WORLD SECURITY REPORT

Official Magazine of

International Association of
CIP Professionals
www.cip-association.org

SPRING 2021
www.worldsecurity-index.com

FEATURE:
Towards 2021 – Upcoming Organisation Risk & Resiliency Trends
PAGE 12

FEATURE:
Maritime Domain Awareness - An Essential Component of a Comprehensive Border Security Strategy
PAGE 17

FEATURE:
Security and Criminology-Risk Investigation and AI
PAGE 19

PHENOMENA OR JUST A 'BAD KARMA'

critical infrastructure
PROTECTION AND RESILIENCE AMERICAS

October 19th-21st, 2021
New Orleans, LA, USA
A Homeland Security Event

Are you sure your national infrastructure is secure?

The ever changing nature of threats, whether natural through climate change, or man-made through terrorism activities, either physical or cyber attacks, means the need to continually review and update policies, practices and technologies to meet these growing demands.

Invitation to Exhibit

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety.

Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure.

The 3rd Critical Infrastructure Protection and Resilience North America brings together leading stakeholders from industry, operators, agencies and governments to debate and collaborate on securing America's critical infrastructure.

As we come out or one of the most challenging times in recent history, off the back of a pandemic, it has stressed how important collaboration in protrection of critical infrastructure is for a country's national security.

Join us in New Orleans, LA, USA for the premier event for operators and government establishments tasked with the regions Critical Infrastructure Protection and Resilience.

For further details visit **www.ciprna-expo.com**

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector

To discuss exhibiting and sponsorship opportunities contact:

Paul McPherson
(Americas)
E: paulm@torchmarketing.us
T: +1-240-463-1700

Paul Gloc
(UK and Rest of World)
E: paulg@torchmarketing.co.uk
T: +44 (0) 7786 270 820

Sam Most
(Mainland Europe, Turkey, Israel)
E: samm@torchmarketing.co.uk
T: +44 (0) 208 123 7909

The premier discussion for securing America's critical infrastructure

Supporting Organisations:

INFRAGARD MEMBERS ALLIANCE LOUISIANA · International Association of CIP Professionals · NS&RC · I-DIEM · IACI International Association of Certified ISAOs · ISIO · SPF

Media Partners:

WORLD SECURITY REPORT · World Security-index.com

CONTENTS

WORLD SECURITY REPORT

» p.6

» p.12

» p.17

» p.30

www.worldsecurity-index.com

Editorial:
Tony Kingham
E: tony.kingham@knmmedia.com

Assistant Editor:
Neil Walker
E: neilw@torchmarketing.co.uk

Features Editor:
Karen Kingham
E: karen.kingham@knmmedia.com

Design, Marketing & Production:
Neil Walker
E: neilw@torchmarketing.co.uk

Subscriptions:
Tony Kingham
E: tony.kingham@knmmedia.com

World Security Report is a bi-monthly electronic, fully accessible e-news service distributed to over 100,000 organisations globally. It tracks the full range of problems and threats faced by today's governments, armed and security forces and civilian services and looks at how they are dealing with them. It is a prime source of online information and analysis on security, counter-terrorism, international affairs, warfare and defence.

LOW-PROFILE VESSELS, SEMI-SUBMERSIBLES AND UNMANNED UNDERWATER VESSELS

A maritime patrol aircraft detected a suspicious vessel and directed the US Coastguard cutter Munro towards it. Munro launched a helicopter aircrew and boarding teams, and together they interdicted a low-profile vessel. The boarding teams discovered 3,439 pounds of cocaine aboard the purpose-built drug smuggling vessel.

It can be seen by the design that it is deliberately incorporating stealth techniques in its design, despite probably being manufactured in a relatively primitive workshop.

US Coast Guard seize low profile narco-vessel

Conventional coastal radar relies on sending out electromagnetic waves in short pulses, which are reflected by objects back to the radar. But to be detected, the objects have to be of sufficient size and have sufficient surface to reflect the electromagnetic waves. These vessels are so low profile that they can only really be detected by airborne downward looking radar.

These vessels are nothing new. As far back as 2010 Ecuador Anti-Narcotics Police Forces and Ecuador Military authorities seized a fully-operational submarine built for the primary purpose of transporting multi-ton quantities of cocaine.

The twin-screw, diesel electric-powered submarine was about 30 meters long and about nine feet high

READ THE FULL VERSION

The full version of World Security Report is available as a digital download at www.torchmarketing.co.uk/WSR from the deck plates to the ceiling. The sophisticated vessel also has a conning tower, periscope and air conditioning system.

In 2019 Spanish authorities captured a 22-metre submarine after its three crewmen transported US$121-million worth of cocaine 7,700 kilometres across the Atlantic Ocean from Colombia, then scuttled it and ran.

This latest vessel was detected and interdicted, but how many get through undetected. Its significant payload of nearly 1.7 tons, would make a very sizeable bomb if this sort of vessel ever got into than hands of terrorists. And links between terrorist groups and organised crime are well known.

Video: Incredible footage of the U.S. Coast Guard Cutter Munro crew boarding a suspected drug smuggling vessel

After all, it is nothing new. The Tamil Tigers or Sea Tigers as their naval component were known, successfully used low profile vessels, semi-submersibles and submarines in their terrorist campaign of the 80's to early 2000's.

These low profile, submersible and semi-submersible vessels represent a real security challenge and a serious threat to ports, shipping and waterside critical infrastructure.

Later in this issue Commander J.J. Jones (Retired) and Captain Charlene Downey (Retired) formerly of the U.S. Coast Guard, discuss how Maritime Domain Awareness (MDA) must be viewed as an essential component of a national strategy to protect vital economic and environmental interests as well as the lives and property of citizens.

Who could argue?

Tony Kingham

Editor

Phenomena or Just a ‘Bad Karma’

In our cutting-edge technological era - Why we are still witnessing incidents in which a civilian aircrafts are gunned down by “mistake”? Should we be worried?

We are living in a super advanced era in which monitoring, control and identification systems allow us accuracy rates never seen before; controlling satellites in space, high resolution navigation systems (GPS) and sophisticated communication systems are at the grasp of almost every country and airline.

So, why do we encounter events, from time to time, in which civilian passenger’s aircrafts are being shot-down by ‘Surface to Air’ (SA) missiles? Is it always a matter of purely “bad luck” or maybe our answers lye in other fields? Should we, as costumers of the ever-growing** travel industry, be more concerned about that?

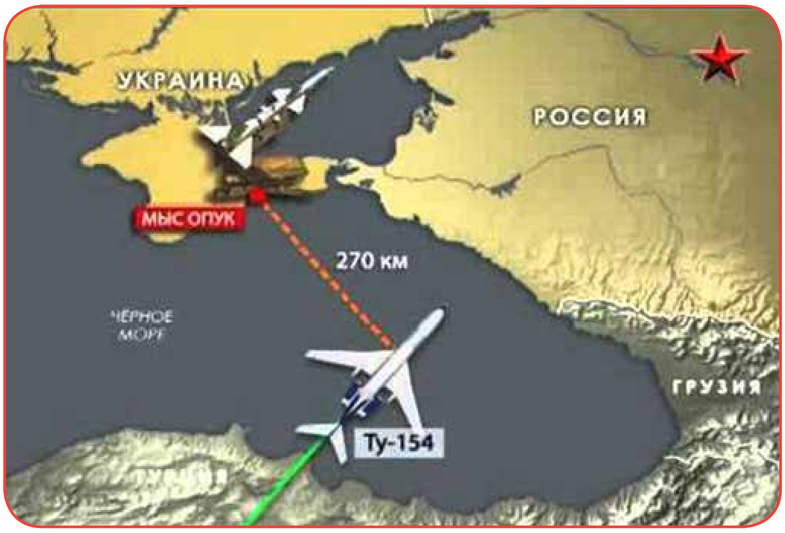
This review focuses on airlines' aircrafts that where identified mistakenly or negligently as "enemy" military aircraft or as an offensive cruise missile, and due to that, where targeted by "Defence Forces" of some nature. Within the article I will review several past incidents, include my personal perspective, and offer some action alternatives for decision makers to consider.

There was no preliminary sign that morning of October 4th, 2001. It was just another routine day at Ben-Gurion Int'l Airport (TLV) with passengers en-route their destinations while airport staff are doing their best to check them in properly. Around 12:45pm airport's directors started to receive phone calls informing us about info that flight SBI18212 Siberian Airlines (today identified as S7) destined to Novosibirsk, that departed the airport earlier around 10:00am – had vanished from radar screens at some point along its route. I can still remember the chill running down my spine from the sound of those words that no aviation industry professional is ready to hear someday.

Considering the fact that it occurred less than a month after 9/11 mega terror attack, and while civil aviation is still in a state of shock and slowly recovering from the consequences of that event – the pace and reaction here in the airport were both obviously influenced. Being a manager within the ranks of the airport's security division team (and especially in Israel) – my colleagues and I immediately assumed it was a terror related event, but silently hoping it was "just" a malfunction of the aircraft…

Within few hectic hours, in which we've run our most thorough pre-planned security emergency protocols, assessing the situation, diving into every aspect of the flight preparations and procedures. We needed to conduct a deep debrief with our horrified employees (especially security team and ground handling agents were directly involved in the processes; some still remember the faces of the passengers on-deck). Some employees already finished their shift and went home to sleep, so we were forced to call them back to the airport for personal and collective debriefs and reconstructing line of events. Joining hands with all airport's relevant stakeholders, with law enforcement community and governmental authorities, and with everyone that might have some information regarding the plane, the crew, the passengers, its cargo and mail, and many more angles in no-time – it became a grueling task. Piece by piece we've managed to assemble information, data and evidences to create almost a complete puzzle that enabled us to assess possible weaknesses that may have contributed to a disastrous result.

Obviously, we've shut down all aviation activity at the airport (with the immense operational "headache' it involves) and consider specific decision making for every inbound flights or recent departures (that were still airborne). We had to deal with worried passenger's families, mass media attention and requests for 'responsible' information from different entities, etc. Therefore, part of the team was needed to be reinforced by additional manpower summand from home.



SBI 1812 Hit Illustration

In some point, an Armenian Airlines pilot reported that he saw an aircraft flying high above him, exploding and dropping into the Black-Sea beneath, while he was en-route at the area. That kind eye-witness testimony description can indicate a technical malfunction, a terror event and more scenarios (weather was reported as fair).

After eliminating all prospects of ill mechanical treatment on ground stop-over, or an airport staff failure, failing to conclude what was the reason for the catastrophe – we got a word through some diplomatic channels that an American satellite images analysts managed to spot two flame signatures (one looks to be on ground and the other might be in mid-air). That could match or indicate that a 'surface to air' missile had been shot and hit the aircraft mid-flight.

To be honest - a momentary sigh of relief went briefly between us

Russian-made S-200 missile launcher

argument of "we were in high alert anticipating armed retaliation after an Iranian attack on US bases in Iraq" – is not acceptable at all. Local authorities should conduct preventive steps to ensure safe passage for civil aviation or halt traffic.

and then we became (until today) simultaneously sad and enraged about the pointless unnecessary loss of human lives. Those 5 hours of uncertainty are forever engraved into my professional consciousness.

Later it was argued and reported that a Ukrainian Army units were in a military drill that day, and one of their air-defence S-200 missile batteries "accidently" identifies that aircraft as a 'part of the drill targets'. Sadly, it was too late and didn't matter for the misfortune casualties on-board.

Counting rundown of some past major events, locations and "reasons" include:

- A year ago, January 8th, 2020, we've horrifically witnessed Ukraine Int'l Airlines Flight PS752, B737-800 shot down (with 176 casualties) by 9K331 Tor-M1 (SA-15) missile, merely 6 minutes after takeoff from Iran's Teheran Int'l Airport, due to a so called "Human Error". Quite quickly this became evident to AVSEC professionals, and 3 days later it was admitted publically by local authorities as an event created by the hands of the hosting country armed forces (IRGC)!! Their

It took several more months before an Iranian Civil Aviation Authority official came forward admitting that it was confirmed by reading recovered data from the aircraft "black boxes" (which are actually orange in true color – to ease the search after a crash) that the aircraft continued to fly additional 19 seconds at least after being hit by the first missile (people on-board where alive at this point!!) until it was hit and eliminated by the second lethal missile, leaving no chance for survivors.

- July 17th, 2014: Malaysia Airlines Flight MH-17, B777-200ER (299 casualties) – Intercepted by a 9K37 Buk (SA-11/17) missile shot by "mistake" by a "rebel Ukrainian vigilantes" (supporting Russia) over Crimea peninsula dispute.

- October 4th, 2001: Siberia Airlines Flight S7-1812, TU-154 (78 casualties) was hit by an S-200 Dubna (SA-5) missile, fired from the Crimea peninsula during a Ukrainian military exercise, by "mistake". As I've mentioned earlier, that flight departed from my home-base airport TLV.

- July 3rd, 1988: Iran Air Flight IR655, Airbus A-300 (299 casualties) was "mistakenly" intercepted by a RIM-66 Standard surface-to-air missile from USS Vincennes Navy cruiser over Persian Gulf

- 1985 in Afghanistan, 1987 in Angola, Mozambique and again Afghanistan, 1988 in Pakistan, 1993 in Abkhazia and many more across recent decades involve gunning down civilian aircrafts over disputed conflict zones, mostly done in purpose and then "justified" as "mistakes".

Source: https://en.wikipedia.org/wiki/List_of_airliner_shootdown_incidents#

Ukraine Int'l Airlines Flight PS752 case study - Video footage (print screen) source: https://twitter.com/i/status/1217254454300479494

In my opinion, if you are an official 'state empowered entity' and responsible to hold and operate that kind of weapon systems - there's only a thin line running between making an intentional 'legitimate' act of self-defense and a pure act of almost unruly terrorism – according to international laws and common values. Evidently, when the outcome is a civilian aircraft being shot-down (especially one that wasn't servicing army/governmental duties) it applies to latter option. Technical faults may occur when systems are tuned to 'Auto-Shoot' for interception of potential threats. Yet, we haven't heard much of such events so far. That itself indicates that even when Radar Auto-Detection is switched on – there is always some involvement / intervention of a human factor prior to 'no-return point' of shooting decision, which

1 - 1st Missile en-route to intercept

2 - 1st Missile Impact

3 - 2nd Missile en-route to intercept

4 - 2nd Missile Impact

5 - Aircraft Fireball in Midair

by nature is prone to suffer from ill judgment or mistakes (not to forget bad intentions).

One of the main reasons for these kinds of events is the widely spreading vector of para-military units/organizations that are gaining access and control over those types of weapon systems. Some of these semi-official groups or even rogue elements are claiming rights over "national defence" with backup of state administrations. It is very tempting to wave-off these events as 'accidents', rather than admitting the harsh true that these were avoidable errors. Having several organs playing armed defending role, specifically in rather small area, amplifies the risk and creates complex coordination environment allowing room for "Blame Game".

Stepping aside a bit from main focus of this article, I cannot ignore mentioning the numerous events in which Civilian/Cargo/Military aircrafts carrying civilians or soldiers on-board where targeted on purpose by rivals using SA or Manpads. Same goes for reviewing civil airliners being intercepted by Airforce fighter-jets. These threats are worthy of a separate analysis in other occasion. Just for the "taste" of it – there's a couple of prominent events:

- November 22nd, 2003: DHL Express GmbH Cargo A300 owned by European Air Transport was targeted by surface-to-air missile short after departure from Iraq's Baghdad International Airport, and managed to land safely.

International Association of
CIP Professionals

www.cip-association.org

Join the Community and help make a difference

Dear CIP professional

I would like to invite you to join the International Association of Critical Infrastructure Protection Professionals, a body that seeks to encourage the exchange of information and promote collaborative working internationally.

As an Association we aim to deliver discussion and innovation – on many of the serious Infrastructure - Protection - Management and Security Issue challenges - facing both Industry and Governments.

A great new website that offers a **Members Portal** for information sharing, connectivity with like-minded professionals, useful information and discussions forums, with more being developed.

The ever changing and evolving nature of threats, whether natural through climate change or man made through terrorism activities, either physical or cyber, means there is a continual need to review and update policies, practices and technologies to meet these growing and changing demands.

Membership is currently FREE to qualifying individuals - see **www.cip-association.org** for more details.

Our initial overall objectives are:

- To develop a wider understanding of the challenges facing both industry and governments
- To facilitate the exchange of appropriate infrastructure & information related information and to maximise networking opportunities
- To promote good practice and innovation
- To facilitate access to experts within the fields of both Infrastructure and Information protection and resilience
- To create a centre of excellence, promoting close co-operation with key international partners
- To extend our reach globally to develop wider membership that reflects the needs of all member countries and organisations

For further details and to join, visit **www.cip-association.org** and help shape the future of this increasingly critical sector of national security.

We look forward to welcoming you.

John Donlon **QPM, FSI**
Chairman
IACIPP

- November 2002: Arkia Israeli Airlines Flight IZ582, B-757 was the subject of an attempted shoot down by two (2) SA-7 ("Strela") surface-to-air missiles, missing its target by fractions of seconds/ meters (Aircrew actually witnessed the missiles passing-by in close proximity to the aircraft during after departure climb!). This was one half of two simultaneous attacks carried out by Somali Al-Shabaab terror group operatives (affiliated Al-Qaeda), while the other was aimed to tourist hotel in town using a driven car-bomb.

SA-7 ("Strela")

Source: https://en.wikipedia.org/wiki/2002_Mombasa_attacks#Aircraft_attack

- September 1st, 1983: Korean-Air flight KE007 was intercepted be a Russian Fighter-Jet 'Air to Air' missile for penetrating their prohibited airspace due to navigation error, and was suspected as an American espionage aircraft.

Source: https://en.wikipedia.org/wiki/Korean_Air_Lines_Flight_007

Getting back to the risk of being shot-down by nation-state forces (or 'presumed to be') and without jumping to conclusions, it is required to examine some common aspects, shared by these events:

- The origin of the involved weapon systems manufacturer? Should we dare to assume these weapons lack sufficient identification/safety mechanisms?
- The over-all geographical spread-out is an eye-catching alert as well. Twice at least: over Crimea Peninsula, over Iran, over Afghanistan…
- Is there a culture of an "easy trigger finger" by their actual field operators?
- Are some countries airspace is more prone to trouble? Is that to attribute a negligent approach towards human lives or is it some sense of 'political immunity' even in a case of severe results?

Now, who is responsible to determine which conflict has "matured enough" to the level to recommend no commercial overflights? There's a never-ending debate whether airlines should independently stop flights to/from/across disputed territories and conflict zones or should it be national/International decision. Most countries usually follow US FAA recommendations as a benchmark to their airlines, not to fly in specific region or even ban them. But maybe others should step-in.

Summary – what can be done?

On the one hand, nation-states should work to reduce weapon distribution to "'bad actors' (endangering civilian aircraft). They also must place more checks and balances for their own weapon systems usage – considering airports vicinity and/or airlines routes in use.

Aircraft manufacturers should also enhance efforts to produce even better identification codes and implement "Missile/Battery lock sensors" to notify pilots in time, so they might take mitigating actions, if they can. There are operational systems already installed on commercial aircrafts (not only for "Airforce 1"), but they are still not part of the regulations (cost related?), and may solve just part of the threat vectors.

Isn't there something else that int'l civil aviation actors & regulators (e.g; ICAO, IATA, FAA, CAA, etc.) should pursue or promote? I argue that there is sufficient room for them to implement better risk assessments and binding "Golden Guidelines".

Airline's management (security directors) should play a profound role in calculating risk management vs. routes economic operational efficiency, balancing considerations (keeping in mind the small profit margins in the industry). Security professionals should cling to international regulators recommendations on one hand, but must also independently analyze world's current threats and trends, assess what might bare considerable risk to normal service, and be able to react and influence routing due to non-recommended flight areas.

Preserving precious human lives should be everybody's first priority. But other priorities are the enormous damage in direct cost such as lost aircraft, compensations, and insurance. And indirect costs (diplomatic disputes between effected nations and aggressor side, loss of routes etc.) such as the inevitably damage to the airlines brand.

Bon-Voyage!!

By Roni Tidhar
Head - Int'l Consulting Services at
IAA. Israel Airports Authority

*** This article was initiated in pre-Covid-19 era*

Towards 2021 – Upcoming Organisation Risk & Resiliency Trends

From early 2020, businesses around the world collectively experienced the impacts of COVID-19 where there were business disruptions and even stoppages imposed by government regulations in a bid to contain the pandemic.

This disaster put an incredible strain on the national economy and had global impacts on the supply chains industry; as an example, when China, the world's factory, was impacted, global supply chains were affected. This tested the efficiency and strength of Business Continuity Plans (BCP) in organisations when disruption of common resources such as their workforce, supply chain, materials, transportation, and communications arise. Many organisations without a BCP or contingency plan also scrambled to put in "quick-fix" plans to counter the issues faced.

As we move into 2021, we explore what are the potential risks and top scenarios in the coming years and review our plans and ask "is there a need to review our plans that have served us well in 2020?"

2021 Risk Scenario and Profiling - Looking ahead by looking back

The core objective of any risk management system is to ensure the organisation endures whatever circumstances it may face during the course of business. As we look into planning for the upcoming year and ahead, we took reference from various reports such as Insurance Reports, the Global Risk Insights by the United Nations Security Council and other risk focused reports to sense on the key risk concerns.

Covid-19 is still the top risk. In 2021, it is high likely that the operational risks and business continuity concerns will still revolve on the topic of COVID-19. Though there are vaccines developed, with many countries having already started vaccination exercises for their citizens, many hope that this will slow the spread of the virus. However, it is expected to take 12 to 18 more months before we start to see the numbers in control or declining and another 2 to 3 years for recovery back to pre-COVID times. In total, the pandemic could take up to 5 years from outbreak till recovery.

In recent months, there is a call for concern regarding the emergence of new mutated COVID-19 strains such as N501Y (Africa, England) & E484K (Africa, Brazil). These new strains are more infectious and have the potential to spread faster than before. Many governments have been quick to re-imposing lockdowns to curb the spread. With the infection rate growing daily, COVID-19 will still be a top risk to watch out for in 2021 both affecting businesses and our daily lives. We believe more mutation of the virus is likely to happen and the challenges of effective vaccines are likely to continue for a while.

Changes in global economics. The economic policies from governments around the world will also become a major focus in the beginning of 2021. The trade war between two top economic powerhouses, US and China will continue for the foreseeable future. With the changes in leadership of a few leading governments, there will also be more uncertainties as we wait to see the direction of the new governments. How, then, does this impact business continuity and how about your supply chain?

There is also a false sense of security for many people. Thoughts of "we have survived 2020 and the pandemic, there is no need to make any further changes to our recovery strategies". It is important to note that with the successes of implementing Work-from-Home (WFH) strategy and other contingency plans, it is still crucial to conduct exercises to better improve these existing plans and to counter other scenarios that have not yet been tested in the past year. So far, majority of the major decisions are still made on the country level. Once we have moved to the recovery phase, business continuity planners are expected to take over and make these decisions. Are you ready for this? In the prolonged Pandemic crisis that has lasted for months and is projected to last even longer, businesses should consider how to survive a double crisis such as a typhoon or social unrest or even cyber-security outbreak. Always Expect the Unexpected.

Cyber-Security as an Emerging Risk. With the many changes to workplace operations involving the Work-from-Home strategy and the other contingency plans, there exposes many organisations to vulnerabilities involving Cyber-Security as employees work from less secure networks and having to bring more work operations online. Email phishing is also a growing threat with more people relying on a higher volume of emails, a less vigilant employee may just let a cyber threat slip in through the cracks. An effective IT strategy driven by management and leadership is one of the primary enablers to ensuring resilience. What is your recovery strategy and has it been put to the test?

A quick poll with over 50 participants showed that the top 3 risks that most concerns risk and business continuity practitioners are most concerned with Infectious diseases (87%), Cyber Security (85%) and Supply Chain breakdowns (62%), with Political unrest & demonstration (45%) coming in at a close fourth choice. Prolonged crisis complications and threats are also increasingly included as a top 2021 risk scenario. Risks and threats are also highly industry-specific, and it is recommended to discuss within your team, the senior leadership and industry-peers, to identify the top risks pertaining to your organisation and industry.

Continue strengthening and updating your Business Resiliency programmes to fit into the New Normal

Though we are 1 year into this New Normal of the COVID-19 world, there are still many unknowns– How long will the pandemic last? When will it peak? And when will subsequent waves hit? What we do know is that the COVID-19 related risks are unlikely to decrease substantially in the short run.

Especially now, we cannot let our guards down and get complacent about our business resiliency programmes. We used to encourage BC professional to plan for "Just in case" (JIC) but with the current environment we have to start considering the "It will happen" mentality. There

Building Trust and Co-operation through Discussion and Dialogue

Co-Hosted by:

HELLENIC REPUBLIC
Ministry of Migration & Asylum

REGISTER TODAY

Register for your Delegate Pass online Today

Greece lies at the crossroads of East and West, Europe and the Middle East. It lies directly opposite Libya so along with Italy is the primary destination for migrants coming from that conflict zone and is a short boat trip from Turkey, the other principal migrant route for Syrians fleeing there conflict there.

Greece has over sixteen thousand kilometres of coastline and six thousand islands, only two hundred and twenty-seven of which are inhabited. The islands alone have 7,500 km of coastline and are spread mainly through the Aegean and the Ionian Seas, making maritime security incredibly challenging.

The sheer scale of the migrant crisis in late 2015 early 2016 had a devasting impact on Greek finances and its principle industry, tourism. All this in the aftermath of the financial crisis in 2009. Despite this, both Greece and Italy, largely left to handle the crisis on their own, managed the crisis with commendable determination and humanity.

With their experience of being in the frontline of the migration crisis, Greece is the perfect place re-convene for the next meeting of the World Border Security Congress.

The World Border Security Congress is a high level 3 day event that will discuss and debate current and future policies, implementation issues and challenges as well as new and developing technologies that contribute towards safe and secure border and migration management.

The World Border Security Congress Committee invite you to join the international border security and management community and Apply for your Delegate Pass at **www.world-border-congress.com.**

We look forward to welcoming you to Athens, Greece on March 31st-2nd April 2020 for the next gathering of border and migration management professionals.

www.world-border-congress.com

for the international border management and security industry

Confirmed speakers include:

- Jim Nye, Assistant Chief Constable – Innovation, Contact & Demand & NPCC Maritime Lead, Devon & Cornwall Police
- Dr Olomu Babatunde Olukayode, Deputy Comptroller of Customs, Nigeria Customs
- Sanusi Tasiu Saulawa, Deputy Superintendent of Customs, Nigeria Customs Service
- Heiko Werner, Head of Security Group, Federal Office for Migration and Refugees, Germany
- Gerald Tatzgern, Head of Joint Operational Office, Public Security Austria
- Peter Nilsson, Head of AIRPOL
- Wayne Salzgaber, Director, INTERPOL Washington
- Tatiana Kotlyarenko, Adviser on Anti-Trafficking Issues, OSCE
- James Garcia, Assistant Director, Cargo & Biometrics – Global Targeting Advisory Division National Targeting Center – U.S. Customs and Border Protection
- Valdecy Urquiza, Assistant Director – Vulnerable Communities – INTERPOL General Secretariat
- Hans Peter Wagner, National Expert, Senior Chief Inspector, Federal Police
- Mile Milenkoski, Senior adviser, Department for borders, passports and overflights, Ministry of Foreign Affairs, Republic of North Macedonia
- Manoj Kumar, Second in Command, Indian Border Security Force
- Rear Admiral Mohammed Ashraful Haque, Director General, Bangladesh Coast Guard Force

Supported by:

OSCE Organization for Security and Co-operation in Europe · European Association of Airport and Seaport Police · AFRICAN UNION · ISIO · International Association of CIP Professionals · NS&RC

Media Partners:

BORDER SECURITY REPORT · WORLD SECURITY REPORT · World Security-index.com must be efforts made to further strengthen them and meet the changes in business models in this New Norm. It is evident that organisations with adaptable business continuity programmes fared better and were more resilient than other organisations – a clear indicator of the competitive advantage of business continuity. The Good news is that we now see higher awareness and attention on Risk and resilience from the Senior Management and Board of Directors (BOD).

We recommend considering the following to strengthen your BCP:

1. Your programme should be consequence-based rather than hazards-based –

It is simply not feasible to have one plan for each incident or scenario. Having more scenarios means that it is more difficult to maintain and too time-consuming to be effective. The key to a good Business Continuity Programme is to be flexible to cater to the various consequences such as loss of staff, loss of resources, equipment, data, critical applications and many others.

2. Involve Management in the Business Resiliency process –

Ensure the Board are involved in the process and made aware of the essential versus non-essential services so there are no conflicts between the management and the business management team during an incident. Leverage on the increased awareness and spotlight on business resiliency to increase management support and ensure buy-ins. Capitalise on the enhanced visibility of business continuity as a result of COVID-19 to push for more support for business continuity and related plans and activities.

3. Certification and Transition to ISO 22301:2019 –

If you are certified with ISO22301:2012, it is suggested to upgrade and transition to the revised 2019 standards. Being certified to the latest certification standards will ensure that your organisation's programme and plans are aligned and relevant to today's business environment.

4. Your Work-From-Home (WFH) Strategy –

Most office-based workers have adopted a remote working model during the pandemic. If WFH is to be your organisation's only back-up for loss of workplace, ensure that the employee agreements, policies, processes, security, regular testing, and insurance are in place as well as the technology and the leadership and management practices to make it work effectively and securely.

And importantly, one of the most important points to build up your business resiliency is:

5. Conducting Resiliency Exercises for your Top Risks in 2021 –

One key component in the Business Continuity (BC) Lifecycle that cannot be ignored is validation. It is vital to test the viability and workability of your plans or new policies. Conducting BC exercises can be done with different types of exercises and tests such as call tree exercises, tabletop exercises, walk-throughs, functional tests and live simulations.

Identifying your top risks would allow you to better craft the best exercises to better ensure that the objective of the exercise can be met. This is not just a paper-exercise but an opportunity to test your resilience capability in the COVID environment.

A quick poll of 50 participants shows that the most popular exercises that were conducted in 2020 were call-tree exercises, tabletop exercise and live simulation. This shows that even in the conditions that we are in with COVID-19, we can still conduct exercises. Some of the key considerations would be to adhere to the local regulatory guidelines such as safe management measures, social distancing and wearing of masks, avoid mass gatherings in one location.

Be sure to make use of technology to increase engagement through online simulation tools and to collect their responses and ease the exercise process. Another technological tool to take advantage of is emergency notification tools to reach all staff and collect responses quickly with instant reporting.

Conclusion

In a nutshell, a disruption in business operations and services, whether from a pandemic, natural disaster, a terrorist strike, a cyber-attack or a simple glitch, can seriously reduce your revenue and even do long-term damage to your business image. Taking reference to our current situation, nobody expected COVID-19 to have such a disastrous impact on a global scale. We need to aim to be flexible and adaptable, to have a strong business resiliency programme to pull through even the toughest situations.

It is recommended to think of the risk profile in the long term and not just year by year. As a prepared organisation, long term planning is needed to ensure the resiliency of an organisation. Plan for smaller 3-year milestones and a major milestone for your 15-year risk cycle to achieve your set risk profile. Get your Board of Directors and Senior Management to be on board and expand your business resiliency while there is a high awareness of risk and business continuity currently. When you and your organisation always adopt an "It will happen" mentality and be always prepared for the worst, you have a solid business resiliency programme.

by Mr. Henry Ee, Managing Director, Business Continuity Planning Asia Pte Ltd

Henry Ee is the Managing Director for BCP Asia (www.bcpasia.com). He is a certified professional with more than 25 years of experience in the business resilience industry. Henry has developed business continuity and crisis management programmes for the healthcare industry, inclusive of hospitals, clinics and their corporate offices. Currently Henry holds many voluntarily positions including Vice-President of RIMAS, Chairman for BCI Singapore Chapter, Member of UNDRR. He sits in the working committee for SS ISO22301.

BCP ASIA®
Preparing Business. Enhancing Minds

Maritime Domain Awareness - An Essential Component of a Comprehensive Border Security Strategy

For centuries, boundary lines have been used to identify a particular geographic area, city, state, province, or country. These borders not only represent jurisdiction over the area and all things in it, but they symbolize a transition from one set of laws, regulations, traditions, culture, norms, and even time zones to another. Sometimes these transitions are starkly different, and other times they are unnoticeable.

When we think of borders, we most often think of land with internationally codified boundaries that are easily discernible on a map. These are often identified or protected by some form of physical barrier, security force, or signage. However, in the maritime domain, there are no physical barriers or indications of a change in jurisdiction except perhaps a line on a nautical chart. In addition, while controlled entry at a legitimate Port of Entry (POE) is managed by government representatives, such as customs and border guards or police, the openness of the sea allows for numerous points of unobserved and uncontrolled entry. Seaports allow vessels carrying goods and people to pass through geographic boundaries and directly access a nation's sovereign territory. Unlike a vehicle that is stopped at a land border for inspection and can be denied entry, a ship enters sovereign territory before final immigration, and customs checks take place. While access can be

Ukraine-Russia border - Kharkiv Oblast, Ukraine (JJ Jones, March 2019)

denied at the POE by immigration and customs officials, the ship, as well as passengers and cargo, have physically entered the territory of the country and thus become the responsibility of the receiving nation.

The use of the maritime domain evolved slowly over a long period of time. As such, the culture and traditions associated with the maritime environment have deep roots and are very institutionalized. The broad availability of materials and knowledge for building vessels as well as ease of access to rivers, lakes, and oceans also resulted in the movement of people and cargo by sea becoming routine and unremarkable. For thousands of years, a ship's captain was god-like in the sense that he or she was the sole authority with no external oversight or control. Only recently, with technological advances such as the invention of GPS, satellite-based Internet, and space-based communication, has monitoring ships and routine communication at sea been possible.

The accessibility of the sea and its adjacent coastline also paved the way for the maritime domain to be far less controlled and predictable than its land counterpart. For many years, commercial shipping activity took place whenever and wherever the captain could locate a safe place to make landfall. This eventually evolved to the modern-day concept of commercial intermodal ports with dredged and marked channels. As maritime commerce evolved, ships also became larger and more powerful and could move more cargo over longer distances. These changes were also seen in military vessels that were able to project power at sea far from their homeland. These advancements led to important developments in determining sovereignty, such as establishing lines of demarcation on the seas, including territorial waters, the contiguous zone, the Exclusive Economic Zone, and International waters to represent a sovereign state's jurisdiction and rights to living marine resources, crude oil, and sustainable energy. However, the concept of freedom of navigation is still alive and well in the maritime domain and has the potential to impact any nation's maritime sovereignty at any given time. Therefore, it is absolutely vital for every maritime nation to adopt a Maritime Domain Awareness (MDA) system that allows the responsible government to observe what is happening at any given moment in the maritime environment and respond with an appropriate level of control to ensure the safety and security of its citizens as well as protect its economic interests and national sovereignty.

While no two ports are the same, the value and importance of the Marine Transportation System must be shared among nation-state leaders and therefore requires a common vision and mindset of having an effective MDA strategy. The Marine Transportation System (MTS) is a highly complex "organism" consisting of waterways, highways, railways, bridges, people, vessels, trucks, cargoes, and trains. The ports can be thought of as the heart, but the MTS extends well beyond the ports to landlocked regions around the world. It is the lifeblood that keeps trade, commerce, oil, fuel,

fisheries, and the supply chain and economy flowing. If one part of the MTS is damaged or weakened, it has cascading and potentially crippling effects on the entire system-locally, regionally, and globally.

A strong MDA strategy requires a systematic and layered approach using a variety of "hard techniques," such as tools, resources, and tactics to ensure safety and security for planned and unplanned events, and daily operations. For example, commercial vessel arrivals and departures require advance notice of arrival, cargo screening, and notification of their last port of call. Commercial vessels may also require a port state control inspection, review of the crew manifest, an escort, as well as a moving or fixed safety or security zone while in port and upon arrival/departure. This process requires risk-based decision-making tools, databases, radars, and security boats and crews trained in advanced security tactics and procedures. It requires trained inspectors, communication and surveillance equipment, intelligence analysis, cybersecurity, a properly marked channel, and a safe mooring. It requires rules and regulations to govern decisions and resolve discrepancies to ensure the safety and security of the vessel, crew, cargo, terminal, longshoremen, waterway, and all agencies in the harbor. This process happens around the clock and around the world every day. However, because every port is uniquely different, there must be a constant effort to adopt and improve "hard techniques" to enhance MDA strategy and adapt to the unique aspects of every port and geographic region.

The systematic and layered approach of a strong MDA strategy must also include "soft techniques" which are less visible, less tangible, often overlooked, undervalued, and highly complex, but are at least equal in importance and potentially more so than the "hard techniques." There are long-standing principles exclusive to the maritime environment that have withstood the test of time throughout history. For example, a naval captain is inescapably responsible for all aspects of their unit, and with that responsibility comes absolute authority and accountability. While legal responsibilities are outlined in laws and regulations, moral responsibilities in this inherently dangerous environment are critical for survival and resilience both at sea and ashore. Moral responsibilities among seafarers may differ from time to time, or region by region, but some are timeless, universal, and valued by all. For example, if there is a vessel in distress at sea, most mariners believe they have a moral responsibility to render assistance regardless of nationality or registry of the vessel in distress.

Another shared principle among seafarers is that the captain makes every attempt to save the crew and vessel before themselves -- a selfless servant to their crew. These same widely accepted leadership principles of responsibility, authority, and accountability at sea, must extend throughout the maritime domain, including among interagency stakeholders. ***The strength of maritime partnerships in large part determines the strength and resilience of the maritime domain***. These partnerships include all levels of government, private companies, public businesses, non-governmental organizations, labor unions, media, and both appointed and elected officials. Creating an MDA culture of coordination of information and operations among all maritime stakeholders requires considerable time and effort; however, collaboration is what creates lasting and effective relationships, ensures transparency, and ultimately builds trust. Principle-centered leadership, a common MDA vision, effective relationships, interagency, and international cooperation, and moral responsibility are critical components of building and maintaining an effective and resilient MDA posture.

Maritime Domain Awareness does not happen overnight and is perhaps never fully achieved due to the ever-changing dynamics of technology, leaders, adversaries, and the environment, yet it is a just and worthy cause. ***MDA begins with government leaders making it a priority and establishing the legislation and policies necessary for implementation.*** Transformational leadership is necessary to cause people who are responsible for oversight and regulation to think about their roles differently. They must look beyond themselves and their personal interests to promote cooperation among agencies charged with providing maritime security for the country and its citizens. This transformational leadership must be a marked departure from the transactional leadership that often takes place in the port and maritime environment where personal interests and enrichment supersede and

[Container ships at anchor off Huntington Beach waiting to enter the Ports of Los Angeles and Long Beach, CA, USA]

undermine the primary role of government officials. Leaders who adopt principles that promote a strong MDA posture both within and beyond their local or regional responsibilities are essential to the prosperity of the entire MTS. Trust is the glue that holds an organization together in good times and bad.

The maritime domain is a "system of systems" that functions together to be effective, and MDA must become a mindset for everyone involved. In practice, this means the people responsible for leadership and management must understand and cultivate a sense of ownership and a moral obligation for their respective piece of the system. Information flow and coordinated decision-making between the systems will help synchronize efforts, prevent competition for resources, and reduce interagency competition. Cooperation and communication ensure relevant and timely information is available to each responsible decision-maker in each system. This happens routinely in business situations where, for example, it is critical to have the right people such as longshoremen, crane operators, truck drivers, logistics personnel, and others available to ensure goods are loaded or unloaded to minimize the time a ship is in port and delays in the supply chain. MDA takes this type of coordination to a higher level and aims to deconflict and resolve problems before they happen to avoid large scale disruptions in the maritime environment and all that it impacts. ***MDA must be viewed as an essential component of a national strategy to protect vital economic and environmental interests as well as the lives and property of citizens.***

Commander J.J. Jones, U.S. Coast Guard, Retired
Border Security Advisor at CRDF Global

Captain Charlene Downey, U.S. Coast Guard, Retired
Owner of SeeWorthy Coaching & Consulting LLC

Cybersecurity for 5G: ENISA Releases Report on Security Controls in 3GPP

Cybersecurity for 5G: ENISA Releases Report on Security Controls in 3GPP

The European Union Agency for Cybersecurity (ENISA) provides authorities with technical guidance on the 5G Toolbox measure for security requirements in existing 5G standards.

The Agency has released its Security in 5G Specifications Report about key security controls in the Third Generation Partnership Project (3GPP), the main body developing technical specifications for fifth generation of mobile telecommunications (5G) networks. As vendors, system integrators and operators build, deploy and manage 5G networks, the ENISA publication underlines the need for cybersecurity and for the national regulatory authorities in charge of cybersecurity policy development and implementation to have a good understanding of these controls.

This new ENISA report is directly driven by the objectives set in the EU toolbox for 5G security - mainly technical measure 'TM02'. This technical measure calls on the relevant authorities in EU Member States to ensure and evaluate the implementation of security measures in existing 5G standards (3GPP specifically) by operators and their suppliers.

The aim of the report is to help national and regulatory authorities to better understand the standardisation environment pertaining to 5G security, 3GPP security specifications and key security controls that operators must implement to secure 5G networks.

Security and Criminology - Risk Investigation and AI

The security industry enters the 4th industrial revolution by merging technology with manpower. All practitioners will be involved one way or the other with AI (artificial intelligence) and therefore need to know what it is, how it works and how best to get the most out of it.

Millions of perpetrators are in a constant state of trying to beat the security system which is the technology and manpower. The vulnerability landscape is changing at a rapid rate because of this number of assailants trying to conceive new types of crime, the methods to accomplish their missions, or copying and perhaps updating or improving existing criminal methods to achieve their objectives.

The instrument is only as good as the user

The practitioner needs to out-think and outsmart the perpetrator therefore needs to use critical situational awareness thinking. This thinking process needs to comprehend intimately the full nature of the beast in order to select the appropriate technology and layer the manpower by skillsets to limit the level of collateral damage.

Based on the principle, ''security success depends on the level of situational awareness of the people on the ground (decision-makers) and their reaction speed'', the practitioner can use a variety of technologies to avoid deadly outcomes. Reaction speed is vital when a person is detected lying

Endorsed

IFPO INTERNATIONAL FOUNDATION FOR PROTECTION OFFICERS KNOWLEDGE TO PROTECT

ISIO - International Security Industry Organization

motionless on the ground. The appropriate technology that can summon speedily summon the manpower would most certainly save lives.

Situation

Already, many are using in some fashion AI, be it the security officers on the ground, crime analysts and investigators. There are AI systems at border control protecting the perimeter of the entire country and controlling the inflow and outflow of people. Safer cities being upgrade with technology and new aged cities springing up with buildings so high that they are above cloud level that are being run and managed with the state-of-the-art technology. These cities and neighborhoods all have video analytics that are in a consistent state of observation by watching for 'predictable' incidents.

AI impacted by the pandemic.

The lockdown because of the active biological threat got the IT people focused on the same goal in finding solutions from their perspective. The IT people ran onto the market making social distancing detection besides mask detection software. These do not serve much purpose for many reasons and furthermore can be dangerous if linked to a 'sound alarm' because panic can lead to deadly outcomes.

AI being used in this sector do require IT specialists but also security, criminology-investigation professionals because both intellects are required to ensure the AI system is built for purpose. Reason being is because of the surge of crime, be it new crime or evolving copycat crime will be intensive because of many reasons related to the pandemic and the outcome of the pandemic being the economic meltdown.

There are many companies that have already purchased the bells and whistles but not getting anything out of it or, some are using technology that is frowned upon and some using illegitimate technology. They may go far as to lay the blame squarely at the software designers, but this is not the issue.

The free downloadable booklet describes what is AI, how it works, and how to get the most out of AI. The principles and the formulas along with the scenarios give the users a method to conventionalize the framework to consider what technology and layered manpower by skillsets are best suited for a project. This is because – security is not a one size fits all kind-of-thing.

The AI users must address and focus on their field of interest, but regardless in one way or the other, they must be aware of the current multiple threats in theater because they more than likely will experience fallout from such. This talks the relevancy for this more important period.

At this moment in time, budgets could be stripped to the bare minimum and the practitioners must make do with what they do have or altering a few objectives to ensure that their technology and layered manpower by skillsets will be effective.

AI can assist in avoiding deadly outcomes and financial loss

There are specific sectors where security investment must be done because their field of interest has shifted up the ladder of high value targets whereas they may experience incidents leading to deadly outcomes or perhaps suffer intensive financial losses.

This is the time where transnational and local organized crime besides street gangs would grow in size due to the demand for specific goods that is at all-time high levels. Therefore, AI in all sectors where tracing and tracking of goods and people will grow in demand, besides increasing the need for alert notification technology so as to increase the reaction speed by responders.

And most importantly, there is essential software that is designed to seek out specific scenarios which could lead to emergency and medical support or other interventions that need to be implemented to save lives. For example, identify man-down which speaks for itself as an essential software.

This moment in time must be considered in a different light. To illustrate the meaning of such would be like describing the difference between crime investigators and security investigators. Crime investigators are only summoned after the fact.

Security investigators must find the crime or issues before the fact.

Find the crime using data!

The objectives are to find a person of interest and then to determine if they are working on their own with others either voluntarily or under duress. It is suggested to use triangulation research which means using all intelligence gathering methods and investigation methodologies to bring all the information together to get the big picture.

The AI user therefore needs to encapsulate security and criminology-risk knowledge besides knowing the motivations for crime and the methods used by criminals to find a person of concern. They then may need to use investigation or incident software methods of reporting and then to flag to identify incidents that will lead to finding a person of interest.

The booklet gives direction on the types of information resources to consider which could be technologies that can secure the evidence and provide proof of the fact. By identifying the pattern quickly and following the pattern, the investigator can then select remedies in the form of technology or skilled manpower to limit the level of collateral damage.

In this way, the AI would machine learn – perhaps make programmed decisions and act or react (machine doing) besides using the human factor.

No practitioner living at this moment in time has experienced this form of multiple threats and practitioners in the future will always manage threats that others have ever experienced before. This is the time to equip one's intelligence of the tools in hand and get to know and mix with like-minded practitioners.

The above and more is outlined in the free booklet AI link to view or print - https://www.human-investigation-management.com/ai-for-security-criminology-risk-investigation-management

By Juan Kirsten

ISIO [International Security Industry Organization] and IFPO [International Foundation of Protection Officers] have endorsed AI for Security Criminology-Risk.

How artificial intelligence can help transform Europe's health sector

A high-standard health system, rich health data and a strong research and innovation ecosystem are Europe's key assets that can help transform its health sector and make the EU a global leader in health-related artificial intelligence applications.

The use of artificial intelligence (AI) applications in healthcare is increasing rapidly.

Before the COVID-19 pandemic, challenges linked to our ageing populations and shortages of healthcare professionals were already driving up the adoption of AI technologies in healthcare.

The pandemic has all but accelerated this trend. Real-time contact tracing apps are just one example of the many AI applications used to monitor the spread of the virus and to reinforce the public health response to it.

AI and robotics are also key for the development and manufacturing of new vaccines against COVID-19.

A fresh JRC analysis shows that European biotech companies relying on AI have been strong partners in the global race to deliver a COVID-19 vaccine.

Based on this experience, the analysis highlights the EU's strengths in the "AI in health" domain and identifies the challenges it still has to overcome to become a global leader.

High standard health system safeguards reliability of AI health applications

Europe's high standard health system provides a strong foundation for the roll out of AI technologies.

Its high quality standards will ensure that AI-enabled health innovations maximise benefits and minimise risks.

The JRC study suggests that, similarly to the General Data Protection Regulation (GDPR), which is now considered a global reference, the EU is in a position to set the benchmark for global standards of AI in health in terms of safety, trustworthiness, transparency and liability.

The European Commission is currently preparing a comprehensive package of measures to address issues posed by the introduction of AI, including a European legal framework for AI to address fundamental rights and safety risks specific to the AI systems, as well as rules on liability related to new technologies.

A word from the Chairman

John Donlon
Chairman
International Association of CIP Professionals
(IACIPP)

International Association of CIP Professionals

Preparation & Resilience

Some months ago, I wrote in this publication, about the need to be both better prepared for and more resilient in managing and recovering from the impact that an outbreak of an infectious disease can have on every aspect of our daily lives. My comments were not only related to this current pandemic but were to be considered across the range of threats that our nation's infrastructure face whether they be natural or man-made. The International Association of Critical Infrastructure Protection Professionals has also provided some significant focus on these matters through its network of Regional Director's and within the pages of its website.

It has been refreshing to see how much is currently being written and published about preparedness and resilience but such a pity that more attention has not been levelled on this subject prior to the challenges we have faced in the past year. Security professionals have for some time been espousing the need for greater investment, research and understanding on these issues but often this has fallen on deaf ears, across both the public and private sector.

Each year, the World Health Organization tracks approximately 200 epidemic events globally. Many of these are controlled at a local or regional level but, some infections, as we have seen with COVID-19, pose a pandemic threat to the world. As that threat becomes a reality the costs are heavy both in terms of the loss of life and the impact on the economy. As infectious disease outbreaks increase in frequency it is somewhat reassuring to note that there seems to be emerging a greater understanding and an acceptance that we must improve preparedness and build for pandemic resilience.

Within the United Kingdom there is a Joint Committee which is appointed by the House of Lords and the House of Commons to consider the National Security Strategy. This group has recently (December 2020) published their findings on Biosecurity and national security. This is an extremely interesting read delving into several areas, which include:

- Getting ready–Identifying and preparing for biological risks
- How prepared core capabilities were in the face of covid-19
- Resilience on the 'frontlines'
- Strategy leadership – and –
- Planning for unexpected futures

The report found that although the UK had extensive and well-regarded plans for a significant disease outbreak—those plans were mainly focused on a flu pandemic. This review clearly highlights that the challenges faced by the UK Government in dealing with COVID-19 reflected long present gaps in the planning and preparation for biological risks.

Towards the end of 2020 we also saw the introduction of a National Preparedness Commission in the United Kingdom. The stated mission of which is to promote better

The Results Are In...

The IACIPP Poll

The results are in! Responses to the recent poll give the following insight.

Q. What new security technology do you plan to employ in your enterprise in 2021?

- We plan to use some of these technologies - 27%
- No plans for any of these - 27%
- We currently use some of these technologies - 18%
- Artificial Intelligence - 9%
- Security robots - 9%
- Security cameras - 9%
- Drones - 0%

Vote on our next poll at www.cip-association.org:

Does your organization have a policy addressing the use of personal devices (BYOD) in the workplace?

preparedness for a major crisis or incident. The remit of the Commission is not just the considerations around future pandemics but across the myriad of threats that are out there. Although at a very early stage of its formation the Commission has the potential to significantly impact top-level thinking in achieving a whole system approach to resilience and preparedness.

The Commission is funded by businesses, including the likes of Amazon, and is made up of some very experienced and influential individuals (45 in total) including people from the NHS Confederation, Tesco, the British Red Cross, Google Cloud, Unilever, the Bank of England, the National Grid and many more. I wish them every success in their endeavours, as their successes will benefit us all in the future.

These are just a couple of recent examples of where we see the importance of preparedness and resilience rising to the top of both the political and commercial agenda. There is no doubt that the current pandemic has been a catalyst to trigger the drive for some coordinated action. Sometimes it takes a difficult and challenging situation to make us reflect, to make us learn and to put us in a better position to manage any future national or international crisis.

John Donlon QPM FSyI
Chairman
International Association Critical Infrastructure Protection Professionals (IACIPP)

Latest Resources from IACIPP

Members of IACIPP can enjoy benefits including access to a range of online resources including video presentations, conference papers and magazine back issues, as well as a whole range of White Papers.

Latest White Papers include ‘Cyber Terrorism and Extremism as Threat to Critical Infrastructure Protection book’ by Denis Caleta, James F. Powers and ‘Indication of Critical Infrastructure Resilience Failure’ from Assoc. Prof David Rehak, Ph.D., VSB – Technical University of Ostrava, Faculty of Safety Engineering.

More details and access to the Resources and White Papers can be found at www.cip-association.org.

Resilience and Social Unrest: Tentative hypotheses for forecasting movements that manifest violent social unrest.

I expect than most readers will already have a social unrest plan as part of their duty of care to their staff. This plan will vary massively in scope, detail and threat depending on where their staff are in the world. For those of you who have not personally been caught up in violent social unrest it can be a deeply troubling episode especially if you are unable to anticipate the level of this threat. The speed at which the threat of violent unrest can manifest itself is stunning and the cause can be wholly unpredictable.

Academics at University College London have anticipated a 'cascading effect 'of social unrest post Covid and many other studies endorse the growth in social unrest. Although trying to distil a predictive model for potential violent unrest is plagued with notable exceptions, variables, and valid counter arguments, nevertheless, some attempt at logic and some perhaps intemperate generalisations can form hypotheses for a more sophisticated model in due course.

This brief article examines some limited factors which promote violent social unrest and offers some tentative hypotheses which could be considered in response planning.

What are we looking for?

The current literature considers

many aspects of social unrest ranging from causality to prediction . Historical analysis of social unrest, such as Archer's , has focused on the root causes with corollary consideration of subsequent effects. The specific issue of the potential for violence is less considered. I am not going to debate causes or flashpoints or the impact of social media worthy though these debates are. The article focuses on just three issues (amongst many others) that help to predict a social movement's propensity for violent unrest.

These are:

- The legitimacy of the cause.
- The leadership or otherwise of the movement.
- The maturity of the movement.

Legitimacy

Legitimacy is important as it gives any movement credibility which in turn generates intellectual and political (with a small or large P) debate and/or traction for the movement. Legitimacy has several subsets, three of them are, realistic aims and objectives, a structured opposition to their aims and a moral foundation,

Realistic clear aims and objectives

If success is to be considered, then the movement has to have, or have had a realistic clear strategic or tactical intent in the first place. For example, the poll tax 'rioters' (1989-90) , the UK suffragette movement , had relatively clear aims and they can easily be distinguished from other episodes such as the bizarre St Scholastica Day riots in Oxford in 1354, which lacked any intent for national social change (it began as an argument over the quality of wine in a tavern but nevertheless cost 90 lives) . This need for stated aims seems critical in the first place, albeit aims can be clarified and refined as the movement gains momentum. For example, in terms of gay rights timelines , the UK Wolfenden Report in 1954, recommending the decriminalisation of homosexuality, could scarcely have envisaged the far-reaching developments that have occurred since. Nevertheless, a movement with wholly unrealistic, or ill-defined ambitions are far less likely to achieve any success. For example, the student riots in France (and elsewhere) in 1968 are widely regarded as almost spontaneous, 'These rebellions were not planned in advance, nor did the rebels share an ideology or goal' (nor did they have any single charismatic leader). They originated in demands for sexual liberalism in halls of residence, morphed into demands for educational reform and ended in the proposition of a socialist revolution   The result was, the re-election of the incumbent President de Gaulle's party with a larger majority.

The presence of realistic bounded aims and objectives whilst not vouchsafing peaceful protest does at least indicate a focus to them and limited realistic ambitions which can be taken seriously.

Opposition; the sincerest form of flattery?

Paradoxically in the case of the UK Suffragette movement, a powerful voice against their cause was from a well organised and an intellectually credible women's anti suffrage campaign. However, the further paradox is that the formation of a coherent group in opposition meant that the proponents' arguments for suffrage were actually worthy of opposition and inherently had some merit.

The proselyting force with which the proponents make their arguments is also a distinguishing feature of a credible movement. (Please note, this is not the same as endlessly iterating a baseless allegation so that it eventually gains traction with the gullible). The sheer passion with which suffragettes held their opinions was commented on by Bush .

'Anti-suffragists could not match the fervour of their opponents, but they were clearly a force to be reckoned with rather than merely a target for suffragist ridicule'.

Thus, coherent opposition to a cause is not merely flattering, it conveys intellectual credibility to the proponents of the movement.

A moral foundation

The successful movement (and potentially increasingly less violent) also appears to have a more readily recognisable moral basis which is begrudgingly appreciated even by non-sympathisers. This is very difficult to define as even terrorist organisations claim a moral high ground. Nonetheless, movements closely allied to seeking equality, freedom, justice, or some redress of legitimate grievances appear to have more chance of success unless confronted with a resolutely totalitarian or highly effective government backed opposition.

This power of a moral foundation was commented upon (in a US context) by Jasper (1997)

'Moral protests spans not only state lines but class boundaries… What moral visons inspire outrage about often distant practices and institutions.'

It appears that this moral basis is a unifying feature that allows shared values to generate global empathy with just causes.

Summary

A movement demonstrating legitimacy through these three elements will tend to be, focused, taken seriously and less willing to compromise its legitimacy by violence which risks robbing it of its moral position.

A charismatic leader

Despite the success of some 'cellular' movements which act as a loose federation, notably the anti 'Poll Tax Movement' in the UK and the disparate aims of the 'Gillet Jaune' in France many movements coalesce behind a single charismatic figure . This is especially the case of political movements such as Indian Independence, Gandhi, South African Apartheid, Mandela, and more recently the Ugandan opposition leader and former singer Bobi Wine. Generally, this leadership makes the movement less prone to violent protest; many effective leaders actively discourage violence especially if their cause is 'externally' and/or 'globally' perceived to be legitimate. For example, Svetlana Tikhanovskaya, the arguably disenfranchised candidate pitted against the long-time incumbent Alexander Lukashenko in the Belarus elections, once deported to Lithuania called specifically for peaceful protests . In most of these cases any violence resulting from initially peaceful protests is generally directed at government and state institutions. However, a movement with a leader with a less moral credibility can be prone to incite followers to forms of insurrection and unilateral action by factions is possibly more likely as evidenced by the unfortunate events in the USA recently.

In many ways the USA violence was curious hybrid between a led movement, the Republican Party, and a leaderless faction with a supposed 'shadowy' virtual leader 'Q', part of the Q Anon movement. The cellular and in today's terms 'virtual' leaderless version of a movement is probably the least predictable. The implicit autonomy granted to local or regional organisers is by implication almost unbounded. Without denigrating in any way, the aims of Black Lives Matter, (BLM) it currently has no leader akin to the earlier US Civil Rights Movement where leadership could be seen to vest in Martin Luther King or depending on persuasions, even Malcom X . Consequently, the demonstrations of support for BLM ranged wildly from Formula 1 drivers 'taking the knee' before the race to, in the immediate aftermath of the killing of George Floyd, widespread opportunistic arson and looting with little or no relationship to the cause of BLM as well as more minor sympathetic disturbances outside the US.

Thus, an assessment of the leader, their control, their degree of legitimacy, and naturally their direction to followers is critical to forecasting the potential for violent protest.

Maturity of the social movement

As social movements mature and their aims and objectives are either taken seriously or achieved to a limited extent they often shift from any violent conflict to a more persuasive conventional position. As noted by Blumer (1995) .

'As a social movement develops, it takes on the character of a society. It acquires organization and form, a body of customs and traditions, established leadership, an enduring division of labour, social rules and social values.'

The argument is that mature movements pose less threat of violence than their less predictable embryonic siblings for whom violent protest seems the only thing that attracts attention their cause. Interestingly, in the UK the Black Lives Matter movement has already rebranded to become the 'Black Liberation Movement'. thereby gaining legal status, allowing donations and memberships. Arguably the movement is becoming a more mature and controlled conventional movement where non-adherents to direction can be excluded from membership.

Summary

One hesitates to summarise these propositions but as a rough guide on which one might base security decisions, I offer the following 'rules of thumb', or more precisely hypotheses, which I encourage you to debate at your leisure.

- Embryonic movements tend to use violent protest to attract attention to their cause.
- Any organisation with a 'Youth Wing' will almost certainly be prone to violent protest.
- Any movement without clear aims and objectives and/or a moral foundation might be more prone to compensatory violent protests.
- Any serious repression of almost any legitimate social movement with a reasonable moral foundation will tend to lend it legitimacy and globalise it.
- Charismatic leaders of morally credible movements tend to discourage violent protest.
- Cellular, dispersed, factional protest organisations without a strong leader are less predictable and prone to violent protest.

by Dr Chris Needham-Bennett, MD
Needhams 1834 Ltd

WMO boosts regional cooperation in Asia-Pacific

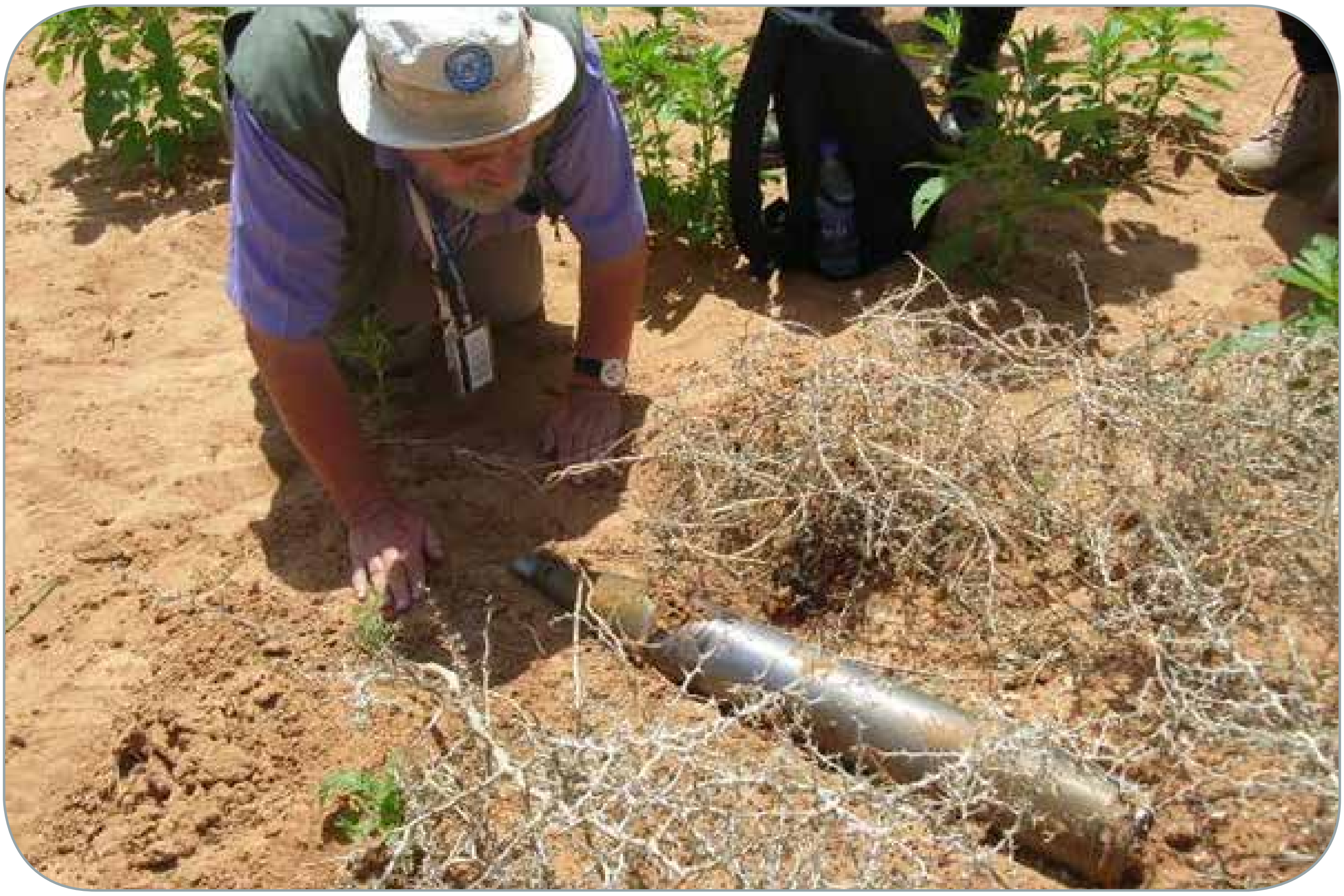
The Typhoon Committee, which symbolizes the successful cooperation between WMO and the United Nations Economic and Social Commission for Asia and the Pacific, holds its 53rd annual session, woth participants from the National Meteorological and Hydrological Services (NMHSs) and national Disaster Risk Reduction (DRR) agencies who will exchange information on achievements of the past session, review activities of the Members, as well as operational and research collaborations, with the clear focus on reducing the number of lives lost and damage to property caused by tropical cyclones and typhoons.

On top of the disruption and catastrophic impacts caused by COVID-19, the Asia-Pacific region was hit by successive hazards in 2020, including tropical cyclones, floods, droughts, sand and dust storms and heatwaves. 23 named tropical cyclones of tropical storm intensity or above formed over the western North Pacific and the South China Sea.

The strongest tropical cyclone of the season was Super Typhoon Goni (2019). It made landfall over northern Philippines on 1 November and caused catastrophic damage. A minimum pressure of 912.1 hPa was reported in Virac and a maximum gust of 198 km/h was reported in Legaspi City. 25 people died and 399 injured, and the social and economic loss was estimated to be over 17 billion Philippines Peso, according to a report from the Philippines national meteorological and hydrological service PAGASA.

Two major tropical cyclones hit the Korean Peninsula within a few days in early September, with Typhoon Maysak making landfall near Busan on 3 September, followed by Haishen on 7 September. Maysak brought 1037 mm of rainfall over two days to a site on Jeju Island, and wind gusts on the island up to 165.6 km/h, with high waves of more than 8 m. The damage costs of Mayask and Haishen reaches over 200 million USD, with a possible recovery cost of 548 million USD, according to a report submitted to the Typhoon Committee by the Korea Meteorological Administration. Both tropical cyclones led to significant flooding on the Korean Peninsula and in western Japan, and 41 lives were lost when a ship sank off western Japan during the passage of Maysak.

State Sponsored Terror: The Djebokaye Bomb



"Man that is born of woman hath but a short time to live," I looked around at the sombre scene, beyond the rank of blue-helmeted soldiers the desolate desert stretched away. By my reckoning the nearest waterhole to the North was in Libya, three days' drive away.

"In the midst of life, we are in death" Certainly true for the remains, just bare bones really, of the people we had found here – how many, and how old, we had no way of knowing. Certainly there were families – men, women and children by their various skeletal remains, but in this harsh landscape there was no telling their history.

Indeed, it was lucky that I had the Anglican service to hand, only because the week before I had been tasked to investigate the remains of a Sudanese Air Force helicopter gunship shot down by 'rebels' and, since it was made in Russia, we needed to see the serial numbers to determine if supplying it was possibly a breach of the arms embargo on the Sudan. I expected that the crew would still be there, and indeed they were, so we gave them as decent a burial as we could.

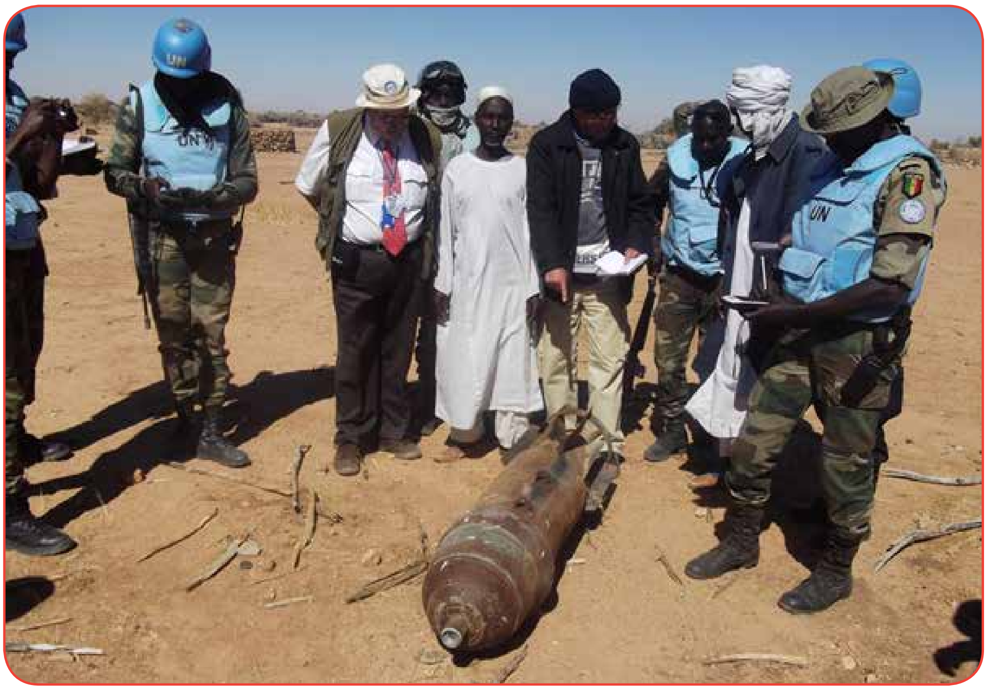
In this case too, we set to and buried them, as they had presumably lived, together in a big trench-like grave carved laboriously out of the 'serir' –the hard packed gravel and clay surface of the desert floor here in the remote corner of the Sudan that was northern Darfur.

I finished my reading and nodded to my escort commander – a Major in the army of far away Senegal – who gave the order. The troops came to attention, presented arms, and we stood motionless for a moment before getting back into our vehicles to continue our quest.

For we were on our way to look for evidence of a war crime, a "crime against humanity" in lawyer speak.

With me was my close colleague Mohammed Moufid, who before he retired was Director of Civil Aviation for the Kingdom of Morocco. Now he was the Aviation Expert of the UN Security Council's Panel of Experts on the Sudan whilst I was the Arms Expert on the same Expert Panel.

We were looking for a speck on the large scale map of northern Darfur that contained the remains of the village of Djebokaye, where it was alleged that the Sudanese Air Force had dropped a napalm bomb or bombs, to the severe detriment of the civilian population and also clearly – if true – breaching the Geneva Conventions(the 1980 addition, for the pedants amongst us). At that time the Sudanese had developed the bad habit of dropping bombs from Antonov transport aircraft, just by rolling them out of the open rear door – this in turn meant that the aiming was clearly inaccurate and that the bombs often failed to explode because the fuzes didn't work properly.(The good side if that, of course, is that it's much easier to examine an unexploded bomb for markings, serial numbers, etc., than one that's gone bang and is in lots of bits)



Tine ZAB The Djebokaye Bomb with (centre) the author, Ali Ahmed, the village headman, and Mohammed Moufid....

The Air Force had bombed, of course, because the area was allegedly controlled by rebel factions – terrorists, freedom fighters or 'armed opposition groups' depending on your standpoint, and thus a civil war was undeniably raging. Indeed, a few weeks later and we, the UN force, in our turn were harassed by helicopter gunships of the Sudanese Air Force who later claimed that they had 'mistaken' us for rebel troops.

Hence the escort, we had flown in to the tiny town of Tine the previous day by helicopter from the Darfurian capital of El Fasher. Tine is on the border with Chad and just south of the frontiers with Libya and Egypt. It's not the most vibrant of towns but it does hold a base for the UN peacekeeping troops there.

Now you can't go safely into a war zone without packing a fair amount of muscle yourself – well, not unless you fancy being a latter day Terry Waite and becoming someone's hostage for quite a while.

So we had a company of infantry as protection, around 180 men, in eight desert-ready lorries, plus three Land Cruisers for us, our bodyguards, the escort commander and two civilian policemen from – of all places – China. To look after this little lot we had a breakdown truck, and ambulance with paramedic, a fuel truck for us and a fuel truck for the visiting helicopter support. To guard all this desirable booty we had four armoured cars from the Pakistan Army. As the phrase goes, we were 'mob handed'.

Driving in the desert is an art form in itself – the going routinely ranges from bad to atrocious, but after being bogged down a few times, which can be a real bugger, you hopefully learn to read the terrain. So, while you might want to set a compass course to your objective, then your actual route seen from above will look like the trail of a demented spider as you skirt around dunes and try to avoid deep wadis, or valleys.

It was in one of those that we came across the bones with which I started this account and where we'd stopped to pay our respects.

Another hour of hot, dusty travel passed by before we found the remains of the scattered village – more or less where we thought that it would be. Good navigation on everyone's part. We went into defensive mode, throwing out pickets with the armoured cars in support before starting to talk to the remaining villagers and also to examine a real, live, napalm bomb, which had failed to explode. So we were able to examine it, ensure that it had been rendered safe and load it up to take away as evidence.

The sun was already well past its' zenith – and we didn't want to be unprepared for nightfall which comes quite suddenly in those parts – so we swiftly began to retrace out tortuous way back to Tine, where I had the warhead – which alone weighed empty some 46 kilos – cut up and prepared for shipment back to El Fasher.

Because I knew that the Sudanese authorities would be somewhat unhappy with my findings I made some underhand preparations of my own and surreptitiously shipped the warhead out, manifested as 'spare parts for repair' to the UN logistics base of Entebbe in Uganda, to await my arrival there later, after which is was simple to DHL it back to the UK, again marked as 'spare parts'. It duly arrived unquestioned....

It was a Russian made bomb –a ZAB 250-200 made by the Bazalt company near Moscow - but don't get too caught up by that because it doesn't mean in the topsy-turvy world of the illegal arms trade that the Russian knew where it had ended up.

Indeed, I'd had first - hand experience of the fact that things didn't always go where they were intended few weeks previously when my night's kip in a Khartoum hotel was rudely interrupted by Israeli bombers attacking the Yarmouk arms factory on the other side of the Nile from me. Some ammunition made there had ended up in the hands of Hamas, who had used it against them. The Sudanese government protested afterwards that this supply was done without their knowledge and, for once, I'm inclined to believe them.

A few months later I was able to travel to a Godforsaken spot called Sopo in south Sudan, near the border with the Central African Republic where, again, we were able to prove the use of napalm on the local population. So, time to make a formal report…….

It made perhaps half a page in the February 2012 Report of the expert panel to the Security Council which, normally, would have been published by the March of that year. But it wasn't because a member of the P5 (the five permanent members of the Security Council) vetoed it No prizes for guessing which one…..

And there matters rested for several years. True, there were outstanding arrest warrants issued by the International Criminal Court at The Hague for President Omar Hassan Ahmed Al Bashir and his henchmen but they were apparently securely in power and couldn't be touched in their Khartoum power base.

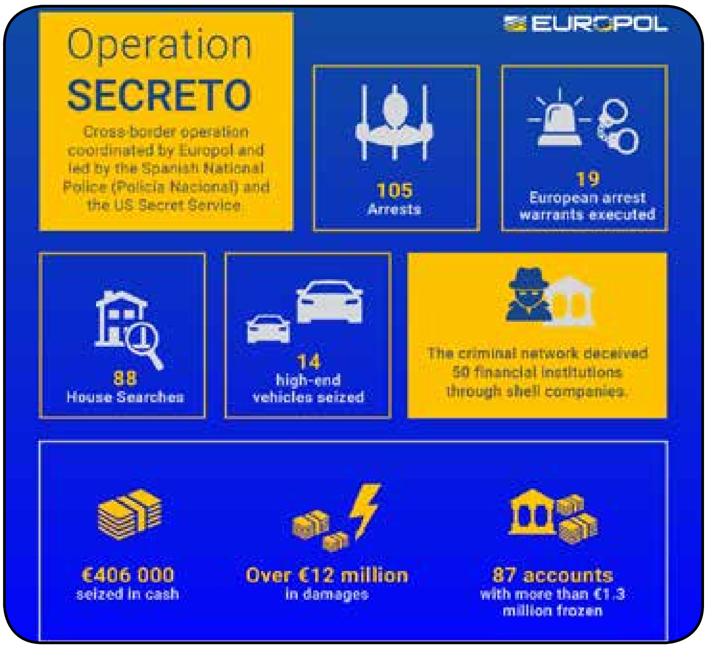
But then there was a revolution and their world changed, not for the better, The new government of the Sudan has now agreed, as part of a peace deal, to send them all to The Hague to be tried.

Indeed, the first of them, the former Janjaweed militia leader Ali Mohammed Ali, aka Ali Kosheib, has surrendered to the Court already and is now in custody at The Hague awaiting his trial later this year.

It is still remarkably unusual for Governments to be held accountable for their actions but maybe justice will be finally given to the villagers of Djebokaye and Sopo and all the other people in Darfur who have suffered so much for so long …..

by Brian Johnson-Thomas

105 Arrested For Stealing €12m from US-based Banks



EUROPOL

Operation SECRETO

Cross-border operation coordinated by Europol and led by the Spanish National Police (Policía Nacional) and the US Secret Service

105 Arrests

19 European arrest warrants executed

88 House Searches

14 high-end vehicles seized

The criminal network deceived 50 financial institutions through shell companies.

€406 000 seized in cash

Over €12 million in damages

87 accounts with more than €1.3 million frozen

A cross-border operation coordinated by Europol and led by the Spanish National Police (Policía Nacional) and the US Secret Service resulted in the dismantling of an organised crime group involved in fraud and money laundering. The operation involved also police services from Austria, Denmark and Greece as well as the US Department of Justice and the US Financial Crimes Enforcement Network.

On the coordinated from Europol action day, law enforcement offices carried out more than 40 house searches, arrested 37 suspects (2 in Austria, 11 in Greece, 23 in Spain and 1 in the UK) and seized 13 luxury cars. The follow up actions led to the freeze of 87 bank accounts worth €1.3 million.

The criminal organisation, mainly formed of Greek nationals, set up shell companies in the United States and opened bank accounts for these companies. To gain the trust of the financial institutions, members of the criminal network made transfers to the US-based accounts from different locations in the EU. Based on this trust, the American-based banks issued debit and credit cards for these accounts. Retailers in on the scam, most of whom were in Spain, used the payment cards to finance the available credited amounts on the cards. To launder the stolen funds, they transferred them to different bank accounts, owned by members of the criminal network located in several EU countries. More than 50 American financial institutions became victims of these fraudulent activities losing over €12 million.

Ten Hackers Arrested for Sim-Swapping Attacks Against Celebrities

A total of 8 criminals have been arrested on 9 February as a result of an international investigation into a series of sim swapping attacks targeting high-profile victims in the United States. These arrests follow earlier ones in Malta (1) and Belgium (1) of other members belonging to the same criminal network.

The attacks orchestrated by this criminal gang targeted thousands of victims throughout 2020, including famous internet influencers, sport stars, musicians and their families. The criminals are believed to have stolen from them over USD 100 million in cryptocurrencies after illegally gaining access to their phones.

This international sweep follows a year-long investigation jointly conducted by law enforcement authorities from the United Kingdom, United States, Belgium, Malta and Canada, with international activity coordinated by Europol.

Initiated in the spring of 2020, the investigation uncovered how a network composed of a dozen criminals worked together to access the victims' phone numbers and take control of their apps or accounts by changing the passwords.

This enabled them to steal money, cryptocurrencies and personal information, including contacts synced with online accounts. They also hijacked social media accounts to post content and send messages masquerading as the victim.

This type of fraud is known as 'sim swapping' and it was identified as a key trend on the rise in the latest Europol Internet Organised Crime Threat Assessment. It involves cybercriminals taking over use of a victim's phone number by essentially deactivating their SIM and porting the allocated number over to a SIM belonging to a member of the criminal network.

INTERPOL and OECD to identify areas for enhanced cooperation

INTERPOL and the OECD have signed a letter of intent expressing a shared interest to identify areas for increased cooperation.

INTERPOL Secretary General Jürgen Stock and OECD Secretary-General Angel Gurría signed the letter at a virtual ceremony on the margins of the commemoration of the 60th anniversary of the signature of the OECD Convention.

Areas identified for enhanced cooperation include artificial intelligence, environmental security, corruption and financial crimes, cyber and cyber-enabled crimes, and crimes related to mineral supply chains.

The letter builds on recently intensified strategic consultations between the two Organizations in the framework of recent engagements with the G7 and G20, and addressing the unprecedented impact of the COVID-19 global pandemic.

Terrorist groups using COVID-19 to reinforce power and influence

The impact of COVID-19 on global terrorism, trends and potential risks related to attacks on vulnerable targets and bioterrorism is the focus of a new report issued by INTERPOL.

The assessment takes into consideration the following five main threat factors: COVID-19 outbreak characteristics and medical advances; Global or national response; Social climate; Resilience of the security apparatus; Strategies and capabilities of terrorists and other non-state actors (NSAs).

As COVID-19 cases subside in some regions and surge in others, the report underlines the critical need to monitor the reaction and response by terrorist networks, violent extremist groups, and other potentially dangerous NSAs.

Early in the pandemic, certain terrorist groups and other NSAs used the pandemic to reinforce their power and influence, particularly among local populations, or to expand their external financial resources. The report also highlights how the impact of COVID-19 on the global economy is likely to indirectly affect funding available to terrorist organizations.

"Our terrorism assessment report is another tool to help law enforcement identify and address these evolving threats, in what continue to be challenging circumstances," added Secretary General Stock.

The use of disinformation and conspiracy theories also appears as a common denominator across all idealistic spectrums, and as an indicator of prevailing threats against priority targets.

The presence of far-right supporters in anti-COVID-19 activities in a growing number of western countries illustrates attempts to use the pandemic to exploit divisions. Law enforcement will continue to face attempts by far-right violent extremists to radicalize social movements, such as clashing with far-left groups and/or provoking the use of force.

INTERPOL report charts top cyberthreats in Southeast Asias

An INTERPOL report has highlighted the key cybercrime trends and threats confronting the Association of Southeast Asian Nations (ASEAN) region.

INTERPOL's ASEAN Cyberthreat Assessment 2021 report outlines how cybercrime's upward trend is set to rise exponentially, with highly organized cybercriminals sharing resources and expertise to their advantage.

It provides strategies for tackling cyberthreats against the context of the pandemic which has seen more people going online using mostly unprotected mobile devices, creating a surge in cybercriminal activities profiting from the theft of personal information and credentials.

The report further describes the essential collaboration on intelligence sharing and expertise between law enforcement agencies and the private sector, facilitated by INTERPOL's global network.

The INTERPOL's ASEAN Cybercrime Operations Desk (ASEAN Desk) with the support from law enforcement agencies in the region and INTERPOL's private sector cybersecurity partners identify the region's top cyberthreats: Business E-mail Compromise; Phishing; Ransomware; E-commerce data interception; Crimeware-as-a-Service; Cyber Scams and Cryptojacking.

"Cybercrime is constantly evolving. The COVID-19 pandemic has accelerated digital transformation, which has opened new opportunities for cybercriminals," said Craig Jones, INTERPOL's Director of Cybercrime.

INTERPOL

Cybersecurity for 5G: ENISA Releases Report on Security Controls in 3GPP

The European Union Agency for Cybersecurity (ENISA) provides authorities with technical guidance on the 5G Toolbox measure for security requirements in existing 5G standards.

the Agency released its Security in 5G Specifications Report about key security controls in the Third Generation Partnership Project (3GPP), the main body developing technical specifications for fifth generation of mobile telecommunications (5G) networks. As vendors, system integrators and operators build, deploy and manage 5G networks, the ENISA publication underlines the need for cybersecurity and for the national regulatory authorities in charge of cybersecurity policy development and implementation to have a good understanding of these controls.

This new ENISA report is directly driven by the objectives set in the EU toolbox for 5G security - mainly technical measure 'TM02'. This technical measure calls on the relevant authorities in EU Member States to ensure and evaluate the implementation of security measures in existing 5G standards (3GPP specifically) by operators and their suppliers.

The aim of the report is to help national and regulatory authorities to better understand the standardisation environment pertaining to 5G security, 3GPP security specifications and key security controls that operators must implement to secure 5G networks.

Cybersecurity challenges in the uptake of artificial intelligence in autonomous driving

A report by the JRC and the European Union Agency for Cybersecurity (ENISA) looks at cybersecurity risks connected to artificial intelligence (AI) in autonomous vehicles and provides recommendations for mitigating them.

By removing the most common cause of traffic accidents – the human driver – autonomous vehicles are expected to reduce traffic accidents and fatalities.

However, they may pose a completely different type of risk to drivers, passengers and pedestrians.

Autonomous vehicles use artificial intelligence systems, which employ machine-learning techniques to collect, analyse and transfer data, in order to make decisions that in conventional cars are taken by humans.

These systems, like all IT systems, are vulnerable to attacks that could compromise the proper functioning of the vehicle.

The report by the JRC and ENISA sheds light on the cybersecurity risks linked to the uptake of AI in autonomous cars, and provides recommendations to mitigate them.

CISA Releases New Gloabl Strategy for International Engagement

Brandon Wales, Acting Director of the Cybersecurity and Infrastructure Security Agency (CISA) announced the release of the agency's first-ever international strategy, CISA Global. During the fireside chat with BCIU President and CEO Peter Tichansky, Acting Director Wales shared how CISA will work with international partners to fulfill the agency's mission and create unity of effort across mission areas.

"Today's globally interconnected world presents a wide array of serious risks and threats to critical infrastructure," said Acting CISA Director Brandon Wales. "There are no borders to the cyber risks we face, and now – more than ever – we must work together. CISA Global describes how we will engage with international partners to build CISA's capacity and strengthen our ability to defend against cyber incidents, enhance the security and resilience of critical infrastructure, identify and address the most significant risks to critical functions, and provide seamless and secure emergency communications."

CISA Global outlines how CISA will leverage its global network to strengthen partner capacity and build a better, collective practice posture and response to urgent threats that are critical to U.S. national security interests. The strategy describes CISA's international vision and identifies four goals:

Advancing operational cooperation; Building partner capacity; Strengthening collaboration through stakeholder engagement and outreach; and Shaping the global policy ecosystem.

CISA is committed to promoting an open, interoperable, reliable and secure interconnected world within a global, operational and policy environment where network defenders and risk managers can collectively prevent and mitigate threats to critical infrastructure.

Sepura's SCG22 Mobile Radio Approved for Use on Airwave and BDBOS Networks

Sepura's SCG22 mobile radio has been approved for use by both Airwave and BDBOS for use on the UK and German public safety national networks.

The network approval enables UK and German public safety organisations – including police, fire and ambulance users – to deploy the SCG22 to their fleet vehicles, control rooms and associated critical communications functions.

Sepura has developed the SCG22 to meet the needs of demanding users looking for a tough and powerful TETRA mobile that can be deployed in cars, trucks, trains, boats, on motorcycles or in control rooms as part of solutions that support operations with intelligent automated features.

The SCG22 mobile complements the SC20 and SC21 hand-portable radios, by extending the same powerful connectivity and functionality to a mobile radio. Combining advanced connectivity through Wi-Fi and Bluetooth, the SC Series enable fast access to mission critical data, adding value to the solution.

In addition, the Wi-Fi connection supports the use of Over the Air Programming, enabling much quicker fleet programming and management, with much less impact on fleet administrators.

Sepura have made the process of upgrading to the new mobile radio as simple as possible, reducing the cost of deploying maintenance staff and taking vehicles out of service for extended periods. Many of the accessories and connecting cables from the SRG3900 can be reused, and the SCG22 fits the same mounting units.

Steadicopter expands the RUAV Black Eagle family into a comprehensive solution for homeland security, offshore and military missions

Steadicopter is expanding the applications for the Black Eagle family to include homeland security, police, offshore and military ISR missions. Exhibiting for the first time at the IDEX event, the company will highlight the capabilities of the lightweight unmanned robotic helicopter that enable it to meet the various challenges of HLS, military forces and law enforcement agencies.

The company has recently signed a number of cooperation agreements with Israeli companies with technological leadership, among them is Simplex – a leading developer of unique, groundbreaking drone control technology, enabling operations of multiple drones beyond visual line of sight (BVLOS).

The integration of FlightOps.io Drone Operating system, by Simplex-C2, with the Steadicopter, Black Eagle will enhance the platform's autonomous operational capabilities.

The FlightOps Drone OS is installed onboard the Black Eagle thus upgrades its autonomous capabilities turning it into a smart, mission aware robot that can operate in shared airspace, making smart autonomous decisions in real time and significantly increasing mission capabilities, efficiency and safety of flight.

This unique integration also allows the operation of multi-UAS in cooperation with other types of systems, sensors and unmanned aircrafts performing collaborative complex missions.

The FlightOps web-based Ground control application provides an easy yet powerful multi-mission and multi-UAS control using a single operator.

US DHS Publishes Free Resources to Protect Critical Infrastructure From GPS Spoofing

The US Department of Homeland Security (DHS) Science and Technology Directorate (S&T) announced today it has published the Positioning, Navigation, and Timing (PNT) Integrity Library and Epsilon Algorithm Suite to protect against Global Navigation Satellite System (GNSS) spoofing, or deceiving a Global Positioning System (GPS) device through false signals. These resources advance the design of PNT systems and increase resilience of critical infrastructure to PNT disruptions.

PNT services, such as GPS, are a national critical function that enable many applications within the critical infrastructure sectors.

However, "The increasing reliance on GPS for military, civil and commercial applications makes the system vulnerable," according to Space Policy Directive-7 (SPD-7), issued on January 15, 2021. "GPS users must plan for potential signal loss and take reasonable steps to verify or authenticate the integrity of the received GPS data and ranging signal, especially in applications where even small degradations can result in loss of life."

The PNT Integrity Library and Epsilon Algorithm Suite address this issue by providing users a method to verify the integrity of the received GPS data. "We are excited to release these resources to the PNT community to improve resiliency against potential GPS signal loss," said DHS S&T PNT Program Manager Brannan Villee.

"Since GPS signals can be jammed or spoofed, critical infrastructure systems should not be designed with the assumption that GPS data will always be available or will always be accurate," said Jim Platt, Chief of Strategic Defense Initiatives at the Cybersecurity and Information Security Agency (CISA) National Risk Management Center. "Application of these tools will provide increased security against GPS disruptions. However, DHS also recommends a holistic defense strategy that considers the integrity of the PNT data from its reception through its use in the supported system."

Smiths Detection's BioFlash shown to detect airborne COVID-19

Smiths Detection has reported that its BioFlash® Biological Identifier is capable of detecting SARS-CoV-2 in the air following tests conducted by the United States Army Medical Research Institute of Infectious Diseases (USAMRIID).

The tests were performed using live SARS-CoV-2 virus in a Biosafety Level 3 containment area at Fort Detrick, Maryland. The SARS-CoV-2 CANARY biosensor used in the BioFlash device demonstrated that it can quickly detect and identify the presence of low levels of aerosolized SARS-CoV-2.

The BioFlash® Biological Identifier is powered by CANARY® technology (a cell-based biosensor) and is combined with proprietary aerosol-collection techniques to provide rapid, sensitive and specific identification of biological-threat agents including viruses, toxins and bacteria.

"We are working incredibly hard to provide a tool that will support the ongoing fight against the coronavirus," said Roland Carter, President, Smiths Detection. "BioFlash is an effective and trusted environmental monitoring tool. These test results provide valuable data in understanding the spread of COVID-19 and help protect people in indoor environments such as hospitals, schools and commercial buildings."

USAMRIID confirmed that Smiths Detection's BioFlash can detect down to an estimated 6,000 airborne infectious particles of the SARS-CoV-2 virus within a controlled environment. This compares to as many as one million particles emitted in a single sneeze by a person infected with SARS-CoV-2. The test results also indicate no cross-reactivity with influenza and Middle East Respiratory Syndrome (MERS), an important consideration for environmental monitoring of the SARS-CoV-2 virus.

Further testing and research is underway at a number of US universities to collect more data on how the detection technology can help prevent outbreaks and guide both public and private organizations in COVID-19 mitigation strategies.

DroneShield announce a partnership with Trakka Systems, designed to better serve the C-UAS, ISR, inspection and UAS marketplaces

By streamlining the collective detection and situational awareness expertise of both businesses, the partnership has produced the TIPS-C (Trakka Interceptor Package Solution) product.

The TIPS-C, mounted on a mobile platform, provides a covert early detect and neutralizing counter-solution to the ever-present UAS hazard. Trakka's new partner DroneShield has provided the DroneSentry-C2™ Command and Control software platform, integrating a common operating picture for drone detection and tracking within the immediate airspace, as well as providing an extensive reporting suite. The TIPS-C utilizes and enhances Trakka's TrakkaCam and DroneShield's RadarZero™ sensors and DroneOptID™ optical AI/ML software, effectively combined to create an exceptional joint-capability drone detection and tracking system, with slew-to-cue camera operations for visual threat assessment and video evidence recording.

With each component seamlessly integrated, the TIPS-C is sophisticatedly capable in detecting, identifying, and automatically tracking drones of any size while dismissing moving objects. This one-of-a-kind capability all but eliminates the false positives that challenge other systems, saving valuable time amid imminent threats.

In January, executive teams from Trakka Systems and DroneShield met with the Tampa Police Department Special Operations Division's Chief Pilot and five members of the TPD Special Ops Groups, plus a Technical Liaison to the FBI, for the premiere demonstration of the TIPS-C at the Tampa Police Training Facility in Tampa, FL. The TIPS-C trial was a sweeping success.

This strategic partnership of Trakka Systems and DroneShield to create the TIPS-C aims to provide an expert suite of low risk, seamlessly integrated UAS detection and mapping solutions that are flexible, aware, reliable, and economical.

Camero-Tech launches XaverTM Long Range system - a portable, high-performance ISR through-wall imaging system for law enforcement and special forces

Camero-Tech is launching its groundbreaking XaverTM LR80 (XLR80) system, which enables detection of live objects behind walls, at distances of over 100 meters. This new capability provides a breakthrough operational advantage in a hostile environment.

Special forces and law enforcement teams conducting urban and rural operations require reliable information regarding hidden live objects to determine the most suitable approach to ensure successful missions and life-saving. Penetrating through walls from a remote location, the XLR80 creates an unprecedented, real-time situational awareness picture of whether there are people present beyond the wall, and if so, how many, their exact distance and their direction of movement. The system is also highly sensitive for detecting unseen micro movements of static live objects. Being able to achieve these capabilities and the high sensitivity, is a game changer in various operational scenarios.

Controlled by a tablet with a simple user interface for intuitive interpretation, the XLR80 features integrated data recording and playback for post-mission analysis, training and debriefing. A dedicate sight is used for accurately directing the narrow beam of the system to the target. The system can be operated by a single user and it is ready for use by a push of a button.

"For the first time, the operator in the field has the ability to see through walls at such long distance," says Amir Beeri, CEO of Camero. "We have developed unique technology on which the XLR80 system is based on. An innovative Ultra-Wideband (UWB) sensor supported by patented algorithms and signal processing, provides the user with real time situational awareness while staying safe at more than 100 meters away from the target."

MCTECH has successfully supplied anti-drone systems to a European country

MCTECH has successfully delivered the MC-Horizon 360D V3 systems. The MC-Horizon D360 V3 systems are tactical and reactive systems designed for protection against drone while in motion or during a hasty deployment. The systems were supplied to the country's anti-terrorism unit and will be used to secure convoys, strategic assets, and public events.

The MC-Horizon 360D V3 systems, developed and manufactured in MCTECH Laboratories, are reactive tactical systems that have been in operational use since 2014 by security forces throughout the world and have prevented dozens of attempts to use drones by terrorist groups in conflict zones or by illegal users.

Chaim Meirovich, the company's CEO, said that "the latest version of these systems is more advanced than ever and gives both system operators and mission commanders a real-time view of what is happening in the arena and zero-time decision-making capabilities. The systems can operate fully automatically to detect threats and to prevent the attack long before it occurs"," It is a great pride to take part in protecting the lives of civilians, soldiers and security forces as part of the ongoing fight against ongoing terrorism in the world. "

Rock West Solutions is launching its new APEX, a high-performance gamma detection and identification system

It is a high-performance gamma detection and identification system comprised of a handheld detector and accompanying analysis software. This device has 5-10x higher resolution than most traditional handheld detectors and is more affordable than comparable products on the market due to the incorporation of commercial-grade CZT crystals.

APEX captures gamma counts, assembles a full energy spectrum, and interfaces with a Windows laptop running the APEX analysis software. The APEX GUI displays the collected spectrum with user-friendly isotope identification tools. RWS uses commercial-grade CZT crystals with cutting-edge electronics designed to provide an economical, high-performance gamma detection and spectroscopy solution. Gamma resolution as low as 1.25% at 662 keV is achievable.

The APEX detector is modular, so expanding its CZT array to fit a specific project is easy and affordable. It can even be modified to meet MIL-STDs for shock, vibration, and EMI requirements. End use possibilities include portal or process area monitoring, man or vehicle mounting for first responders, or industrial or waste inspection. A larger gamma detection system measuring even a few square feet is now feasible and relatively low cost using the APEX detector technology.

RWS has developed proven calibration methods that ensure confidence and accuracy in gamma measurements over wide operating and storage temperature ranges.

"We are excited to present the new APEX product because we feel it provides such a game-changing solution to our customers' problems," said Don Pritchett, General Manager of Rock West Solutions. "In gamma detection and spectroscopy, resolution matters. Our lightweight and portable APEX detector, combined with our straightforward user interface for the associated laptop, will give first responders, US Government customers, and commercial industry a successful solution to the radiation detection problems they face."

World Security Report

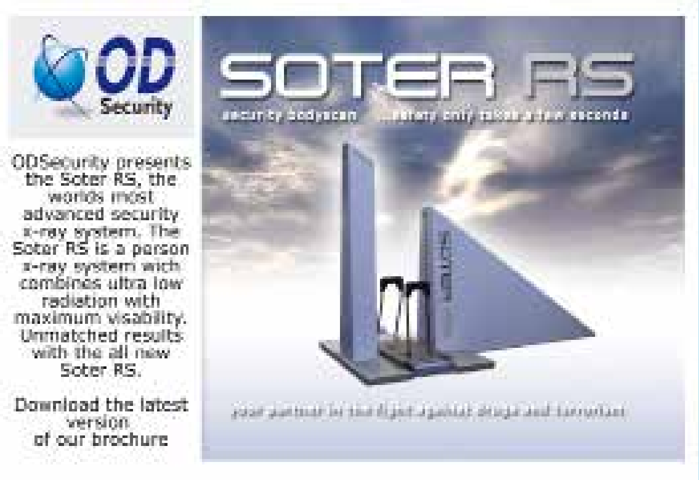
World Security Report is a bi-monthly electronic, fully accessible e-news service distributed to 100,000 organisations globally. It tracks the full range of problems and threats faced by today's governments, security and armed forces and civilian services and looks at how they are dealing with them. It aims to be a prime source of online information and analysis on security, counter-terrorism, international affairs and defence.

Clantect Ltd
Institute of Sound and Vibration Research
Southampton, SO17 1BJ, United Kingdom
Phone: +44 (0) 23 8055 0883
Email: info@clantect.com

www.clantect.com

Border Security Report

Border Security Report is the bi-monthly border management industry magazine delivering agency and industry news and developments, as well as more in-depth features and analysis to over 34,000 border agencies, agencies at the borders and industry professionals, policymakers and practitioners, worldwide.


OD Security
SOTER RS
security bodyscan ...safety only takes a few seconds
your partner in the fight against drugs and terrorism

ODSecurity presents the Soter RS, the worlds most advanced security x-ray system. The Soter RS is a person x-ray system wich combines ultra low radiation with maximum visability. Unmatched results with the all new Soter RS.

Download the latest version of our brochure

Wagtail International
leading specialists in detection dogs and dog handler training

Click here to view our profile

International Procurement Services (IPS)
Electronic Countermeasures Equipment
Sweep Teams
Training
IPS
www.SECURITYSEARCH.Co.Uk

March 2021

9-11
Security & Policing (Online)
London, UK
www.securityandpolicing.co.uk

10-12
Secon Korea
Goyang, Korea
www.seconexpo.com

15-17
Milipol Qatar
Doha, Qatar
www.milipolqatar.com

15-17
Intersec Saudi Arabia
Riyadh, Saudi Arabia
www.intersec-ksa.com/frankfurt/18/for-visitors/welcome.aspx

April 2021

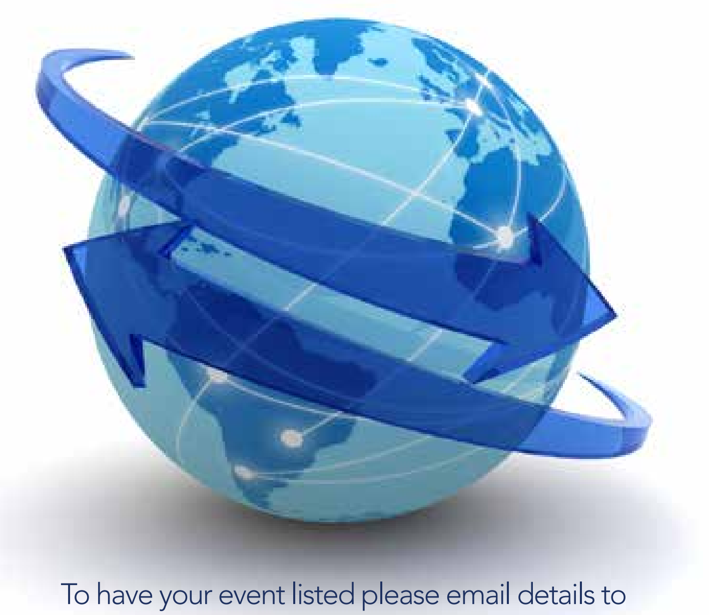
6-8
Milipol Asia
Singapore
www.milipolasiapacific.com

May 2021

11-13
Critical Infrastructure Protection & Resilience Europe
Bucharest, Romania
www.cipre-expo.com

June 2021

8-10
World Border Security Congress
Athens, Greece
www.world-border-congress.com



To have your event listed please email details to the editor tony.kingham@knmmedia.com

July 2021

12-14
IFSEC
London, UK
www.ifsecglobal.com

October 2021

19-21
Critical Infrastructure Protection & Resilience North America
New Orleans, LA, USA
www.ciprna-expo.com

ADVERTISING SALES

Paul Gloc
UK & ROW
E: paulg@torchmarketing.co.uk
T: +44 (0) 7786 270 820

Sam Most
Mainland Europe &Turkey
E: samm@torchmarketing.co.uk
T: +44 (0) 208 123 7909

Paul McPherson
Americas
E: paulm@torchmarketing.us
T: +1-240-463-1700