavily invested in. This preserves capacity for business to ramp back up as the crisis resolves – while protecting the livelihoods of their workers and families. Secondly, removing waste through densification of value-added work results in real time and cost savings that can be reinvested into other activities.

THE ROYAL AIR FORCE HAS REPORTED AN INCREASE IN EFFICIENT OPERATIONS THANKS TO 3D PRINTING

In comparison, defence manufacturers face the predicament of personnel cuts daily. Despite rapid advances in Industry 4.0 technologies, these companies must still retain large human labour forces that cannot work from home and are often hired to support specific programmes. Those skilled labourers must often be delegated to other programmes or let go to preserve cash when programmes are delayed during times of uncertainty such as Covid-19, budgetary shortfalls or other severe disruptions. The companies best able to match their labourers to value-added work have the best chance of retaining them, preserving critical skillsets and the right technology solutions can help highlight those opportunities for workforce realignment.

The pandemic has been a vital period for global military organisations to resolve previous concerns surrounding the management of increasing pressures to decrease workforces and the reduction of admin costs. The adoption of digital transformation and automation within an organisation streamlines administrative tasks and means more efficient back-office processes. Consequently, more resources can be reassigned to the operations that matter – moving resources from non-value-added processes so core operations can increase efficiency with no net change in force size.

REMOTE ACCESS

Planned and unplanned are the two forms of connectivity and bandwidth issues that can face both civilian and defence organisations. Most organisations experience planned or unplanned outages on occasion for system maintenance, natural disasters, physical damage or hardware failure, and in the case of defence organisations, physical attack. On these occasions, organisations will have contingency response plans for these scenarios and can be quite efficient in restoring their networks afterward.

What makes defence organisations unique is the need to perform prolonged operations, often in unfriendly territory, with no connectivity due to the lack of forward infrastructure to maintain secrecy. In this scenario, a critical feature of the operation is a robust Disconnected Operations solution – capable of distributing and reconsolidating data and technical records when connected and operating autonomously when not connected.

Connectivity has become more complicated as the demand for remote work across the world has increased. Remote data access and the ability to continue working while offline and later reconnect and resync will now be sought out by not only civilian companies, but also military organisations. As a formal risk mitigation technique, organisations need to harden their network solution with a true Disconnected Operations mode. Robust Disconnected Operations capabilities can capture, store and resync asset and workforce data regardless of connectivity. Even with workforce and assets globally distributed, robust Disconnected Operations could be the difference in a military's ability to not just recover from planned or unplanned outages, but rather continue operating seamlessly throughout.

PRIORITISING COMPLIANCE

While in the past compliance was associated with regulations and red tape, now it has the potential to determine the defence sector's recovery in a post-Covid world. Compared with the rapid decline and slow recovery underway in commercial aviation, government defence spending has remained relatively stable, with large multi-year contracts still being awarded for major new programmes – placing defence organisations in a secure position to recover from the current global crisis. Only those competitors with the right combination of demonstrated excellence across a variety of compliance areas such as ITAR, FedRamp and CMMC are in a position to compete on certain contracts.

By understanding the critical focus on regulation, defence organisations must keep compliance top of the priority list if they are to transfer to remote operations on a more permanent basis. Therefore, remote operations require flexible software architecture and filing to adhere to regulations. Compliance is also the reason that many A&D organisations are wary to adopt cloud-only ERP deployments. A recent IFS webinar attended by key decision makers within aerospace manufacturing revealed that only 3 percent of respondents deploy their ERP software only using the cloud – whereas 64 percent said they use their software either on-prem only or a mixture of on-prem and cloud-based deployments.

For defence organisations to continue to embrace remote working and unlock further efficiencies while remaining compliant they need a tailored solution. With a managed cloud or secure hybrid enterprise software environment for critical compliance areas such as ITAR, organisations can explore remote capabilities knowing compliance is not an issue.

THE PANDEMIC HAS ALLOWED TIME FOR MORE REFLECTION ON TRADITIONAL PRACTICES

For an industry often identified by its long-standing traditions and rigid processes, the Coronavirus pandemic has accelerated the speed in which defence organisations have actioned transformations that were previously only blueprints. This acceptance of digital transformation, with the support of capable enterprise software solutions, will bring extensive benefits to the industry for years to come. For military organisations, the increased efficiencies, flexibilities and streamlined processes, will be benefits that they will continue to reap long after the Coronavirus pandemic has ended ●

Matthew Medley, senior product manager, ensures IFS solutions meets the demanding needs of defence service and support organisations, defence manufacturers and defence operators and helps bring these solutions to market.

A new working paradigm is now crucial for survival

Picture credit: US Dept of Defense

MESA™

A new spectrum analyzer with Broadband Utility.

Detecting and locating illicit transmitters requires an agile, portable, handheld spectrum analyzer to measure power and frequency of unknown transmissions. The new MESA™ (Mobility Enhanced Spectrum Analyzer) delivers precision, high performance, and versatility for assessing RF energy in a variety of environments. The MESA™ is a handheld RF receiver that detects and locates illegal, disruptive, or interfering transmissions throughout wide frequency spans up to 6GHz, or 12GHz with the Down Converter Antenna.

International Procurement Services (Overseas) Ltd

sales@intpro.co.uk

118 Piccadilly London W1J7NW

phone: +44 (0)207 258 3771

fax: +44 (0)207 569 6767

- **Portable**
- **Efficient**
- **Full touch screen control**
- **Full complement of antennas/probes**
- **Sweep modes:**
  Spectrum View
  SmartBars™ (Patented)
  Mobile Bands
  Wifi
  Bluetooth®
- **Sweep Speed**
  >200 GHz/second
- **Operating Freq. Range**
  10 kHz - 6 GHz /*12 GHz
- **Variable Resolution Bandwidth**
  0.0380 kHz to 312.5 kHz
- **Instantaneous Bandwidth**
  25 MHz
- **DANL - Noise Floor**
  500 kHz RBW
  with Pre-amp:-102 dBm
- **Detection**
  RF, Carrier Current, Acoustic Leakage, IR/Visible Light, Ultrasonic
- **Spurious Free Dynamic Range**
  81.6 dB
- **AM/FM Audio Demodulation with filter options**
  Auto, 200kHz, 20 kHz, 5 kHz
- **Case/Contents Weight**
  15lbs. / 6.8kg

*Down Converter Antenna

GOING SOLO

Craig Swallow *on the challenge of managing the safety of lone workers*

Picture credit: iStock

Within any organisation, the responsibility to protect employee safety and well-being should be a given, but there are cost and productivity benefits to be realised, too. Many different types of workers will become more productive and value their employer more if improvements to their safety standards are adopted. This responsibility should be naturally embedded and form part of an organisation's goals and planning, as employee safety and security is paramount.

When planning, understanding the different risk profiles that staff have needs to be taken into consideration. For example, the risks for a lone worker are different from those of an executive travelling the globe and differ again for someone now working from home. These risks need to be assessed when analysing and implementing safety measures to protect employees.

Significant material costs associated with an incident can arise if the correct safety measures are not in place because management hasn't addressed worker safety risks. In the UK, for example, cases where suitable processes and practices have not been implemented have seen organisations found guilty of corporate manslaughter (as a result of serious management failures that result in a gross breach of a duty of care) under the Corporate Manslaughter And Corporate Homicide Act. The act came into force in 2007 in the UK and can impose unlimited fines and imprisonment on guilty parties.

In 2015, two organisations were collectively fined over £1.1-million and individuals found negligent sentenced to between eight and 12 months in prison, following the death of a lone working employee who fell through the discoloured skylight of a warehouse. This incident could have been avoided had the correct safety procedures been implemented.

Similar approaches to increased fines and possible jail time are being seen in a number of other countries, where an increasing number of health and safety legislations are being introduced.

A point of interest can be added to a location on a map's dashboard in case an emergency should arise

Safety consideration of employees aside, organisations have a brand reputation to build and maintain – and improve, if necessary – a continuous process that can take years. When incidents do occur, the detrimental effects to brand awareness and reputation can be catastrophic where convictions for corporate manslaughter are made – or the employer organisation has breached the terms of the Health and Safety at Work Act 1974. Reputations can be destroyed overnight.

An app-based GPS monitoring system can accurately locate employees in known danger or be used to help advise them if they move into at-risk areas. If an employee is in the vicinity of a terrorist attack or industrial accident, for example, the employer organisation should be able to monitor their location and check their safety status. The organisation can also communicate with the employee to understand their situation and give advice or organise help via emergency and security services if necessary.

The app – an example is the Vismo App – can operate on all smartphone and satellite phone platforms. Satellite phones and trackers are especially useful in areas where mobile coverage is minimal or unavailable.

The system comprises, at the employer's end, a web-based monitoring system, with a dashboard view, allowing location monitoring and communication with app users. At the employee's end, the app is activated on their smartphone device and runs in the background while automatically updating location fixes.

A key aspect of a monitoring system is the ability for lone workers, including employees travelling anywhere in the world on their own or as part of a disparate group, to alert their employer in the event of an emergency. Employees can do that through activating their app's panic button.

That action will automatically trigger a live audio recording that's sent to the system administrators, enabling them to understand the situation better and respond more effectively. They can share information with emergency and security services where appropriate. The system and those services use common mapping software and are therefore able to rapidly share information and liaise about emergency responses, rescue and evacuation included, should they be required.

AN APP-BASED GPS MONITORING SYSTEM CAN ACCURATELY LOCATE EMPLOYEES IN DANGER

Many monitoring systems have geo-fence capabilities, enabling a virtual fence to be placed around a certain area where an employee may be travelling to. As soon as lone workers – travelling executives, journalists and NGO staff or volunteers included – enter or exit one of these virtual fences, system administrators will be notified via the app and given advice if necessary.

Geo-fences can be placed around high-risk areas including airports, war zones and areas or cities of political instability; or a place of safety, for example the hotel where an app user is staying.

To enhance lone worker safety in such sectors as estate agency, district nursing, home care, hospitality (hotels *etc*.) and dispute resolution enforcement, or wherever life can be in danger, a timed check-in function in the app allows users to submit their immediate location information to their system administrator. Workers in sectors like these face increased risks whenever working alone on premises other than their employer's, particularly when meeting people they have not met before. Ditto employees in zones of war and political instability.

The 'timed' element is, broadly speaking, a safety timer. It allows a user to allocate a timescale – eg 30 or 45 minutes or more to a job, and automatically triggers an alert if the user doesn't explicitly cancel it by checking out (after first checking in). If a user doesn't check out, an alert will be triggered and the administrator notified via SMS and email.

Enforcement officers in particular can be faced with potentially distressing and often confrontational situations when entering – or leaving – a property during the enforcement of a court order. In the estate agency, home care and hospitality sectors, employees working on their own can be vulnerable, highlighted

in 1986 (and borne in mind since) after the continued disappearance of estate agent Suzy Lamplugh, when she was due to meet a client at an empty property and did not return from that appointment.

In any situation, at any time and regardless of the app user's location, an administrator can seek 'proof of life' from the user by asking – in case the device has fallen into the wrong hands – questions that only they can answer correctly.

Other features of a monitoring system can include incident management and mass notification functions, both overseen by system administrators who can see them on their dashboard.

Incident management allows organisations to alert travelling staff to incidents that are a threat to their well-being. Alerts are sent via mass notification. Incident management integrates external data incident feeds into the system, ensuring that users of the app in any affected area are automatically identified and then rapidly notified via mass notification.

Mass notification allows the administrators to quickly send potentially critical information via personalised messages. The lone workers can respond with their safety status, enabling the administrators to quickly identify anybody in need and provide further assistance. The messages can be sent to either a wide group of people, workers in a specific geographic area or individuals, with message response options that can be customised to the situation.

Another feature, also visible on the dashboard, is points of interest (POI). A POI can be added to a location on a map's dashboard to help administrators gain a deeper understanding of an employee's location should an emergency arise. A POI can be anything, for example offices, a shop, train station or airport *etc*. It is a point on a map, with a radius around it of the administrator's choosing: 100 feet, 100 metres, several miles/kilometres or more.

Implementing a location-based monitoring system can provide benefits to employees and organisations alike. From a legal perspective, it can help employers meet their legal and moral duty of care obligation to employees, and if an incident was to occur, an efficient communication process is already ready in place to be used. Two-way communication not only helps workers feel supported, but can more easily result in rescue.

Other benefits include reducing costs in areas of the organisation and increased productivity. A policy of supporting and protecting lone workers can help them feel more valued, and so increase loyalty. This result can reduce employee turnover and related costs including the cost of recruiting and training new starters. Increased insurance premiums for a mobile workforce can be avoided, and productivity might increase – certainly not drop if lives are saved and injuries avoided. Investing in lone worker safety has a very clear ROI in a number of respects.

By avoiding an incident, the employer organisation will also have escaped financial costs through loss of time at work, business interruption and any penalties from not complying with legislation. Or, by minimising an incident's impact, any financial costs and penalties are likely to be greatly reduced.

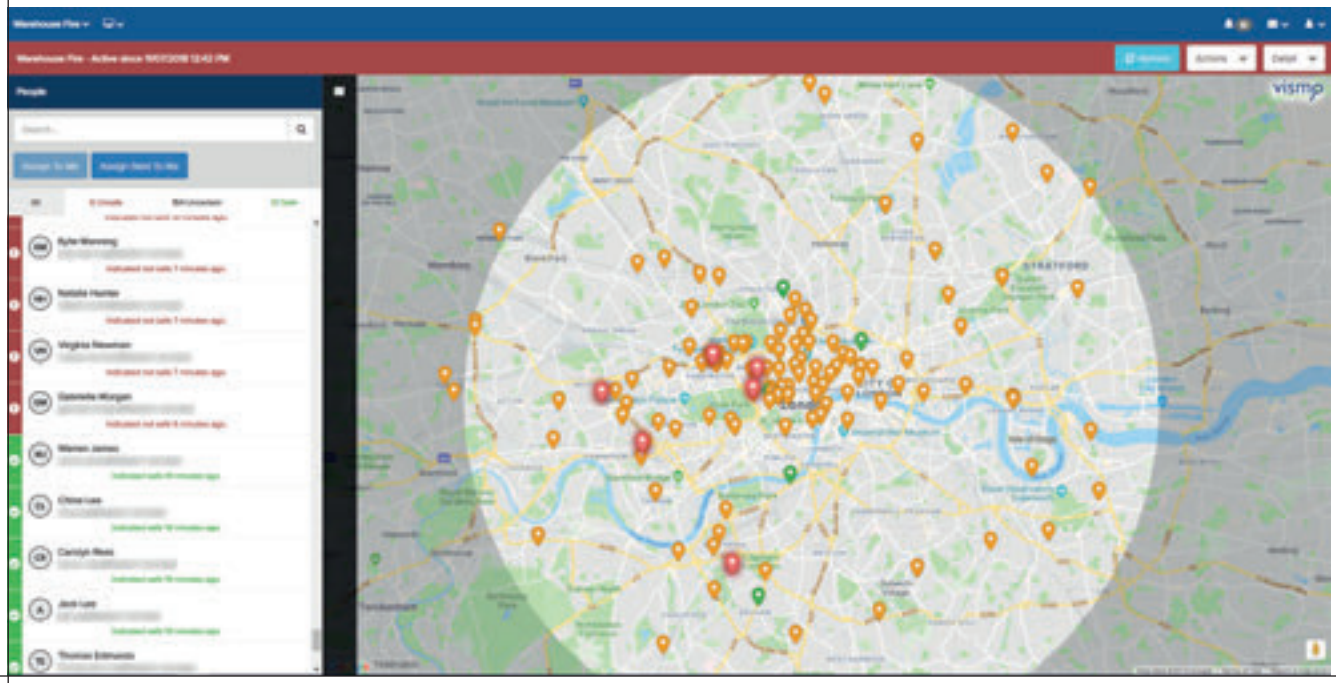
Intangible factors are harder to measure accurately, but can have a significant impact through damaged or ruined brand reputation. Additionally, it's generally accepted that workers who feel safer are happier, and happier workers tend to be more productive. Staff well-being is a major focus point for many employers. Improving staff safety, and being seen to do so, will help staff feel better about their employer and their work.

To conclude, organisations should have health and safety measures at the forefront of their goals and planning. The safety of employees affects many different parts of an organisation, not least the recruitment function within HR, brand reputation, the financial implications of an incident and, most importantly, the lone workers who need to be protected.

Mobile technology has been at the forefront of meeting various health and safety and corporate legislations and will continue to evolve to ensure that duty of care is optimised as much as is possible at the time. Due to the global COVID-19 pandemic, technology has to evolve with the ever changing situation. Implementing a monitoring solution to check the well-being of remote workers or understand how an employee is feeling could be the way forward ●

Craig Swallow is the CEO of Vismo, a lone worker solution provider. With more than 18 years of experience within the lone worker security industry, he has wide-ranging knowledge in lone worker service innovation, marketing and business strategy.

A key aspect of monitoring systems is the ability for lone workers to alert their employer in the event of an emergency



Picture credit: Vismo

ELECTRONIC COUNTERMEASURES

IPS EQUIPMENT & SWEEP TEAM SERVICES

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

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

Looking for a

VIDEO POLE CAMERA
2.0 INSPECTION TOOL

EDD-24T NON LINEAR
JUNCTION DETECTOR (HANDHELD)

TSCM TRAINING
COURSES &
CERTIFICATION
UK/US/GLOBAL

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

Rapid Quote:

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

needle in a haystack?

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

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

***TALAN 3.0* DIGITAL PHONE ANALYSER**

RAKSA IDET SELECTIVE RF DETECTOR (MICRO TSCM DEVICE)

ORION 2.4 HX NON LINEAR JUNCTION DETECTOR

TSCM Equipment supply, training and de-bugging services

The preferred choice of Government & Law Enforcement Agencies worldwide.

Web: www.intpro.com

COVID – A COMPLEX CATALYST

Justin Crump *highlights several knock-on effects of the global pandemic that organisations need to be ready to respond to*

It is a common observation that it is not the first crisis that breaks organisations, but rather the second one that provides the biggest challenge. This is a timely thought for companies already struggling to deal with the huge challenge posed by Covid. While it may not be a universally popular consideration at the moment, the reality is that organisations of all sizes need to be prepared for the acceleration of a wide range of underlying issues that are being exacerbated by the virus. The consequences of which pose clear threats to staff, market access, assets, reputation and their technological base.

The effects of the Covid-19 pandemic need to be put in context in order to predict 'what next'. Here are the most significant factors:

Geopolitics: 67 percent of countries face increasing political risk. Geopolitical tensions such as the Russo-Saudi oil price war and strained US-China relations have been fuelled by the Covid response, adversely impacting supply chains, significantly increasing the risk of state-sponsored cyber espionage and intellectual property theft. These tensions are testing business ethics and forcing some organisations to pick sides, while corporations and Non-Government Organisations will increasingly become pawns amidst rising tensions. Issues such as Brexit have been somewhat overlooked to date, but will fast come back into the limelight later this year.

Civil unrest: 46 percent of countries face surge in civil unrest. Rising unemployment, the fast-track introduction of automation affecting manual jobs, societal tensions, poor climate policies, human rights violations, food shortages and corruption are increasingly mobilising people to take both virtual and physical action. This will likely peak into 2021-2 as the effects of the pandemic become more apparent – and, as is usual with any large economic shock, it takes time for the impact to wash through.

Lone actors: More than 10 significant incidents this year, in France, the US, Canada, the UK, the Maldives, Germany, and Israel. The risk of attacks from lone actors continues and it remains harder for security services to intercept this threat, especially given the use of basic tactics such as stabbings and run-over attacks using vehicles. Lockdown mitigated incidents, but existing mental health conditions have been magnified by isolation, and there is a steadily increasing chance of individuals being recruited online by far-right or Jihadist groups. Moreover, security forces are heavily distracted by the ongoing demands both directly and indirectly caused by Covid, and budget pressures are likely to have further impacts in 2021-2.

Diversified crime: 51 percent of countries are predicted to face increased crime. The crash of the wholesale drug market, closed borders and difficult logistics has done nothing to stop activity. Instead, organised crime groups have used lockdown as an opportunity to diversify, taking advantage of distracted enforcement agencies. Virtual kidnappings have risen, while cybercrime, such as ransomware attacks on corporate systems, has increased by more than 300 percent in hard-hit Brazil, Colombia and Argentina. Businesses are having to adopt new methods at a much faster rate in order to protect their people, assets and data from the rapidly evolving threats.

51 PERCENT OF COUNTRIES ARE PREDICTED TO FACE INCREASED CRIME FOLLOWING COVID-19

Sibylline's Annual Forecast for 2020 was released in November last year – well ahead of the pandemic (although this is, of course, a scenario that everyone long knew was possible, and some CSOs have won major plaudits from their boards for running readiness exercises based on this eventuality)! The Forecast highlighted eight key trends, and it is educational to see how these have now evolved to become even more applicable than ever due to Covid.

Picture credit: Getty

Budget pressure and stretched resources have made post-Covid life hard for the police

Firstly, the principle characteristics of a disruptive and unpredictable US have been evident over 2020, with the Trump administration's continuing use of trade policy as a political tool undermining relations with both China and the EU. Confrontational rhetoric around the origins of Covid-19 is indicative of the President's tendency toward personality-driven and unpredictable policy positions. January's assassination of Iranian General Qasem Soleimani was reflective of Washington's willingness to exchange short-term regional disruption for weakening a strategic adversary, and the competitive environment ahead of the US elections implies that this trend will continue.

2020 has, of course, also seen an increasingly strategically assertive China**,** despite the Covid-19 pandemic and the country's first economic contraction in decades. From consolidating power in Hong Kong and the ongoing repression of the pro-democracy movement in the territory, to its confrontational policies in the South China Sea, Beijing continues to assert itself within the Asia-Pacific region to the detriment of ties with neighbours (particularly Taiwan, India, and Vietnam). Internationally, China is increasingly positioning itself against the US and its allies, as evidenced through recent confrontations with Australia and the UK. US-China tensions are now unlikely to abate, whatever the outcome of the leadership race in Washington, making this a lasting area of challenge for global companies.

Policy flux and polarisation in the G20 has featured prominently over the year so far, with states forced to enact a range of policy solutions to the economic crisis triggered by the virus. Discussions over longstanding policy questions such as the outcome of Brexit and efforts by oil-producing states to diversify their economies have been side-lined, with further pandemic-related policy flux likely in the second half of the year. This means that larger decisions will potentially be rushed or viewed through an inadequate prism, as leaders struggle to cope with purely national issues. "Vaccine nationalism" will become an increasing trend.

The trend of rising authoritarianism has largely been sustained, with leaders in Poland and Hungary exploiting the pandemic to rollback democratic norms, while Russia's constitutional amendments have further consolidated the Putin regime. Authoritarian states, particularly Russia and China, have used the pandemic to harvest citizen data and augment surveillance. Moreover, it is no surprise that these states are rushing vaccines into production ahead of adequate testing, in part to use them as

diplomatic bludgeons. This signifies the global influence struggle to come.

Destabilising civil unrest was largely stymied by lockdowns. However, issues such as inequality and handling of the pandemic have seen the frequency of protests once again rise, while the consequences of years of stagnation have been highlighted in Lebanon and Belarus. Pre-Covid-19 protest movements in France and Chile have not abated, and anti-government demonstrations in eastern Russia suggest longstanding sources of unrest are unlikely to subside into 2021.

The threat of privately operated assets being used as proxy targets has persisted over 2020, driven largely by the deterioration of relations between China and the US. Instances of IP theft have increased year-on-year, with the US' designation of two Chinese tech firms as national security threats and the UK's exclusion of Huawei from its 5G network indicative of the increasingly politicised environment for private assets.

Trends observed around terrorism and militancy at the start of the year have continued. The far-right terror threat was compounded by a February shooting in Hanau, Germany, that left nine dead. While the emergence of the anti-government Boogaloo Bois in the US is likely to sustain the extremist threat. Islamist-affiliated militants remain an enduring challenge, with the rudimentary knife attacks in London and Reading, UK, reflecting the sustained lone-actor threat.

Finally, while direct anti-corporate activism as seen in 2019 through movements such as Extinction Rebellion has so far been limited in 2020, the trend continues to evolve. The Black Lives Matter movement focused attention on corporate diversity and scrutiny on companies' response to protests. Environmental activism is unlikely to abate given the activists' willingness use the Covid-19 crisis to influence any 'new normal', with protests against the wider carbon value chain likely to see the range of corporate targets increase into 2021.

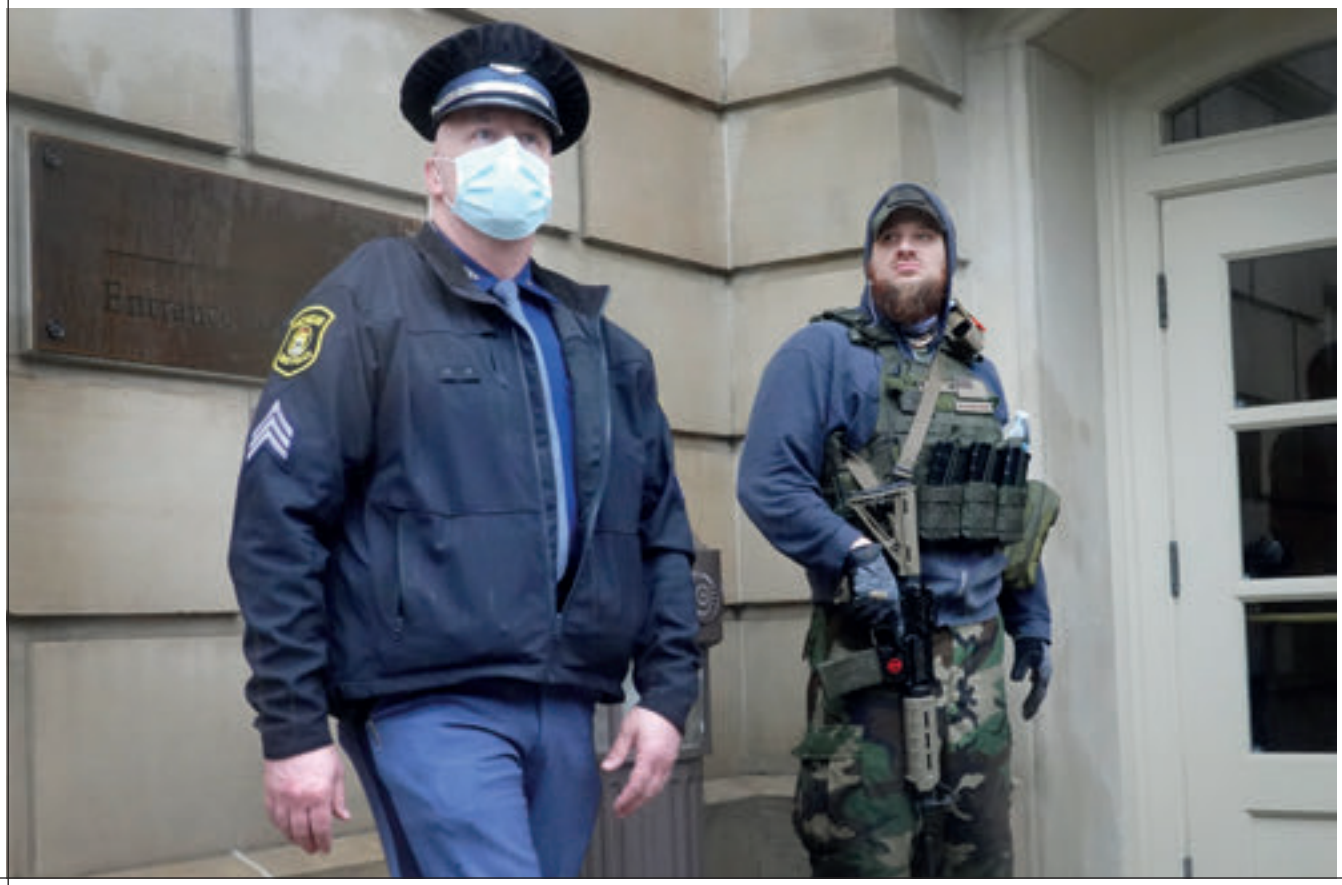
This highlights how we are now at an inflexion point, with some governments offering the possibility of wholesale change towards a 'green economy' and levelling perceived injustices, while others choose instead to consolidate power. Of course, worthy motives may yet fall prey to the harsh realities of economic failure, especially as states struggle with mounting debt and an array of security challenges.

In this light, it is important to note that the socio-economic impact of the Covid pandemic has yet to take full effect – the current phase is, really, just the end of the beginning. Rising unemployment and hardship, as well as an increasing focus on inequality, will undoubtedly serve as a key trigger for unrest across the world on a greater scale than we are yet seeing. Young adults and 'blue collar' roles are set to be most affected, worsening longstanding grievances among marginalised communities.

In this challenging environment, organisations and states that take an irresponsible or uncompassionate stance on redundancies, climate change and equality are set to become targets. This underscores how leaders must take a proactive, intelligence-led approach to decision-making and do the right thing for all of their stakeholders, amidst an increasingly complex and uncertain environment. As security professionals, it is our role to present a clear situational picture and provide adequate "decision support" to enable our organisations not only to survive, but also to thrive, during the coming period of turbulence ●

Justin Crump, is CEO of Sibylline. He is an acknowledged authority on business intelligence, global risk analysis and governance, the Vice President of the Association of International Risk Intelligence Professionals (AIRIP); a member of the UK Risk and Security Management Forum; on the steering group of the International Security Foundation.

A disruptive and unpredictable US has been evident during the last 12 months, including right-wing militia taking matters into their own hands



Picture credit: Getty

TSCM & TACTICAL SECURITY EQUIPMENT & TRAINING

Delivered by the Global leader in Cellular Threat Detection

The threat of Eavesdropping & Cyber Eavesdropping has never been greater

As the world's largest TSCM company, QCC is the clear choice for TSCM equipment procurement & training - Why?

We don't just make and sell TSCM equipment, we use it & understand it.

QCC solutions include:

TSCM & Tactical IMSI Capture solutions - **SearchLight Plus** & the new **BlackLight**.

TSCM equipment from all leading manufacturers, to cover all threats with training.

QCC's other proven and ISO certified services include:

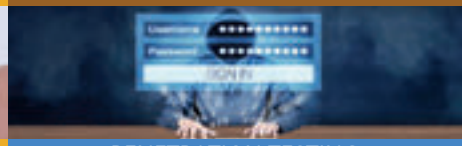

TSCM


CYBER TSCM


CYBER FORENSICS


MOBILE PHONE FORENSICS


SECURE COMMUNICATIONS


PENETRATION TESTING


PROTECTIVE SECURITY


EQUIPMENT

TRAINING

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

SINGAPORE OFFICE
T: +65 3163 7100
E: contact@qccglobal.com
W: www.qccglobal.com

THE BRITISH ASSESSMENT BUREAU ISO9001 Certification No. 193274
THE BRITISH ASSESSMENT BUREAU ISO27001 Certification No. 197110
THE BRITISH ASSESSMENT BUREAU ISO14001 Certification No. 197108
THE BRITISH ASSESSMENT BUREAU OHSAS18001 Certification No. 197109

QCC – Keeping your business, ***your*** business !

MGT europe

DroneTERMINATOR

USING EVOLUTION JAMMER TECHNOLOGY

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

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

JAMMING FREQUENCIES:

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

FEATURES:

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

MGT Europe www.mgteurope.com

SCANNA

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

SCANSILC EOD - DR X-RAY

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

SCANX SCOUT - CR X-RAY

A must in every bomb truck!

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

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

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

XR150

XR200

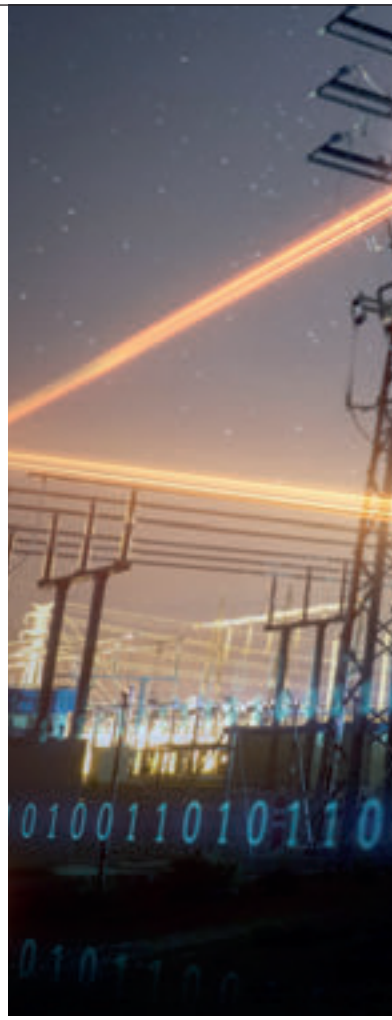
XRS-3

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

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

POWER PLAY

Sanjay Chhillar, Dale Geach and Chaitanya Bisale
examine electrical grid modernisation and emerging cyber risks



Traditional grids involving electromechanical technologies to manage predictable and unidirectional flow of electricity from big power plants to consumers have been reliable for many decades with investment in resilience focused towards large items of plant. Today, with power flows becoming less predictable in the grid, electricity utilities are now recognising the strong need for, and huge benefits of, modernising and digitising their operations. Leveraging industrial Ethernet and IP-based communication and international standards for substation automation, such as IEC 61850, are delivering benefits and enabling a range of new opportunities in support of: real time situational awareness of the grid state; load prediction and shift; rapid fault isolation and recovery; integration of renewables and distributed energy resources (DER); achieving net zero carbon emissions targets; reducing employee health and safety risks and enabling remote maintenance and monitoring capabilities to name just a few. The decentralised model enabled by smart grid technologies provides greater flexibility in the event of disruptions as well as potentially reducing the time needed for recovery, as it might be possible to localise disruptions.

However, grid modernisation also exposes it to greater cyber risks due to increased connectivity and inherent vulnerabilities in legacy systems. It has become vital and urgent to address cybersecurity in smart grid design and within legacy systems while the grids are being modernised.

HIGHLIGHTING VULNERABILITIES

Recent exposures and attacks on grids and industrial networks around the world have highlighted the vulnerabilities that can be exploited by bad actors, including nation states and cyber criminals. Intelligence agencies and governments in the USA, UK, EU and elsewhere have identified cybersecurity of their critical national infrastructure (CNI) as one of the top threats to their national, social and economic security. In fact, the EU was concerned enough to introduce the Network and Information Security (NIS) Directive and, in a move to protect CNI, President Trump signed an executive order banning American grid operators from buying and installing electrical equipment manufactured outside the US.

Though the newer industrial control systems (ICS) and operational technology (OT) systems that are used to monitor and control electricity grids and micro-grids as well as industrial processes can be securely designed and hardened, legacy ICS/OT will still have inherent security issues, such as the use of insecure protocols and the inability to enable secure passwords, which create greater cybersecurity challenges.

Due to the increase in adversary capabilities, the critical role of grid infrastructure to nations and the potential for inherent vulnerabilities in ICS/OT systems, electricity grids make attractive targets for bad actors, including nation states, terrorists and cyber criminals. Depending on bad actors' motives, cyber attacks on CNI could be used for geopolitical advantage by nation states to disrupt or destroy power supplies or for ransom by cybercriminals. Unauthorised access to grids and industrial networks can result in widespread outages, creating loss of productivity and revenue, health and safety risks and impact on society due to disrupted transportation, gas, water and other essential services.

In recent cyber attacks, bad actors have demonstrated their capabilities and continued willingness to conduct malicious adventures against CNI. A few examples include STUXNET cyber attack on a nuclear facility in Iran causing equipment damage and BlackEnergy (2015) and Industroyer/Crash Override (2016) cyber attacks on Ukrainian utilities causing power outages. In 2017, WannaCry ransomware attack disrupted services/operations globally across multiple sectors including Health and utilities; and NotPetya, a ransomware attack that prevented Maersk from locating and routing shipments, resulting in a reported loss of up to €300-million, also hit many local utilities. In 2018, TRITON/TRISIS, allegedly the first malware specifically designed to attack safety systems, was reported to have hit industrial plants in the Middle East. A ransomware attack on a US natural gas company in 2020 caused a pipeline to shut for two days.

MAINTAINING CYBER RESILIENCE ACROSS ELECTRICITY GRIDS IS A MAJOR CHALLENGE

In most cases, unless ICS/OT systems are directly connected to the internet, which is possible and can be discovered using the Shodan online search tool, bad actors usually gain initial access to a targeted organisation's ICS/OT system via exposed IT systems, or by exploiting a supplier's network. In many cases, utilities and other industrial organisations don't have the capabilities or expertise in "real-time visibility" of their ICS/OT networks to proactively identify vulnerabilities or detect malicious activities and prevent incidents. For example, in the case of the cyber attack on the Ukrainian utilities in 2015, attackers used

Picture credit: Siemens

Modernisation exposes the grid to greater cyber risks due to increased connectivity

spear-phishing techniques to send a malicious Word document via email and compromised an employees' computer before pivoting to their ICS/OT networks. Attackers used compromised credentials and remained in the networks for six months, without getting caught, before causing the outage in December 2015. The attack demonstrated the attackers' sophisticated capabilities and exposed the utilities' inadequate preparations to detect and prevent sophisticated cyber attacks. As a best practice, ICS/OT networks should be segmented from business/office IT networks but in the example above, attackers were able to exploit improper segmentation, design flaws and inadequate security controls to pivot to and gain foothold in their ICS/OT network.

Lack of visibility and monitoring, insecure legacy protocols, unpatched systems, inadequate access controls and improper segmentation plus a shortage of ICS/OT cyber expertise are key challenges for many utilities and other industrial organisations.

Maintaining cyber resilience across electricity grids and CNI ecosystems is a major challenge for governments, owners and operators of essential services. The OT/ICS systems were not originally designed with cybersecurity in mind, so we must live with inherent vulnerabilities in legacy systems for some considerable time to come. Cyber threats are a new reality in today's hyperconnected world, but any panic or fear due to hype must be avoided. With the right strategy; cross sector collaboration; partnerships with governments and intelligence agencies; and board accountability, threats can be adequately addressed and organisations can prepare for and handle any emergency.

For effective cybersecurity measures, international standards and best practices such as IEC 62443, NIS Directive, NERC CIP, NIST CSF, MITRE ATT&CK framework for ICS, *etc*. may be very helpful. In a realistic world, there is nothing even close to 100 percent protection, so organisations need to be pragmatic in their approach. It is important to understand the threat landscape and prioritise mitigations based on risks and impact to critical systems rather than trying to implement everything in one shot. In the ICS/OT world, we must be aware that patching of all systems may not be realistic and segmenting an existing OT network may not be feasible. Therefore, leveraging passive monitoring solutions for gaining visibility into assets, communication flows and detecting anomalies and intrusions may be a powerful value proposition and deliver a better return on investment.

Cybersecurity measures are more than technologies and processes. An effective cybersecurity programme requires board/executive management support and leadership and a security culture across the organisation, built upon proactive risk management and ability to recover in a predictable manner from an attack.

The risk landscape is continuously changing so strategy and plans must evolve and be adjusted to keep pace. The Chief Information Security Officer (CISO)/ Chief Risk Officer (CRO) should be reporting to and periodically updating their boards about cyber risks and their preparedness. Cyber capabilities should be realistically assessed, as well as the organisation's security posture compared with their risk appetite and industry peers. Cyber threats are inevitable and no

Risk Management, Governance and Board Oversight	Secure by Design	Continuous Threat Monitoring and Incident Response
☐ Threat modeling and risk assessment	☐ Secure network architecture and hardening	☐ Baseline and continuous threat detection
☐ Board oversight and accountability	☐ Change and configuration management processes	☐ Monitoring for unauthorised changes
☐ Supplier risk management	☐ Updated inventory	☐ Continuous vulnerabilities assessments
☐ Awareness and skills development	☐ Role Based Access Control	☐ Periodic tabletop exercise to test incident response plan
☐ Policies, plans, metrics and reporting	☐ Segmentation between IT and OT network, Transient Systems	☐ Retainer's services agreement with an external incident response partner in the event of an emergency (optional)
	☐ Periodic patching (wherever feasible or as per compliance requirements)	

Sanjay Chhillar, Head of OT/ICS Cybersecurity at Siemens UK
Dale Geach, Technology and Innovation Manager at Siemens UK
Chaitanya Bisale, Cyber Security Product Manager and Senior Key Expert at Siemens

matter how robust an organisation's security posture is, it is still susceptible to zero-day and sophisticated attacks. Therefore, in addition to having robust security design and risk management practices, organisations must prepare for emergency situations and always have a tested incident response plan in place and a team of experts trained and ready to handle incidents.

The table above provides a high-level summary of the core pillars and sub-objectives (covers only the key objectives) for establishing a sustainable cybersecurity/cyber resilience programme.

As we transform our traditional grids to modern/smart grids, we will have to deal with hybrid environments containing OT/IOT components that are very advanced and legacy components that are very old and everything in between. Network segmentation may not be easy and patching of all legacy systems will not be realistic, so we must live with inherent security vulnerabilities. To counter cyber threats to grid networks and CNI in general, organisations across all critical sectors and international governments need to partner to secure their CNI without creating an environment of fear and panic. Boards must be held accountable for security of their critical infrastructure and regulatory agencies must empower and incentivise organisations to continuously enhance cyber resilience. Only a secure by design network with continuous threat detection, tested emergency response plan and enterprise risk management with board oversight can defeat adversaries and defend national, social and economic security ●

Electricity grids make attractive targets for bad actors

Picture credit: Siemens

HEALD®

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

THE EVO BOLLARD

THE VIPER

THE RAPTOR

@healduk Heald Ltd

www.heald.uk.com

Secured by Design SBD Police Preferred Specification

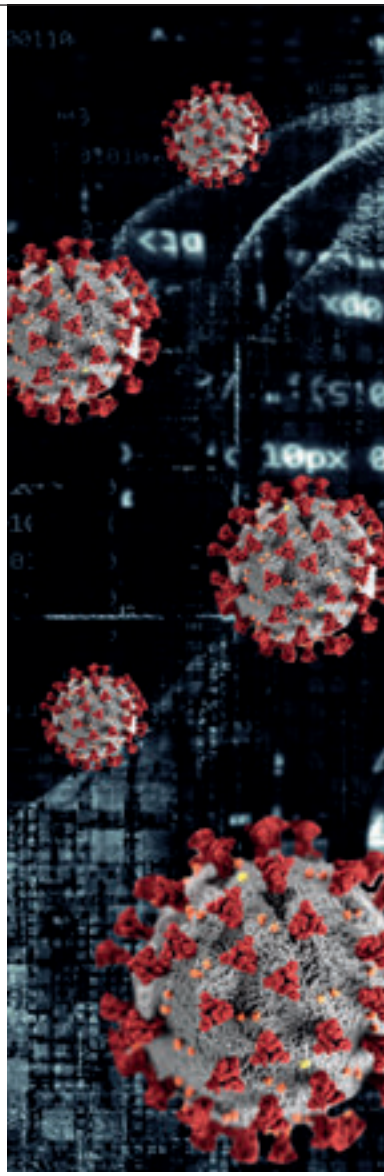
MADE IN BRITAIN

MADE IN YORKSHIRE

PSSA

THE CYBER PANDEMIC

Etay Moor *reports on the importance of defending against the advanced threat actors profiting from COVID-19*



Troubled times have always created opportunities for threat actors, from common criminals to state-sponsored APT groups. With few events in living memory rivalling the upheaval of the COVID-19 pandemic, it is no surprise that cyber criminals have been out in force attempting to capitalise on the disruption.

Our researchers have closely monitored shifting cyber criminal activity around the world during the pandemic and have collated some of the most prevalent tools, techniques and procedures (TTPs) being used to take advantage of the situation – as well best practice for minimising the risk while continuing to operate during the crisis.

As a rule, state-sponsored attackers tend to thrive during global crises, and COVID-19 has been no exception. Nation-state activity has taken a variety of forms with differing targets and motivations, with some specifically going after COVID-related targets, and others simply using the disruption as a convenient smokescreen for their usual activity.

Three major state-sponsored campaigns have particularly stood out during the pandemic so far:

RUSSIA

In February, what is believed to be a Russian state-sponsored hacking group known as Hades was observed targeting Ukraine with a multi-faceted operation. This included both a campaign of disinformation as well as the spread of malware, with the apparent aim being to create panic and confusion around Coronavirus. The threat actors attacked the Center for Public Health of the Ministry of Health of Ukraine with malware-laden phishing emails as well as spreading fake news on social media, contributing to a series of riots and unrest that erupted shortly after.

More recently, in July the National Cyber Security Centre (NCSC) and international counterpart intelligence agencies reported with near certainty that Russian state-sponsored actors had targeted COVID-19 vaccine operations around the world. The group designated APT29, also widely known as Cozy Bear, is believed to have attacked drug companies and research groups in the UK, Canada and the US. Such attacks are unsurprising, as the country to develop the first successful vaccine will not only be able to better save the lives of its citizens, but will also stand to make enormous profits.

NORTH KOREA

Later in February, government officials in South Korea were targeted with phishing emails again claiming to contain information about the country's response plan, but actually laden with the BabyShark malware. This has previously been used by a North Korean group labelled Kimsuky, which has previously launched multiple attacks on South Korean targets including governmental bodies and aerospace and defence companies.

CHINA

The largest number of targeted spear phishing attacks we identified appeared to originate from China. Known APT groups such as Mustang Panda and Vicious Panda were found to target multiple individuals in countries including Vietnam and Mongolia. The phishing emails were again loaded with malicious files, this time in the form of .rar files that covertly installed backdoor trojans into the victim's machine.

Alongside elevated nation state level attackers, common cyber criminals have redoubled their efforts in recent months to exploit organisations struggling to cope with severely disrupted operations. Most have put a new COVID spin on old familiar techniques, while some more ruthless groups have specifically targeted organisations involved in fighting the pandemic.

Attackers have been quick to home in on the opportunities presented by the new regime of remote working. Many organisations were forced to quickly establish a fully remote workforce with very little time to prepare or test their operations. Tools such as VPNs can provide an easy route to access the network or hijacking a user's device, particularly when it comes to workers using their own personal machines to work from home.

In particular, threat actors have sought to exploit the use of online meeting platforms as a replacement for face-to-face meetings. Our Vulnerability Risk Analyser (VRA) found a sharp increase in cyber criminal discussions on vulnerabilities and exploits in the leading online chat and meeting platforms.

For example, before being resolved in an update, Zoom was vulnerable to unauthorised message processing. This would enable an attacker to spoof User Datagram Protocol (UDP) messages from a meeting attendee or Zoom server to invoke functionality in the target client. From here, the attacker can perform malicious actions including hijacking shared screens or spoofing messages from attendees.

This year has seen a sharp increase in all forms of cyber threat

Similarly, the Cisco Webex Meetings desktop app previously possessed a flaw that enabled an attacker to execute commands as a privileged user. This vulnerability required a locally based authenticated user, but a threat actor leveraging remote management tools would be able to gain access.

Phishing has long been one of the most popular cyber attack methods as it requires very little technical expertise and can largely be executed using legitimate software tools and contact lists easily acquired over the Dark Web.

Phishing is always centred on an element of deception, and criminals have frequently been found to weave key dates and events into their fraudulent narrative, from Christmas sales and Valentine's Day to the latest global news. Predictably, we detected a huge spike in phishing activity at the start of 2020, and especially after most countries entered national lockdowns in March.

We closely monitored the registration of new domains that included the words "Corona" and "COVID" and saw an exponential increase in just three months. In 2019 there were just 190 domains containing these key words, but this soon rose to over 1,400 in January and 5,000 in February. In March, numbers skyrocketed to over 38,000. While some of these domains were created for legitimate reasons, many we investigated were certainly used to host phishing attacks.

We also detected a huge spike in COVID-related phishing emails, and a large number continue to circulate. Criminals have incorporated the pandemic into their deceptive narratives in a variety of ways, but a popular theme is to pose as a known authority and offer advice. In one campaign we examined, attackers impersonated the US Department of Homeland Security (DHS) offering advice, with a link through to more information and testing for symptoms. The link redirected victims to a download address instead, infecting them with an information-stealing malware.

Some cyber criminal groups actually announced early into the pandemic that they would not be attacking medical or healthcare organisations during the crisis. The DoppelPaymer group even stated that if such an organisation was hit by mistake, they would provide it with a free decrypter code to undo the damage.

Unfortunately, the old adage that there is no honour among thieves holds true, and we have observed several major ransomware attacks targeting organisations involved in combating the pandemic.

One of the most prominent examples was the Maze ransomware group, previously known for targeting everything from small US-based law firms to the German Government. On 14 March, the group attacked London-based Hammersmith Medicines Research (HMR), a company that undertakes clinical

tests for drugs and vaccines. The company had previously worked on treatments for Alzheimer's and Ebola among others and had recently started work developing a COVID-19 vaccine. Luckily HMR was able to detect the ransomware outbreak in progress and was able to halt the infection and restore its systems in the same day. However, a week later Maze proceeded to leak over 2,300 medical records online.

In another early example, the Champaign Urbana Public Health District (CHUPD) in Illinois was attacked by the NetWalker ransomware group in early March. The attack commenced with a COVID-themed phishing email, including an attachment called "CORONAVIRUS_COVID-19.vbs" which included an embedded executable file for the NetWalker ransomware.

The NetWalker group has been prolific this year and has embraced the opportunity presented by COVID with gusto. Their MO has often centred around attacking educational institutions, and particularly those involved in virus research. Most recently they successfully struck the University of California San Francisco (UCSF) in June, which had been researching potential COVID-19 cures. The university eventually paid a colossal ransom of $1.4-million to restore operations and vital research data.

2020 has seen a sharp increase in all forms of cyber threat, from low-level opportunist criminals to state-sponsored APT groups. As the pandemic stretches on, all organisations involved in medical research related to COVID-19 are likely to remain in the cross hairs of both state-sponsored attackers working an espionage or geopolitical agenda, as well as the more callous organised cyber gangs. However, businesses in all sectors should be aware that they will be facing an elevated threat level for some time, particularly as they continue to utilise remote working practices.

The good news is that although the volume of attacks has increased and threat actors have adjusted their tactics to exploit the pandemic, most threats can be countered with the same core security strategies. Even APT groups still tend to commence their attacks using the same phishing techniques and the exploitation of software vulnerabilities.

Simple human error can swiftly open attack paths for threat actors, so organisations must be especially vigilant to try and compensate for a more isolated remote workforce. A drive towards employee education will help to keep the environment secure, particularly in regard to the proper and secure use of remote access tools and other software. Organisations should ensure that their remote workforce is only using authorised software that has been fully patched and updated, and ideally via a corporate machine rather than a personal one. Mandating strong passwords and the use of 2FA will also help to reduce the risk from phishing attacks targeting user credentials.

In addition to basic security hygiene, organisations should also ensure that they have access to intelligence on the latest threats. Organised groups such as Maze are quick to innovate and discover new software vulnerabilities and attack paths, so organisations must be ready to act quickly when intelligence on new exploits or active campaigns comes in.

Organisations should also be continuously assessing their risk profile as the situation develops, particularly whenever they adopt new software or working practices. Remote working and collaboration tools such as VPNs and virtual meeting rooms will continue to be high on the hit list, so a thorough risk assessment should be conducted before new tools are used. All existing assets should also be assessed for vulnerabilities as a matter of priority.

While we can continue to expect an increase in Corona-themed cyber attacks, getting the security basics right will continue to mitigate the threat of most strikes. Access to good threat intelligence will also be more valuable than ever in the coming months in order to keep track of fast-moving developments from threat actors. In particular, an organisation working in the medical field or with ties to governmental bodies will need to be armed with the latest intelligence to stand a chance against the APT groups and state-sponsored actors that may have them in their sights ●

Etay Moor is Chief Security Officer at IntSights. As CSO, Etay leads the security advisory practice where he works with CISOs and other senior cybersecurity executives to develop risk management-based cybersecurity programmes.

Remote working tools such as VPNs and virtual meeting rooms will be high on the cyber criminal's hit list

MGT europe
Bespoke Surveillance & Counter Surveillance Electronics

Unit 12, Hamilton Business Park
Stirling Way - Borehamwood
Hertfordshire, WD6 2FR
London - UK

www.mgteurope.com info@mgteurope.com

MGT NOTE-33

DIGITAL STEREO AUDIO RECORDER

FEATURES

- *Digital stereo audio recording to removable Micro SD Card.*
- *Dust protected Micro SD Connector.*
- *Compact sturdy aluminum case.*
- *Easy to use and set-up with Windows PC software or Android App.*
- *Android App for recorder settings and audio listening (through USB OTG cable).*
- *Headphone output for audio quality check.*
- *Cable remote control switch.*
- *Uncompressed, best quality audio files with embedded time and date (.WAV file format).*
- *Low power high SNR audio Codec.*
- *Differential (balanced) microphone audio inputs.*
- *Manual and automatic microphone gain control (AGC).*
- *Optional audio files encryption (AES 256).*
- *High quality, reliable LEMO connectors for microphone inputs.*
- *One button recording start-stop.*
- *Recording initiated by button, voice activation, schedule or remote switch with cable.*
- *Line level possible with adapter (ll-36-p).*
- *Audio playback using (CTL-44-P adaptor).*

Unit 12, Hamilton Business Park, Stirling Way, Borehamwood, Hertfordshire, WD6 2FR - London - UK
T: +44 (0) 208 207 0079 - F: +44 (0) 208 953 9162 - M: +44 (0) 7770 390 324

OPTIMISING DATA SECURITY

Glenn Warwick *weighs up whether an apparent obsession with compliance in the UK is having a positive or negative impact on cyber security*

With ever-increasing legislation governing business operations, it's clear that organisations are shifting focus to fall in line with these standards. Ensuring compliance is no longer a 'nice to have', instead it's essential in maintaining reputation, building consumer trust and safeguarding long-term continuity. But it must also be regarded as more than just a tick-box exercise.

Is legislation actually having a negative impact in some cases? As businesses become more and more obsessed with being fully compliant, there is an emerging culture of investing huge volumes of money in security controls that may not be needed. For many organisations stuck in this compliance mindset, this approach can create a short-sighted desire to simply display compliance credentials, rather than work strategically to ensure that the right practices are put in place – and, as a result,

they are likely to be missing real opportunities to increase their overall cyber maturity.

So, the question remains: are businesses genuinely working to uphold higher levels of industry best-practice, or has this laser-focus on legislative compliance led UK organisations to become a nation of 'compliance chasers'?

Organisations have long been expected to run in line with legislative requirements, and this reached a pinnacle with the introduction of GDPR in May 2018. As part of this legislative change, organisations were closely policed on their data security, with significant fines imposed for data breaches – and as a result, many businesses undertook urgent reviews of their security measures, with many deciding to implement security standards such as ISO 27001.

This increased incentive to achieve compliance forced many businesses to attain a level of certification against these standards. But without true organisational buy-in, simply achieving certification is no guarantee of genuine cyber-security. In the first quarter of 2020 alone, at least 68 GDPR fines were issued totalling nearly €50 million. Clearly, it isn't enough just to go through the motions of compliance; businesses must commit to ongoing workforce education and invest in the right resources to truly reap the benefits of upholding these standards.

Following the introduction of GDPR, businesses undertook urgent reviews of their security measures

GETTING IT RIGHT

The first step in improving cyber security is to implement the correct standards. According to Risk Based Security research published in the 2019 MidYear QuickView Data Breach Report, the first six months of 2019 saw more than 3,800 publicly disclosed breaches, with 4.1 billion compromised records. As such, it's clear that there is still a long way to go in terms of improving security standards. But if organisations don't maintain a healthy cyber security culture or implement the right dedicated resources to manage their security on a daily basis, widespread adoption of these operational security practices is unlikely.

To achieve true, long-lasting cyber security, organisations must continually assess and reassess risks, educate employees and make sure that they're investing in the right resources. By ensuring that their security controls are keeping pace with the changing threat landscape, companies can continually deploy the latest and greatest techniques to combat exposure. In turn, this will allow them to avoid breaches, as well as any heavy associated fines.

Assuming that a security certificate alone will provide adequate data protection is the riskiest part of the UK's current 'compliance culture'. If businesses focus on simply achieving certifications, then there is a risk of breeding a culture where employees do not feel accountable or responsible for upholding best practice. This, in turn, is likely to result in reactivity rather than proactivity; where companies only invest time and effort when renewing their certifications. Any subsequent staff awareness campaigns are then likely to be geared towards passing an audit, rather than genuinely raising awareness or educating staff about cyber security. While this approach can satisfy the desire for compliance, simply going through the motions won't keep the company secure. So, while organisations must follow industry standards, it's clear that the key to success comes when they are adopted into daily business operations.

When it comes to data security, one of the weakest links is the risk of human error. If the workforce is not operating in a secure way, the risks of a data breach increase exponentially. According to recent analysis of data from the UK Information Commissioner's Office (ICO), 90 percent of data breaches that occurred in 2019 were caused by user error. The data also showed an increase in breaches caused by user error in 2019 over 2017 and 2018, which is when GDPR came into effect.

By running phishing campaigns, regularly updating antivirus software and implementing mandatory password updates and multi-factor authentication, businesses can start putting best practice in place. However, it's essential to educate staff about the importance of upholding these processes to ensure they fully understand the risks of non-compliance, even if it is time consuming or inconvenient to do so. This will help achieve widespread organisational buy-in for utilising best-practice security measures, and most importantly, will mitigate against attempts to circumvent the processes in place.

IT ESSENTIAL TO IDENTIFY THE CORRECT LEVEL OF SECURITY FOR EACH ORGANISATION

Security needs are ever changing, and never more so than in the current climate. The Coronavirus pandemic has forced many businesses into new ways of working with increased reliance on technology and connectivity, meaning that there has been little choice for those businesses but to accelerate digital transformation.

As part of that transformation driven by the pandemic, organisations have had no choice but to reassess their security software and processes. This is largely driven by the large-scale global shift to working remotely. With millions of employees now working from home, workforces have been forced away from using their secure on-site servers and are instead reliant on users' home networks. Allowing access to business networks through those home networks creates more risk as security is a lot harder to monitor.

It's no surprise, therefore, that almost half of organisations have suffered a cyber security incident as a result of the sudden shift to remote working, according to a survey undertaken by Barracuda Networks. It was discovered that 46 percent of organisations across the UK, US, France and Germany have suffered at least one "cybersecurity scare" since the lockdown began, suggesting that scammers are taking advantage of the unprecedented situation to infiltrate organisations' newly vulnerable security systems.

With the combined consequences of a weakened set of operational security resources, reduced revenue, furloughed staff and redundancies, a lot of companies have been hit hard by the pandemic. As

such, the resulting financial and logistical issues have meant that these businesses are not necessarily able to operate with the same level of security as before the pandemic – and now, more than ever, this makes it important for businesses to make sure they maintain the strongest possible levels of security resilience within their organisations. Another potential from the pandemic could be an increase in insider threats with heightened levels of redundancies and layoffs causing concern that disgruntled employees may try and retaliate via security attacks.

TO ACHIEVE TRUE, LONG-LASTING CYBER SECURITY ORGANISATIONS MUST CONTINUALLY ASSESS RISKS

By keeping abreast of the various different attack methods that businesses may face, vulnerabilities can be better identified, monitored and managed to prevent any adversaries or malicious attackers from exploiting software or process-based weaknesses. This is a continued threat; and as such, it's essential that organisations can promptly and proactively mitigate against any vulnerabilities as soon as they are identified. Typically, this can be achieved through maintaining basic cyber security hygiene practices. This can be accomplished through software patching, via alternative mitigating strategies such as the hardening of an operating system or additional security measures such as firewalls and antivirus software.

It's also essential to identify the correct level of security for each organisation. By working as a community, different sectors can capitalise on a central service from a competent authority; using a baseline cyber assessment framework against which they can measure their own security practices and identify areas of improvement.

Of course, as previously discussed, simply complying with this baseline is not enough. Without considering an organisation's individual needs, it is likely that they will end up with inappropriate, ill thought-through security controls that have been put in place simply to meet arbitrary security requirements. Compliance is one part but adhering rigidly to a prescriptive set of requirements is quite another. Working with a security expert can help businesses pinpoint their own specific needs within the restrictions of legislative compliance; determining the security controls that they need and supporting them to make the right decisions.

Above all, working to implement the right security in the right places will reduce the organisational culture of 'compliance showcasing'. Rather than scrambling to pass an annual audit or achieve the latest ISO accreditation, businesses can move away from blind legislative compliance to truly focus on the 'why' – helping them to navigate the uncharted waters of lockdown, keeping their reputation intact and staying secure for the future ●

Glenn Warwick is Principal Cyber Security Consultant, Bridewell Consulting.

In October 2020, British Airways was fined £20-million for data breaches by the ICO

MCQUEEN TARGETS

LIVE FIREARMS TRAINING TARGETRY

THREAT ASSESSMENT TARGETS

Various hostile/non hostile situations can be created by using the overlay solutions. All targets are designed to fit onto standard NATO backing boards – 458mm x 1143mm (18" x 45").

LIFESIZED 3D FOAM TARGETS

Manufactured in separate parts with repairable foam to withstand 3-4000 rounds. Create your own realistic shoot/no shoot scenario's. Full range of replica accessories available.

STANDARD POLICE AND MILITARY TARGETS

Police

Military

McQUEEN TARGETS, Nether Road, Galashiels, Scotland, UK, TDI 3HE
Tel: +44 (0) 1896 664269 Email: targets.ukgal@sykes.com W: www.mcqueentargets.com

INCIDENT BRIEF

Europe

2 September, Sofia – Bulgaria
Riot police clashed with protesters as protests against Bulgarian Prime Minister Boyko Borissov turned violent.

8 September – West Sussex – UK
Selsey beach was closed after a diver discovered a mortar bomb believed to be from the Second World War. A navy EOD team safely detonated the device.

12 September, Cambridge – UK
Counter-terrorism police arrested a man after a package containing a small improvised explosive device was sent to a residential address in north London. The Metropolitan police said the suspect was detained on suspicion of attempting to cause an explosion, or making or keeping explosives with intent to endanger life or property.

12 September, Paris – France
Riot police arrested 154 people and used teargas to disperse protestors who were setting fire to bins and a car during an authorised protest by the Gilets Jaunes.

16 September, Dover – UK
The port of Dover was closed, causing 10-hour tailbacks after a suspected terror suspect removed his ankle tag and escaped. The man eventually handed himself back into police.

16 October, Paris – France
Police carried out 40 raids on the homes of suspected radicals after a school teacher was beheaded for showing controversial cartoons of the Prophet Muhammad to his pupils.

Americas

31 August, Tallahassee – Florida
Employees at the Florida Department of Economic Opportunity were evacuated from their place of work after the office received a bomb threat. Police are investigating the motivation for the call.

3 September, Miami-Dade – Miami
A 16-year-old student was arrested for launching a cyberattack that paralysed the first three days of virtual classes for the nation's fourth-largest school district.

4 September, Houston – Texas
Ibraheem Ahmed Al Bayati interrupted a virtual University of Houston lecture with a bomb threat before proclaiming his association to ISIS. He was arrested for making threats, conveying false information to destroy by means of fire or explosives and making a threat over interstate commerce charges.

4 September, New Brighton – Minnesota
Federal authorities charged two men with attempting to provide material support to Hamas. The men described themselves as members of the Boogaloo Bois, a group that espouses a violent ideology and an objective to overthrow the Government.

6 September, West Philadelphia – USA
Authorities are investigating after an explosive device was thrown at a home shortly after 3am. No one was hurt.

9 September, Worcester – Massachusetts
Authorities searching an apartment following the arrest of two men on drug and firearm charges uncovered bomb-making materials. The building was evacuated and closed for several hours.

Asia

1 September, Gardez – Afghanistan
Three police and three assailants were killed in a suicide car bomb blast and ensuing gunfight outside a police camp in the capital of the country's Eastern Paktia province.

2 September, New South Wales – Australia
One police officer was seriously injured and two were injured when a man with a knife slashed them. The incident is being treated as a terrorist act.

3 September, Khyber Pakhtunkhwa province – Pakistan
A roadside bomb targeted a military vehicle in North-Western Pakistan, killing three soldiers and wounding four. The Pakistani Taliban claimed responsibility for the attack.

3 September, Kathmandu – Nepal
Thousands of protesters defied a government Coronavirus lockdown to take part in a religious festival clashed with riot police, leaving several people injured.

3 September – India
A Twitter account posting tweets on behalf of the Indian Prime Minister's personal website and mobile app was hijacked by hackers, who abused it in an attempt to scam 2.5-million followers.

5 September, Madhya Pradesh – India
A device was found on the premises of a private school in Mehgaon town with a letter claiming: "7 more bombs are placed in seven big schools of the town". Police later revealed it was a hoax.

5 September, Beirut – Lebanon
The Lebanese army arrested a terrorist cell reportedly carrying out operations inside Lebanon. The cell is reported to be linked to ISIS.

6 September, Kolkata – India
Two men were killed and another seriously injured after bombs exploded in Kamarhati in the northern outskirts of the city.

9 September, Kabul – Afghanistan
10 people were killed as a roadside bomb targeted Vice-President Amrullah Saleh, injuring 15 others. The Taliban denied responsibility for the attack.

Africa

1 September, Dakar – Cameroon
Seven people were killed and 14 wounded in a suicide bomb attack in a village hosting internally displaced people in Cameroon's far north region. Boko Haram is being blamed for the attack.

1 September, West Tripoli – Libya
A suicide bomber on a motorbike let off their device at a checkpoint in the capital. No one was injured and no one claimed responsibility.

5 September, Sahel region – Mali
Two French soldiers from were killed by a homemade bomb in northern Mali. Islamic extremists are suspected.

6 September, Sousse – Tunisia
One National Guard was killed and another injured in a knife attack which took place in the coastal city. Three terrorists were also killed in the incident. Isis claimed responsibility.

7 September, Borno – Nigeria
The Nigerian military killed five militants and rescued seven people who had been taken hostage the previous day in an operation against Boko Haram in the country's north-east region.

7 September, Jubaland State – Somalia
Three Somali military officers were killed and two others injured in a bombing in southern Somalia believed to have been carried out by al-Shabab.

9 September, Mogadishu – Somalia
Three people were killed and seven others injured in a suicide attack inside a restaurant. Al-Shabab is suspected.

10 September, Multiple cities – Morocco
Morocco's counter-terrorism agency conducted a simultaneous operation in multiple cities against suspected terrorists leading to the arrest of five people. According to the authorities, the arrested individuals were plotting terror acts aimed at undermining the stability of the country.

NEWS

Europe

Thatcham certification withdrawal praised by BSIA

The British Security Industry Association has welcomed certification body Thatcham's extension to the withdrawal of its Whole Vehicle Marking certification to 31 December 2022 to give time for a new standard to be introduced to replace it. The extension has been announced after the BSIA lobbied on behalf of its Asset Property Marking members that the original date of withdrawal gave insufficient time for the industry to find a replacement accreditation – a process that usually takes 18-24 months. As a result and after consulting with the British Standards Institute, the BSIA will now be developing its existing guidance (Form 121) on asset property marking into a British Standard, which will also include guidance found in the Forensic Science Regulator's Office Code of Practice. Peter Jack, BSIA's Technical Officer and BSI panel Chair, said: "The BSIA welcomes the extension of the Whole Vehicle Marking certification and would like to thank Thatcham for their flexibility in agreeing to this and for their willingness to become involved in our proposed British Standard panel of experts. We would also like to commend Thatcham and other interested parties and key stakeholders on agreeing to participate in this ambitious and time-critical project".

Greece acts to stop migrants

Greece is beefing up land patrols to stem a rising tide of migrants trickling in from neighbouring Turkey. With tensions between the two NATO allies at their highest in years, Athens fears Ankara may move to weaponise refugees, sparking a fresh migration crisis on top of a lingering energy dispute. Authorities say they are mobilising scores of special border guards to scour sprawling fields and marshland along the Evros region that divides the two countries. Hundreds more will also be deployed on Greece's Aegean islands to stop sea crossings. United Nations statistics show that illegal land entries into Greece from Turkey, have doubled in the last month alone, stoking concerns of a new migration crisis as tensions between the feuding countries have flared over energy rights in the eastern Mediterranean. Migration Minister Notis Mitarachis explains:"We want Turkey to conform to agreements it has signed to stem the flow of illegal immigration," he said, adding: "Any attempt to weaponise the suffering of refugees for geopolitical interests will not be tolerated."

MONEYVAL report on COVID-19 cyber scams

The Council of Europe's MONEYVAL Committee has issued a report aimed at helping the global community to counter new criminal activities designed to exploit the COVID-19 pandemic, including the sale of counterfeit medicines and cybercrime. The Committee, which specialises in measures to tackle money laundering and terrorist financing, focuses in its new report on threats, vulnerabilities and best practices. The report found that the urgent need to acquire specialised medical equipment and supplies created vulnerabilities for fraud, corruption and subsequent money laundering. Authorities in charge of supervising money laundering and terrorist financing threats have had to find new ways to carry out their tasks by using secure electronic means. Nevertheless, international cooperation does not appear to have been negatively impacted by the emergency measures taken to combat COVID-19. Some findings of the report are also relevant for the general public as a source of information against potential criminal schemes, such as phishing emails, text messages containing links to malicious websites, attachments to obtain personal payment information and social engineering.

Turkey criticises France over YPG/PKK textbook propaganda

Turkey has criticised France over a textbook that's being used in schools, which – it claims – includes propaganda from the YPG/PKK terrorist organisation. Foreign Ministry Spokesman Hami Aksoy said France's attempts to build its foreign policy preferences on almost all issues based on its anti-Turkey rhetoric and while attempting to distort historical truths and the law is worrying, claiming: "It is obvious that this terrorist propaganda, which is a result of the official policy of France, was initiated with the courage taken from those who host the so-called representatives of the terrorist organisation at the Presidential Palace," he underlined. Since 2016, Turkey has launched a trio of successful anti-terrorist operations across its border in northern Syria to prevent the formation of a terror corridor and enable peaceful settlement by locals: Euphrates Shield (2016), Olive Branch (2018) and Peace Spring (2019). In its more than 30-year campaign against Turkey, the PKK – listed as a terrorist organisation by Turkey, the US and the EU – has been responsible for the deaths of 40,000 people. The YPG is the PKK's Syrian offshoot.

GCHQ helps UK security start-ups

Bristol-based tech company Geollect is one of 10 that have been chosen to take part in a special mentoring programme being run by the UK's intelligence, security and cyber agency. The aim of the scheme is to develop creative products based on data science, machine learning and artificial intelligence techniques that have the potential to help communities and businesses. A GCHQ spokesperson explained that the programme will play a crucial role in helping to keep UK businesses and consumers safe: "This 12-week programme will give these companies, using cutting-edge tech, unique access to GCHQ technologists to help hone their products – from helping to prevent the spread of fake news to countering people trafficking," they added. The GCHQ Innovation Co-Lab is a joint venture with The Landing, a tech mentorship hub based in MediaCityUK in Greater Manchester and global tech accelerator UP Ventures.

NEWS

Americas

PureTech Systems to protect power generation sites

PureTech Systems has been awarded a multiple site contract for the deployment of its PureActiv Geospatial AI Video Analytics, multi-Sensor Integration and Command and Control software to provide wide-area perimeter protection at multiple power generation plants in the United States. The system integrates PureTech's geospatial AI Deep Learning video analytics and other sensor technologies into a seamless Common Operating Picture. The automated system is protecting miles of perimeter from unauthorised intrusion through fence-lines and turnstiles. The additional sites are scheduled to be completed by the end of the year. For security reasons, the client cannot be disclosed. "These deployments demonstrate that our patented perimeter intrusion detection software solution can be successfully deployed on a large scale in a very short time frame" stated Larry Bowe, President of PureTech Systems. "It speaks to the 15 years of investment we have made, not only in market-leading intrusion detection and classification algorithms, but also in ease of deployment and use."

US vetoes UN resolution of terrorist reintegration

The United States has vetoed a UN resolution calling for the prosecution, rehabilitation and reintegration of all those engaged in terrorism-related activities, saying it didn't call for the repatriation from Syria and Iraq of foreign fighters for the Islamic State and their families that is "the crucial first step." US Ambassador Kelly Craft noted that the resolution: "supposedly designed to reinforce international action on counterterrorism, was worse than no resolution at all." She dismissed it as "a cynical and willfully oblivious farce." Because of the Coronavirus pandemic, the 15-member Security Council voted by email and the result was 14 countries in favour with only the US opposed. In her statement explaining the US veto, Craft said: "It is incomprehensible that other members of this council were satisfied with a resolution that ignores the security implications of leaving foreign terrorist fighters to plot their escape from limited detention facilities and abandoning their family members to suffer in camps without recourse, opportunities or hope."

Border protection agency asylum screening blocked by judge

A federal judge has blocked US Customs and Border Protection employees from conducting the initial screening for people seeking asylum, in a setback to one of President Trump's efforts to rein in asylum. The Trump administration argued that designated CBP employees are trained comparably to asylum officers at US Citizenship and Immigration Services, another agency within the Homeland Security Department, US District Judge Richard J Leon in Washington disagreed. Leon, who was appointed by President George W Bush, said CBP employees get two to five weeks of distance and in-person training, while asylum officers get at least nine weeks of formal training. Leon also cast doubt on whether CBP, a law enforcement agency that includes the Border Patrol, could do screenings in a non-adversarial manner, as regulations require. "This decision puts an end to the sham process of using adversarial Border Patrol agents to conduct highly sensitive interviews with asylum-seekers," said Julie Carpenter, an attorney for the Tahirih Justice Center, which sued on behalf of asylum-seekers.

Women and minorities under represented in cyber security

Women and minorities are underrepresented in the cyber security workforce, according to a panel of female cyber leaders participating in a virtual panel discussion on women in cyber leadership. Katie Arrington, the Defense Department's chief information security officer for the undersecretary of defense for acquisition, noted that the DOD has done a great deal to change that, but still has a long way to go. "We're actually going out and trying to cultivate really young women into our workforce," she said, before adding: "We look for our counterparts in different fields, specifically cyber, and we switch jobs. And in doing that, we have the opportunity to really get involved in the commercial sector with women and educate them as to why they would want to work for the Defense Department." While equality in pay is an area in which Arrington believes DOD does well, she also observed that the DOD is working diligently to try to make a level playing field in terms of pay for men and women: "Anything we do now in cyber is so incredibly important. Don't ever doubt yourself."

Increased biometric data collection for US immigration

The Department of Homeland Security is planning to expand its use of biometric data for immigration and increase its use of DNA to verify family relationships. The proposal would give DHS the authority to require biometrics for every application, petition or related immigration request. Currently, US Citizenship and Immigration Services, the agency responsible for managing immigration benefits, requires biometrics only for applications that need background checks. Last year, Immigration and Customs Enforcement began using DNA testing at several locations along the southern border to identify individuals as families, but the new rule would give the department broad authority to use new technologies that could include voiceprints, iris scans, palm prints and facial photos. The proposed rule will allow the agency to collect DNA to verify a genetic relationship, where establishing a genetic or familial relationship is an eligibility requirement for the immigration benefit. Raw DNA will not be stored, but the results of the test will be saved in an immigrant's 'A-File', the official file for all immigration and naturalisation records, consistent with current procedures, while the information may be shared with law enforcement, the new rule does not change the procedure for other agencies to access the files.

NEWS

Asia

ASD admits that listening to Australians is "essential"

The head of Australia's top foreign cyber-intelligence agency says spying on some Australians is essential because authorities are in a "near-impossible game" to defeat terrorism and espionage. Rachel Noble – the first woman to lead the Australian Signals Directorate (ASD) – has warned that the country's strategic circumstances are the most threatening in decades. ASD is tasked with intercepting foreign communications and disrupting the activities of overseas criminals and hackers. The prospect of it helping police to target Australians has stirred intense debate in Canberra, especially after police raided the home of News Corp journalist Annika Smethurst after she reported the Federal Government was contemplating expanding surveillance powers for spy agencies. In a speech to the Australian National University's National Security College, Ms Noble declared: "ASD cannot, under law, conduct mass surveillance on Australians." Before going on to highlight an intelligence bill passed in 2001 that gave the organisation the power to collect intelligence on Australians overseas who posed a threat, although only with ministerial authorisation.

Afghan authorities release Taliban prisoners

Afghan authorities have resumed a controversial release of Taliban inmates, marking an important step towards breaking an impasse that has delayed the start of peace talks for months. Negotiations were supposed to begin in March but were repeatedly pushed back as the Taliban and Afghan government squabbled over the precise details of the exchange, which included hundreds of battle-hardened insurgents. "Our prisoners have been released and we see this as a positive step that paves the ground for the start of intra-Afghan talks," Taliban spokesman Suhail Shaheen said. Meanwhile, another Taliban official from the group's prison commission said that 200 prisoners had been released by Kabul and in return for their prisoners, the militants had released four Afghan commandos who had been held captive. Under the terms of a US-Taliban deal in February, Kabul was supposed to free 5,000 militants and the Taliban were meant to free 1,000 Afghan troops. Both sides met most of their obligations, but Kabul had balked at the release of a final 400 inmates who President Ashraf Ghani himself said were "a danger to the world".

Australian casino group accused of money laundering

Australian casino group Crown has revealed it is being investigated for possible breaches of anti-money laundering and counter-terrorism financing laws. It told the Stock Exchange it has been contacted by the country's financial crime regulator and it's understood that if the breaches are proven it could face millions of dollars in fines and threats to its casino licences. This comes as bad news for the company, which is already facing separate inquiries into its licences and questions over how it brought in high-roller gamblers, largely from China. In a statement, Crown said the Australian Transaction Reports and Analysis Centre had raised concerns after reviewing its Melbourne casino's "management of customers identified as high risk and politically exposed persons". These included "concerns in relation to ongoing customer due diligence" and complying with "an anti-money laundering/counter-terrorism financing programme."

Indian Railways increases security for festive season

Indian Railways has reviewed its security, crowd management and enforcement of COVID-19 protocol, as footfalls have started increasing ahead of the festive season. "Since the footfall in stations and trains is slated to increase during the festival season the need was felt to launch a focused initiative across all zones for the safety and security of women passengers," said the Ministry of Railways. In an effort to provide better safety and security for passengers, a new 'Meri Saheli' initiative has been launched to instil a sense of security among women. Indian Railways also explained that it was felt that offenders involved in human trafficking may try to indulge in the trafficking of women and children taking advantage of the festive season rush as they are most vulnerable to this crime. "An action plan to curb the menace of human trafficking during the upcoming festive season has been discussed. It was decided that a sustained and concerted drive will be launched to identify and apprehend the traffickers," they stated. Meanwhile, field formations have been directed to continue a drive against touts cornering reserved railway tickets and selling them to needy passengers at a premium.

Australians lose nearly $90-million to scams

According to data analysed by the Atlas VPN research team, Australians have reported 99,321 scam events since the beginning of the year, resulting in $89.6-million in losses. Of these, some $3.3-million were lost to Coronavirus-related fraud. There has been a slight drop in the number of reported scams from 1 January to 31 July 2020 compared with last year, however, the financial damage caused has risen by more than $10-million or over 13 percent. The report highlights that losses have been steadily growing since 2017 and if we were to compare the amount of money lost to scams within the first seven months of 2017 to the equivalent period in 2020, the amount has grown by 93 percent. Rachel Welch, COO of Atlas VPN, notes: "Even though the number of scams is not growing, what is concerning is the fact that scams are becoming more sophisticated and are able to lure out more money per every successful attempt." April was the most successful month for scammers in 2020. In total, there were 17,701 fraud cases recorded that caused damages of close to $16.4-million. July, however, saw the most scam complaints. There were 18,579 scam events in July alone, which together robbed victims of nearly $12.3-million. Most fraud complaints have come from people aged 65 and over. This group has reported 14,286 (14.4 percent) scam cases and lost close to $30-million (23.4 percent) to fraud.

ALL PRODUCTS HOSTILE VEHICLE MITIGATION APPROVED ANTI-TERRORIST BARRIERS

Safetyflex Barriers at Redfern Station in Sydney, Australia.

Safetyflex Barriers

A world-leading British manufacturer of anti-terrorism security measures acclaimed for its innovative products could be setting a new design trend with its latest project in Australia.

Bollards made by Coventry-based Safetyflex Barriers have been given a striking makeover for an installation to help secure one of the busiest railway stations in Sydney from potential vehicle attacks.

Indigenous artists have put their stamp on the bollards outside Redfern Station, a major transport hub within the inner-city suburb with more than 70,000 journeys a day, which can stop attacks from vehicles travelling up to 80mph.

The installation at Redfern Station was carried out as part of a new entrance being created by the News South Wales Government to improve the movement and safety of passengers.

The heritage-listed station has strong ties with the local Aboriginal community which has been reflected in the design of the new entrance and the bollards.

The artists have transformed the look of the slim line steel bollards with Aboriginal symbols to mirror designs on the windows within the entrance.

It is the latest project to have been completed with Australian distributors EZI Security Systems as Safetyflex Barriers continues to expand its global reach as a leading force in providing preventative measures to counteract terrorist threats.

Marcus Gerrard, director at Safetyflex Barriers, said: "We have a growing presence in Australia and are helping to secure numerous locations there to protect people and key locations from potential vehicle attacks.

"This was a particularly enjoyable project as it formed part of major improvement works to a high-profile station in Sydney and involved local Aboriginal artists transforming our bollards.

"Aside from providing superior protection against terror threats involving vehicles, our bollards have a stylish aesthetic which means they do not detract from the appearance of sites they help secure.

"This is the first time that our bollards have been given a makeover but the resulting design makes a fantastic statement in reflecting the culture of the local community and the new look of the station entrance.

"The feedback has been great and we are expecting this to signal an exciting new trend with more locations that we are working with both in the UK and overseas looking to put their own stamp on our bollards to reflect their identity and surroundings."

The company's innovative range of barriers and bollards help to secure areas at risk such as shopping centres, sports stadiums, government and military buildings, utilities and key infrastructure centres.

It has recently been recognised with the ADS Security Innovation Award by the Home Office, and Product of the Year Award at the Australian Security Industry Awards.

02476 662116
www.safetyflexbarriers.com

safetyflex
ANTI-TERRORIST BOLLARDS BARRIERS & CRASH FENCES

NEWS

Africa

778 Boko Haram suspects handed in for profiling

The 4 Special Forces Command, Doma, in Nasarawa State, has handed over the 778 women and children that were working for Boko Haram and subsequently captured in 17 states of the north for profiling and re-integration into society. Handling over the terrorists, Maj-Gen. Moundhey Ali explained that the Darul-Salam Islamic sect was taken over by Boko Haram for attacks on the seat of government in Abuja, before revealing that the group was responsible for the mayhem along Okene/Lokoja, Lokoja/Abuja and Toto/Umasha roads, making economic activities unsafe for communities around the areas. "The 778 women and children are members of Boko Haram that came from 17 states of the nation. These women and children are the real terrorists, as they are the people that indoctrinate the newly kidnapped as well as doing banking transactions for their husbands," he explained. According to the commander, arrest of the terrorists was made possible through the joint operations of the Doma army command with Operation Whirl Stroke, Nigerian Navy Ship Lugard, Nigerian Air Force, Guards Brigade, police and the Department of State Services.

CASLER claims foreign support is helping Boko Haram

Civil society organisation, Centre for African Liberation and Socio-Economic Rights (CASLER), is claiming that some human rights groups and foreign non-governmental organisations are behind the "elongation of the Boko Haram crisis" in Nigeria. According to its report, the groups have been assisting in the recruitment of members for Boko Haram through covert means. "Our investigations revealed that they are hired by some vested interest to publish damaging reports on the operations of the Nigerian army emphasising human rights violations and extrajudicial killings of innocent people and other despicable acts," a spokesperson claimed. The report went on to suggest that some western countries are being dissuaded from selling arms to Nigeria to help carry out the war on terrorism effectively. "Some International NGOs in north-east Nigeria have been providing Boko Haram with logistic supplies under the guise of humanitarian assistance. They go as far as carrying out espionage activities by obtaining details of operational strategies of the Nigerian military and subsequently passing same to the leadership of Boko Haram."

Six million Nigerians flee Boko Haram attacks in 10 years

In the last 10 years, an estimated six million Nigerians have fled their homes for fear of extermination, abduction, and other forms of treatments by Boko Haram in Nigeria, a recent report has revealed. The report, which is a follow up of an earlier project, stated that in the north-east alone, the decade-long attacks have displaced over 1.8-million people. According to the study, the Internally Displacement Monitoring Centre estimates the total number of displaced peoples in the country between January and December 2018 to be above two million with Borno State alone accounting for 1.4 million of that figure. It claims that about 2,000 in the first half of 2019 were displaced by natural disasters, namely flooding, while violent conflicts were responsible for more than 140,000 cases during the same period. The study also identified the proliferation of small arms and light weapons as critical factors associated with high propensity of deepening violent conflicts with potential for displacement of the population.

Kenya vow to take on terrorism

Kenyan President Uhuru Kenyatta has vowed that his government will enhance its counter-terrorism efforts in Eastern Africa by working with regional governments and partners. Speaking at a virtual meeting of the Aqaba Process on COVID-19 convened by King Abdullah II of Jordan, Kenyatta told the global community that Kenya will leverage on its membership in the UN Security Council to contribute more to global peace and security. "Through Kenya's non-permanent member seat at the United Nations Security Council, Kenya further aims to contribute to global peace and security, with the ultimate goal being the attainment of sustainable development for the year 2021-2022," he said. Kenyatta said Kenya aims to provide leadership in the Horn of Africa by exploring and implementing diplomatic measures in counter-terrorism financing and to work with partners in the broader spectrum of efforts within counter-terrorism, as well as to stem other forms of transnational organised crime. Kenyatta said frontline states in the fight against terrorism and violent extremism should be assisted by strengthening their capacities to deal with both emerging and pre-existing security challenges in order to address security challenges made worse by COVID-19.

Be "bold and courageous" implores Nigerian army chief

Nigeria's Chief of Army Staff, Lt.-Gen. Tukur Buratai, has tasked the Army Armoured Corps to be "bold and courageous" in tackling insurgency when deployed to the theatre of operation. Buratai gave the speech during a live firing demonstration of the newly purchased VT4 MBT and ST1 light tank. He said the training of the personnel of the corps had prepared them to take decisive action in the ongoing fight against terrorists in the north-east of the country. "I am just coming from Maiduguri and Damaturu and I have seen the tremendous effort made by the troops of Operation Lafiya Dole and we expect you very soon to mobilise with these vehicles to go and round up," he said. Buratai urged personnel to deploy the practical experience they had gained from the training in manning and maintenance of the new platforms before emphasising the need for continuous training of officers and soldiers of the corps to be able to carry out second, third and fourth line maintenance.

DIARY DATES

2020/21 Conference and Exhibition planner

9-11 November MAST 2020/ Japan Defense 2020
Sheraton Miyako,Tokyo, Japan
Organiser: MAST Communications Ltd.
Tel: +44 (0) 7411 732978
Email: paul.hunt@mastconfex.org
mastconfex.com

2-3 February Platinum Security Exhibition 2021
Grimaldi Forum, Monaco
Organiser: Coges Events
Tel: +33 1 44 14 51 11
Email: info@cogesevents.com
www.psemonaco.mc

2-4 February Digital Document Security 2021
Vienna, Austria
Organiser: Reconnaissance International
Tel: +44 (0)1932 785 680
Email: events@reconnaissance-intl.com
www. digitaldocumentsecurity.com

10-11 March Enforce TAC 2021
Nurenberg, Germany
Organiser: Nürnberg Presse GmbH
Tel: +49 9 11 86 06-88 06
www.enforcetac.com

7-10 April Indo Defence 2021
Jakarta, Indonesia
Organiser: PT Napindo Media Ashatama
Tel: +6221 8650963
Email: info@indodefence.com
indodefence.com

18-20 May IFSEC International 2021
ExCel, London
Organiser: IFSEC International
Tel: +44 (0)20 7921 8166
Email: ifseccustomerservice@ubm.com
www.ifsec.events/international

19-21 May DSEI Japan 2021
Makuhari Messe, Chiba City
Organiser: Clarion Defence and Security Ltd
Email: japan@dsei-japan.com
www. dsei-japan.com

7-10 June Shield Africa 2021
Abidjan, Côte d'Ivoire
Organiser: Coges Events
Email: hotline@cogesevents.com
www.shieldafrica.com

14-19 June Interschutz 2021
Hannover, Germany
Organiser: Interschutz
www.interschutz.de

15-17 June IFSEC South East Asia
Kuala Lumpa, Malaysia
Organiser: IFSEC
Tel: +44 (0)20 7921 8063
Email: ifseccustomerservice@ubm.com
www.ifsec.events/kl

INTERNATIONAL SECURITY WEEK

30 NOVEMBER - 03 DECEMBER 2020

WATCH LIVE 30 NOV - 03 DE
OR ON DEMAN

JOIN US FOR FOUR DAYS OF EXCLUSIVE CONTENT COVERING SECURITY, COUNTER TERRORISM, CYBER & DISASTER RESPONSE

FREE TO ATTEND

CPD ACCREDITED CONTENT

KEY SPEAKERS NOT TO MISS:

DAY 1: INTERNATIONAL MATTERS

INTERNATIONAL SECURITY EXPO Sponsored by hs security

Lucy D'Orsi
Assistant Commissioner Specialist Operations, CTP UK

Aimen Dean
Former member of Al-Qaeda and Mi6 Spy

Figen Murray
Mother of Martyn Hett, Martyn's Law Campaign

DAY 2: CYBER THREATS

INTERNATIONAL CYBER EXPO Sponsored by tripwire

Chris Greany
Managing Director, Templar Executives

Tracy Buckingham
Deputy Director Security & Cyber Security Exports, DIT, UKDSE

Jenny Radcliffe
The People Hacker

DAY 3: PROTECTING CNI AND ADAPTING LAW AND ORDER

INTERNATIONAL SECURITY EXPO Sponsored by apstec systems

Angela Essel
Senior Home Office Official

Ian Dyson
Commissioner - City of London Police

Shaun Hipgrave
Director of Protect, Prepare, CBRNE and S&T, OSCT - Home Office

DAY 4: DISASTER RESPONSE AND COMMUNICATION

INTERNATIONAL DISASTER RESPONSE EXPO

Anne-Marie Trevelyan
MP for Berwick-upon-Tweed, former Minister for International Development

John Coyne
Head of Border Security - Australian Strategic Policy Institute

Alison Stuart
Counter Terrorism Security Advisor

REGISTER FREE TODAY:

YOUR MOBILITY SPECIALIST FOR ARMOURED VEHICLES

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

TSS International official distributor for:

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

TSS

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

SHOWCASE

SpearUAV unveils Ninox 40 handheld drone system

SpearUAV has introduced its handheld version of the Ninox 40 encapsulated drone system, which offers instant launch and provides immediate intelligence capabilities to any tactical unit, even if it is not equipped with a 40mm grenade launcher or any other special equipment. The system comprises an encapsulated drone and control unit; when launched at high speed, the drone immediately unfolds and stabilises in the air with no operator intervention required. Specifically designed for single-user operation and weighing under 250g – within regulatory limitations – it is lightweight enough to be carried in a soldier's vest during combat. The Ninox 40 Handheld has a flight capacity of up to 40 minutes, extensive ISTAR capabilities, day and night camera for enhanced situational awareness, automatic tracking and can be launched on the move and from under cover.

Getac's V110 rugged laptop

Getac has announced the launch of its next generation V110 fully rugged laptop. The powerful new device is aimed at professionals who need a rugged, yet versatile device they can rely on in challenging indoor and outdoor work environments. Key features include a high-performance quad-core processor and PCIe SSD storage as standard. The V110 also boasts outstanding connectivity for optimal productivity in any situation. The latest 802.11ax wi-fi 6 increases connection performance and stability in dense or congested environments, while WLAN wi-fi 6 offers up to three times faster wireless data speeds than previous generations. A combination of WLAN, WWAN, Bluetooth, 4G LTE and GPS ensures users can get online from anywhere and advanced inbuilt technology lowers power consumption when connected, for more extensive field use between charges. The V110 is built rugged from the ground up, featuring IP65 and MIL-STD-810H certifications, as well as drop resistance of up to 4 feet while in use.

World's most technically advanced surface-submersible

The world's most technically advanced surface-submersible, made in Britain and set to be sold across the globe, is to hit the water in 2021. Capable of operating both on and under the water, VICTA combines the characteristics of a fast surface craft with those of a specialist submersible to deliver divers on or beneath the surface – discreetly. Using advanced design and superior, next-generation technology the craft is designed around the operator and features a number of technical firsts for the maritime sector, putting it well ahead of the competition. Its performance in both domains and the rapid transition between the two is enabled by a unique fly-by-wire control system, which delivers dynamic stability in all conditions. This ensures the craft's safety at all times, while reducing friction in the cockpit and thus leaving the crew to focus on the mission. The craft is made of carbon fibre with a Diab core. A lightweight construction many times stronger than fibreglass, VICTA will be faster and more manoeuvrable than comparable craft. Scott Verney, CEO Subsea Craft, says: "We are on track for trials and testing this coming winter, with the aim of having the craft operational late 2021."

INVISIO launches T7 over-the-ear tactical headset

INVISIO has launched a new over-the-ear headset – the INVISIO T7. The tactical communication headset sets new standards for submersibility, ruggedness, flexibility, and comfort while combining industry-leading hearing protection with situational awareness. Designed for military and public safety professionals on critical missions, the T7 headset is lightweight, submersible, robust and offers three interchangeable wearing styles. When used with INVISIO control units, the T7 provides market-leading hearing protection, state-of-the-art situational awareness and clear communication in all environments. Submersible and rugged, it is operational at altitudes of 12,000m+ and down to 10m of submersion. Lightweight at less than 350g, it comes with a choice of three different ear cushions, including a new, patent-pending ergonomically shaped 3D cushion. It additionally boasts Industry-leading hearing protection with clear communication in extreme noise levels and unparalleled situational awareness, and is available in three different and interchangeable wearing styles with no tools needed when changing.

Cordura goes into service with UK commandos

Cordura fabric is to be used in the new uniforms that are now being issued as part of the Future Commando Force initiative for Royal Marines Commandos . The new uniform comprises individual Combat and Field ensembles all made from Crye Precision's comfort weave MultiCam VTX Ripstop stretch NYCO fabric using INVISTA's T420HT high-tenacity nylon 6,6 fibre blended with cotton. NYCO is said to offer long-lasting comfort and performance for the wearer. Along with delivering the enhanced durability required for Commandos in action, the fabric is a foundation for a new uniform that is lighter weight, has comfort stretch, higher tear-strength, is faster-drying and is more breathable than typical 50/50 nylon/cotton uniform kit. Meaning it can be trusted and relied on in the most extreme and hostile environments on earth – from frozen wastes to jungle and deserts.

3DX-RAY

INSIGHT WHERE IT MATTERS

SECURITY IN A BACKPACK

Rapid deployment.
High quality images.
Fast decisions.

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

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

Optional tablet PC shown.

The complete system fits in a backpack.

www.3dx-ray.com

An **IMAGE SCAN** company

Milipol Qatar 2021

International Event for Homeland Security & Civil Defence

13th Edition

NEW DATES

15 - 17 March 2021

Register online:
www.milipolqatar.com

Doha Exhibition & Convention Centre (DECC)

#MilipolQatar - www.milipolqatar.com

Organized by
Ministry of Interior

The World's Leading Network of Homeland Security Events

www.milipolqatar.com

www.milipol.com

www.milipolasiapacific.com