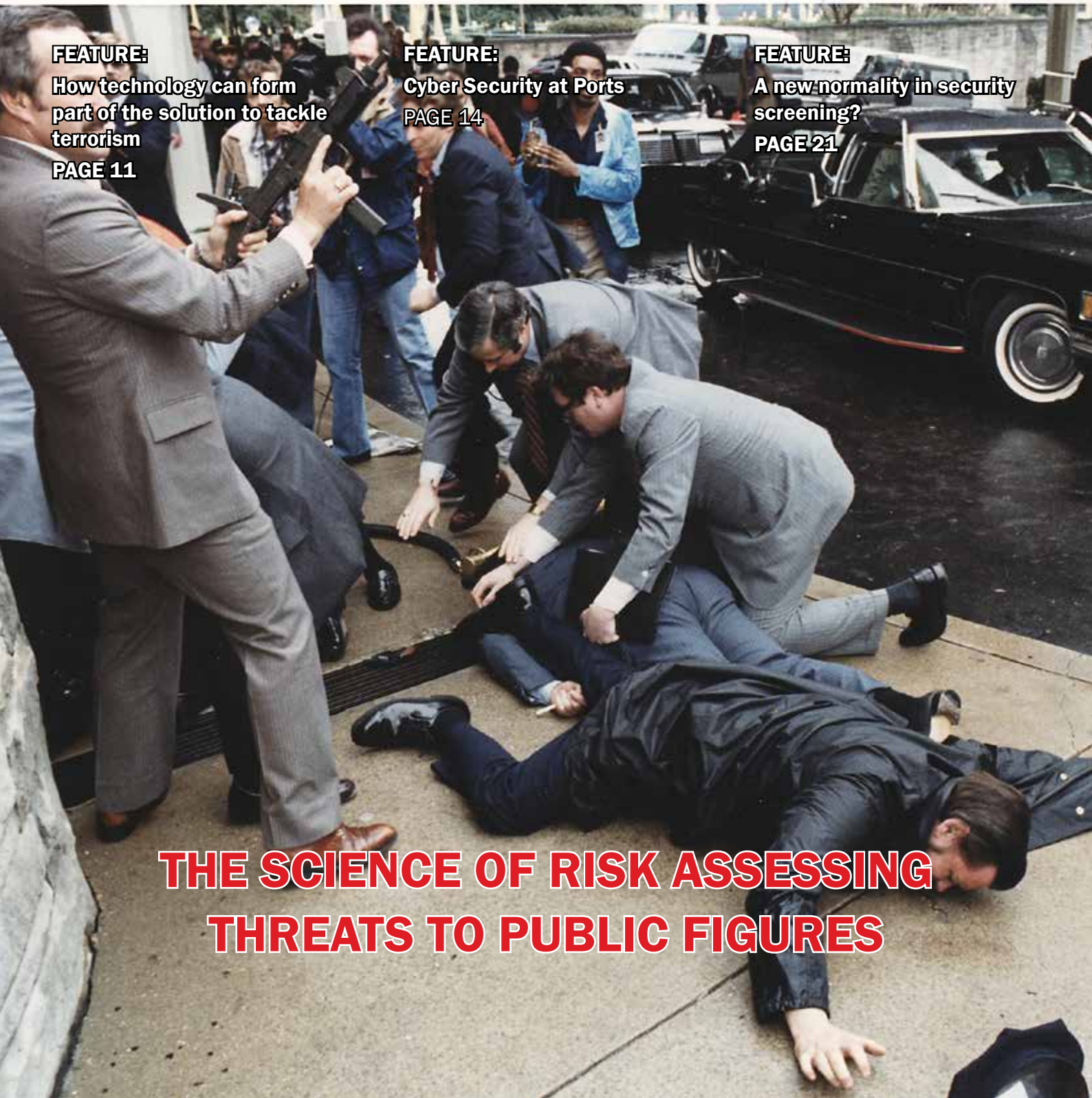
WORLD SECURITY REPORT

Official Magazine of

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

SUMMER 2020
www.worldsecurity-index.com



THE SCIENCE OF RISK ASSESSING THREATS TO PUBLIC FIGURES

critical infrastructure PROTECTION AND RESILIENCE EUROPE

6th-8th October 2020

Bucharest, Romania

www.cipre-expo.com

REGISTRATION NOW OPEN

Early Bird Rates currently apply - Register Today!

Securing the Inter-Connected Society

UN Member States need "to share information [...] to prevent, protect, mitigate, investigate, respond to and recover from damage from terrorist attacks on critical infrastructure facilities, including through joint training, and use or establishment of relevant communication or emergency warning networks."

The 7th Critical Infrastructure Protection and Resilience Europe brings together leading stakeholders from industry, operators, agencies and governments to debate and collaborate on securing Europe's critical infrastructure.

Register online today at www.cipre-expo.com/onlinereg.

To discuss sponsorship opportunities contact:

Paul Gloc
(UK and Rest of World)
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

Leading the debate for securing Europe's critical infrastructure

Owned & Organised by:

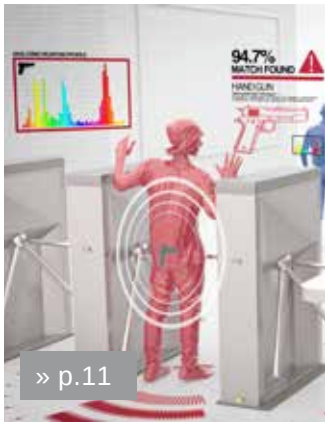
Supporting Organisations:

Media Partners:

CONTENTS

WORLD SECURITY REPORT

» p.7



» p.11


» p.14


» p.25

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 130,000 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.

THE NEXT PANDEMIC: HOW DO WE PROTECT, DETECT AND DELAY?

As we go to press the world is still struggling to cope with the coronavirus pandemic.

The US and Spanish death tolls had just passed that of China, at the time of writing, and the global death toll had passed sixty thousand and is set to keep climbing.

Where we end up, and, how long it takes to get things under control and back to 'normal' is yet to be determined!

But as those that can (bless them) continue to fight the good fight against the pandemic, the rest of us do the only thing we can do, which is to stay at home, and perhaps start thinking about and planning for the next pandemic. Because, unless the human race goes into a collective period of denial post-COVID-19, there will be a 'new normal'.

On Monday 23rd March, UN Secretary-General António Guterres urged warring parties across the world to lay down their weapons in support of the more significant battle against COVID-19: the common enemy that is now threatening all of humankind.

Even ISIL has issued a travel ban on their members.

Guterres was referring to COVID-19, but you could just as easily apply that statement to a yet unknown, unnamed pathogen that could kill millions and plunge the world in recession or depression in the future.

The human race should see COVID-19 as a stark warning of what a pathogen can do and come to realise that the next one could be something altogether more lethal and more devastating.

Throughout human history, pandemics have cut devastating swathes through human populations. Probably the most notorious of these being the Bubonic Plague or Black Death, which killed hundreds of millions over centuries.

But the development of modern medicines, especially antibiotics and vaccines has created a feeling, certainly, in the developed world, that modern medicine will fix all and that epidemics are things that only happen to people in far off places, and not to us.

But just in the last 102 years pathogens have killed; Spanish Flu 1918-19 - 40-50 million, Asian Flu 1957-58 - 1.1 million, Hong Kong Flu 1968-69 – 1 million.

READ THE FULL VERSION

The full version of World Security Report is available as a digital download at www.torchmarketing.co.uk/WSR

In more recent times we have seen SARS 2002-03 – 770, Swine Flu – 200 thousand, Ebola - 11.3 thousand and now COVID-19 - ?

So, these outbreaks should not be viewed as isolated events, but as naturally occurring phenomena that will happen again and again….and probably in the not too distant future. Pandemics have the potential to kill in unimaginably large numbers, but what COVID-19 has done is expose how little has been done to prepare for a pandemic and how little has been spent in developing technologies to help counter one.

By contrast, between 2017 and 2018, the total number of deaths as a result of terrorism was 15,952 (Global Terrorism Index) and falling but globally we have spent multi-millions and continue to do so, on developing and deploying technologies to counter that threat.

The good news is that much of this technology can be used to help to battle pandemics.

The Post COVID-19 World

It the post-pandemic period there will be much discussion and analysis of the various approaches taken by different governments around the world, and it should be relatively easy to identify what approaches worked well and what didn't.

This analysis should presumably be led by the World Health Organization (WHO) and lead to an agreed set of protocols being established and actioned worldwide as soon as a potential pandemic alert is given. The object will be to detect, contain and delay the spread of the virus until a vaccine is developed or the virus runs its course. It sounds easy when you say it like that!

It is too early to say which approach is best, the 'little by little, herd theory' approach of the UK and US or the 'early intervention' approach of Taiwan and other Asian countries such as Singapore and Hong Kong. But my money is on the Asian approach.

Taiwan started taking the temperatures of arriving passengers at airports almost as soon as the Chinese confirmed that the virus posed a threat, and all arrivals were required to self-isolate immediately for 14 days. Self-isolation was enforced by using the GPS on their mobile phones to ensure that they did not leave their isolation address and phoning them twice a day to confirm they were still there and had not just left their phone and gone out. They also did much good work tracing and imposing self-isolation on other people they may have been in contact with such as families, friends and colleagues.

Thanks to security spending, the first and most apparent technology we already have is thermal image cameras. They were quickly introduced to identify people with temperatures at airports, ports, offices, events, prisons - anywhere where there was a large mass of people. They are a quick, easy and remote way of determining whether somebody has a temperature and is, therefore, a potential virus carrier.

Germany's Dermalog, along with the Thai Immigration Authority, have gone one stage further. As part of a pilot scheme, they have integrated their new fever detection system into the biometric border control system at Don Mueang International Airport in Bangkok.

This pilot scheme has the obvious advantage of instantaneously alerting the authorities of any passenger who may pose a 'virus risk'. The authorities can then take immediate steps to mitigate that risk by instructing the individual to self-isolate or in more extreme circumstances, place them in immediate quarantine.

This technology can and should be integrated into new, and retrofitted or existing biometric border control systems. It can also be integrated into existing airport and port security screening systems, such as body scanners and metal detectors.

But border entry points are easy to control, and the technology helps only once the alarm has been raised.

What about passengers that arrived before the alarm was raised?

Once in country, arriving passengers disappear into the local population and it is difficult to track them down.

In the recent issue of BORDER SECURITY REPORT, it was outlined how the Passenger Name Record (PNR) system could be used to trace the movements of recently arrived passengers. PNR is a requirement of the computer reservation system and shares part of a passenger's itinerary between travel agencies and airlines. There is currently no industry-wide standard for the layout and content of PNR, nor has it been universally adopted. But if PNR (or something similar) were to be mandated worldwide, with the inclusion of a contact mobile phone number and the intended address/s for the first ten days of any trip. It would allow the authorities the option to phone or send an alert to the passenger initially directing them to take appropriate action or, if necessary, they could send officials to the listed address or track the individual using their mobile GPS.

The mobile phone GPS can then be used to ensure the individual is following self-isolation directives, as in Taiwan.

Combined with their biometric passport, facial recognition software that is increasingly used on local CCTV systems,

could also prove invaluable in tracking down individuals who are possible carriers of the virus. Of course, this would require immigration and border authorities being able to capture and store the data of passengers for a time of, say, ten to fourteen days.

The next problem is tracking down any people that the passenger may have inadvertently infected.

Again, once the authorities have tracked down the passenger, mobile phones may provide a big part of the answer. Mobile phone forensic companies like Basis Tech (UK), Cellebrite (Israel) and MSAB (Sweden) provide incredibly powerful tools in tracing their network of connections. Mobile forensic systems can provide details of where they have been, who they have been calling, and who they are in contact with on social media etc.

Chris Brown of Basis Technology said, "Together with our partners, we have developed a COVID-19 Tracking and Monitoring solution. This solution utilises existing ad-tech technology to remotely provide location history, and future tracking of infected people, which is a game-changer in preventing onward infections and saving lives. The solution is mobile operator independent with no need to download an app. The solution is also GDPR compliant as no personally identifiable data is used. "

The good thing is that most of the systems and technologies already exist and several countries are showing the way when it comes to using data and technology to defeat this virus and the next one.

There would be grave concerns from some quarters about privacy, data protection and foreign governments holding information on visitors for any period, no matter how short a period it may be.

There may also be some cultural differences in our acceptance of such measures, especially in the western democracies.

But the reality is that most of the information needed to track and delay the spread of any new virus we already share routinely, via our online bookings, travel agents, trusted traveller schemes, visa applications and landing cards.

Agreeing on a global system based on one of the widely accepted existing systems would seem an obvious solution.

And using the technology we already have to locate potential carriers together with anybody they may have come into contact with just makes sense.

There has been much talk about being at war with the virus. Governments and countries are on a war footing, with draconian restrictions on civilian populations and economies and manufacturing being redirected to fight the spread of the virus.

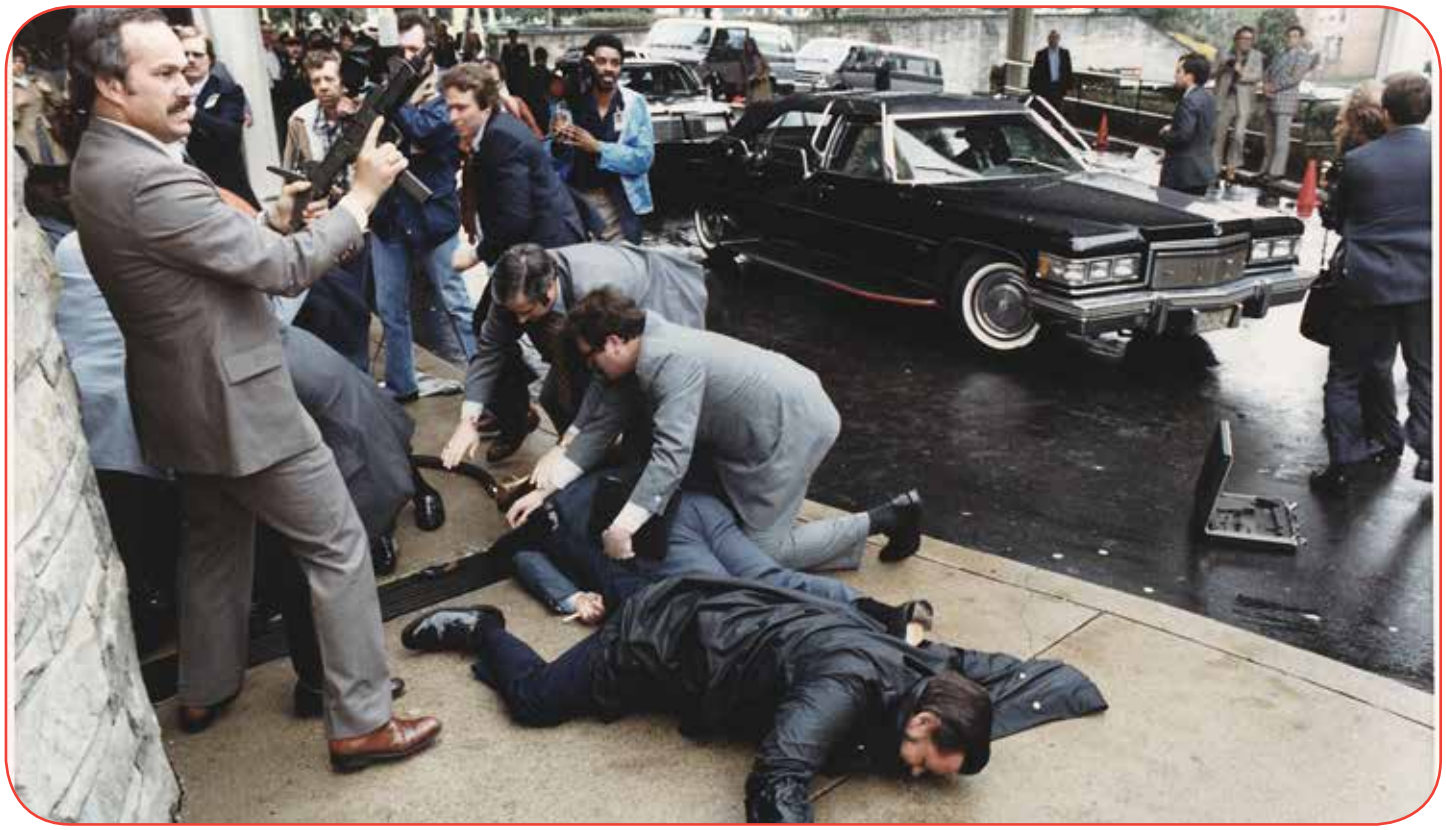
It is vital that we see the pandemic threat very much in that context, of being at war, and that temporary restrictions of some rights and privacy in times of crisis is very much in our self-interest.

It is vital that the lessons of COVID-19 are not forgotten, and we are better prepared for the next pandemic, because there will be a next pandemic!

Tony Kingham

Editor

The Science of Risk Assessing Threats to Public Figures



Secret Service agents cover Press Secretary James Brady and police officer Thomas Delahanty during the assassination attempt of Reagan.

Threat assessments and the subject of targeted violence date back to the 19th Century France and Italy where the work of Laschi & Lombroso was well known and suggested that criminals could be identified based on physical defects. More recently, research has been directed by issues of mental disorder and driven by those from the world of psychiatry and psychology.

This changed in the late 1990s when Fein and Vossekuil were tasked by the US Secret Service to research all assignations and attempts, to ascertain what could be learnt from them and how this might change their operational approach. This project, which is now widely known as the Exceptional Case Study Project (ECSP) started considering targeted attacks, a term created by them, from a security rather than a mental health perspective.

When tasked with assessing the threat that an individual may pose, it is not unusual for investigators to utilise Open Source research. The question is; what is it that you are looking for? Previous criminal history? Association with groups of interest? All very useful, but do they tell you the whole story and could you be missing vital information, information that might enable a more forensic assessment?

Methodology introduced by Philip Grindell MSc Msyl to aid the investigation of abuse targeted at


Image by Garry Knight

British politicians and now used by Defuse Global, a specialist consultancy he launched to assess threats against public figures, suggests that a more forensic approach is possible.

Hunter or Howler?

One of the key aspects is the understanding that those who make threats do not necessarily pose them. In essence, this involves identifying whether the threats are emanating from a 'Hunter' or a 'Howler'. These terms were originally devised by Calhoun & Weston and supported the findings of the ECSP where they found that none of the attackers studied communicated a direct threat to the target directly or to law enforcement.

This suggests that attention should be focused on those who pose a threat, whether or not they have made a threat. This finding is supported by the study into the role of mental disorder in attacks on European politicians between 1990-2004 where they could find no evidence that the person targeted was subject to a direct threat. Human behaviour is more complicated and it would be risky for a security manager to assume this theory as always true as a person of concern who threatens can also attack and the others argued that those who breached the security were more likely to be a threat than those who simply approached. However, it is appropriate to take the view that those that threaten are often 'Howlers' and have no intention to attack. Logic suggests that someone intending to attack is unlikely to give prior notice.

'Hunters' on the other hand are predators, who may leak indicators that they are in pre-attack planning mode. Predatory behavior, once necessary for survival, is now used to satisfy other needs such as to achieve notoriety, wealth, dominance and revenge. Very often the predator will express a complete lack of any emotion during the attack. Developing from the theory of 'Hunters', it is argued that this can be explained by two differing types of violence that separate those who attack a politician as opposed to those who engage in 'everyday' violence.

Affective or Predatory Violence?

Termed as either Affective or Predatory violence, one highly emotional and the other cold and calculated, they have very different purposes. Affective violence is highly emotional, with a sense of arousal, anger or fear. This is 'everyday' violence seen in street fights, domestic violence and gang murders. Predatory violence is not preceded by emotion. In fact, it is the lack of arousal and emotion and the presence of cognitive planning that separate it from the everyday violence we are all too familiar with. The purpose of affective violence is to defend oneself against a perceived threat.

There is a growing body of evidence that psychopaths are more likely to engage in predator violence. This can be seen in stalkers. Intimate stalkers who turn violent threaten their victims and when they attack are often impulsive, choking, pushing, punching and pulling hair. Public figure stalkers plan their attack, rarely threaten and often use weapons.

The theory of pre-attack warning behaviors is a key element of Defuse Global's assessment. The term 'warning behaviors' was used to suggest that the subject had changed their behaviour and was on a period of acceleration towards the attack. They do not predict who is going to attack, but are usually are based on facts, dynamic, acute, and often indicate an acceleration.

Seven Warning Behaviours

They can be useful to help threat assessors manage low frequency intentional acts of violence towards an identified target. In the previously referred to research into attacks on European politicians, 46% showed signs of the warning behaviors before their attacks. The assessment looks at seven warning behaviours. It doesn't suggest that they all will or need to be present, but clearly the greater the cluster, the greater the threat:

1. Pathway to violence: This is described as the period in which the subject researches and plans the attack. This path, often initiated by a grievance, real or perceived, then leads them on to the idea that violence is the only way to resolve this issue and from there they start to research and plan the attack. This grievance can be either personal or ideological. The subject can move along the model escalating or de-escalating the threat depending on a number of variables.

Once a grievance has occurred and the subject had decided that violence is the answer, it follows that they will then start to research and plan what to do next. In the ECSP they found that 67% of the subjects had a grievance at the time of the incident and more than 80% who had a grievance blamed their target for it. However, they also stated that the attacker often considered more than one target before deciding who to attack.

2. Fixation warning behaviour: This is described as an increased pathological preoccupation with either a person or an ideology or cause. Fixation can be a normal part of life, such as the emotion of loving, however when that fixation then consumes your every waking moment and becomes obsessive, it becomes pathological and is often linked to stalking behavior. From a security perspective this can be difficult to identify, however an unnatural volume of interest may be an indicator. One of the risks attached to such fixation is the need for close proximity and when this is frustrated it can metamorphise into strong emotions of anger and emotionally hijacks their lives. Research conducted into attacks on British politicians this century indicated that the fixation in each case was on a cause or ideology rather than the individual. Thomas Mair, the killer of Jo Cox MP, was fixated on extreme right-wing ideology and the idea that immigrants were taking over.

3. Identification warning behaviour: This is described as behaviour that suggests a psychological desire to be a 'pseudo-commando'. This is often associated with those who consider themselves to be 'soldiers' of a cause and dress up in military style outfits. A good example of this is Anders Behring Breivik who dressed up in military uniforms, identified himself as a Commander in the Knights Templar and considered that he was fighting a cause. The research suggests the subjects who demonstrate this behaviour have emotions of anger and resentment. Another sign of this behaviour is the association and research into the actions of other attackers. The subject will have researched other attacks and seek to link himself to that attack or gain confidence. from

4. Novel Aggression warning behaviour: This is best described an act of violence or aggressive behaviour in which the subject is testing their ability to act in such a way. It is usually unrelated to the 'pathway' on which they are travelling and can be totally out of character. The act may be completely unrelated to what they intend on doing and property crimes may be an indication. In October 2014, Michael Zehaf-Bibeau murdered Corporal Nathan Cirillo, a Canadian soldier, and injured three others. Three years earlier, in December 2011, he had walked into the Royal Canadian Mounted Police (RCMP) field office in Burnaby, British Columbia, and said he wanted to be arrested for an armed robbery he committed a decade earlier; no such recorded crime existed. The next night, he tried to rob a McDonald's restaurant with a pencil, then

waited for the police to arrive.

5. Energy Burst warning behaviour: This is a key indicator that the intention is escalating and can occur in the hours, days or weeks before the actual event. It is characterised by an increase in pre-attack activity and can be signs of final preparations, purchasing equipment or conducting hostile reconnaissance or internet activity. In May 2010 Roshonara Choudhry, having radicalised herself online, dropped out university and made an appointment to see her local Member of Parliament, Stephen Timms. She then quickly paid off her student loan and closed her account before buying knives on her way to attending his office where she attempted to kill him. This all happened in a matter of days before the attack.

6. Leakage Warning behaviour: This is where the subject communicated their intention to a third party. This can be done in person, online, in a journal or letters. A recent example of this is Jack Renshaw who told his associates that he was planning to murder someone: Rosie Cooper, his local Member of Parliament. A member of his group subsequently informed on him. There are number of theories as to why someone might 'leak' intent of an attack. These motivations could vary from the need for excitement, a sense of accumulating power, a desire to frighten or intimidate, seeking of attention, or fear and anxiety concerning the impending act. Recently, we have increasingly seen attackers publishing their 'manifesto'. This perhaps suggests that they want to be remembered or associated with the attack in the contemplation of their arrest or death.

7. Last resort warning behaviour: This behaviour is evidenced by language of no hope. It suggests that the subject sees no alternative, and nothing left to live for. It is an indication of a view that there is no alternative other than violence and seeks to justify the action. It can also be witnessed by reckless behaviours which show no concern for future consequences. This behaviour was evidenced by the Westminster attacker five days before the attack in a "goodbye visit" he visited his mother as he [Masood] was leaving the house, he turned over his shoulder and said: 'They'll say I'm a terrorist, I'm not'.

When a threat is received, these steps, when taken together can provide a forensic basis on which it can be assessed, increase accuracy and provide those tasked with providing a detailed rationale for their decision making. It is worth noting that any assessment is just that, an assessment and no model can prove unequivocally that no threat exists.

Defuse Global is a consultancy whose clients include public figures and those who have a high profile, many of whom receive communication that is threatening, abusive or intimidating. Prior to launching Defuse Global, its founder, Philip Grindell was brought into Parliament following the murder of the politician Jo Cox, and to set up and run the team tasked with stopping the next attack whilst investigating the abuse, threats and intimidation directed at British politicians. Having researched threats assessments and relevant research and tested many within Parliament, Defuse Global formulated their forensic assessment of threats, which forms part of `The SAFER Model'.

Philip Grindell MSc MSyI is a member of Association of Threat Assessment Professionals (ATAP), is qualified in Stalking Risk Profile, a member of ASIS and a member of The Security Institute. In addition, he is a trained Counter Terrorist Security Co-Ordinator. The former Scotland Yard detective is founder and CEO of Defuse Global:www.defuseglobal.com or @Defuseglobal on Twitter/ Instagram.

How technology can form part of the solution to tackle terrorism

Today's terror landscape is more fluid and complex than ever. International terrorism remains a serious threat and the threat of domestic terrorism remains persistent overall, with actors committing crimes in the name of violent agendas. It cannot be denied that police and intelligence services are doing their utmost to protect society against the omnipresent threat of a physical attack. But it may not be enough on its own to counter and thwart terrorist attacks.

Whilst there is not a consistent view of what is driving knife crime across the UK, most will agree that the causes are nuanced, and that one single approach on its own, is unlikely to provide a solution to this growing issue. The situation therefore demands a new, more holistic security response that is proactive, adaptable and dynamic.

The evolving threat of terrorism

The nature of terrorist threats have evolved, moving away from large-group conspiracies towards lone operator attacks, which have become more common over recent years with the rate of serious knife crime offences rising sharply in some areas outside London. These lone or small group attackers have often been radicalised online, where they are urged to carry out impulsive acts of violence. Without a clear group affiliation or guidance from a higher power, lone offenders are a lot harder for security

services to stop. The lone assailant has, for many observers, come to represent one of the most urgent security threats facing the UK.

Due to their low-tech nature, these terror attacks carried out by lone operators are incredibly challenging for law enforcement and counter terrorism experts to identify and intercept. The reduced need for advanced planning adds a degree of volatile spontaneity that makes these attacks incredibly dangerous. By comparison, when a number of individuals collaborate to orchestrate a larger scale, more organised attack, they are far more likely to leave communication trails that law enforcement authorities can detect and intercept before the worst happens.

There has been a growing frequency of lone attacks involving a knife or sharp instrument in recent years, across the streets of the UK. A recent report launched by the Youth Select Committee, 'Our Generation's Epidemic: Knife Crime' revealed the number of fatal stabbings in the year ending March 2018 in England and Wales was the highest on record since data collection began in 1946. There were 285 killings by a knife or sharp instrument in the 12 months ending March 2018, Office for National Statistics analysis shows. As knife threats k evolve and become harder to detect, a new solution is urgently needed to make public spaces as secure as possible to help mitigate an attack. Fortunately, technology can be incorporated as part of the solution in identifying weapons before they are used.

Today's security measures

The UK relies heavily on camera surveillance as a way of monitoring criminal activity. While CCTV has gained prominence as an effective way to acquire valuable intelligence in the aftermath of attacks, through the identification of suspects. Real-time interventions are however limited as behavior is only understood as suspicious after the event has occurred. It is a largely retrospective measure that does little to prevent attacks ahead of time.

There is a fundamental lack of systems in place that can detect a concealed or visible weapon or other active threat ahead of time. Instead, police are called to the scene after an attack has occured and are then reliant on the accounts of eyewitnesses or CCTV to identify and catch the assailant.

The constantly changing face of terrorism and transnational organised crime methodologies have made public spaces look at new methods and solutions to tackle these security challenges. The key to preventing future attacks therefore lies in proactive, rather than reactive measures.

This is where new, innovative technologies can be deployed to complement existing systems, thus bolstering on the ground security to create stronger defences. These new technologies allow for force multipliers with existing security staff. By integrating existing CCTV with AI-driven/computer vision object recognition software, visible threats, such as guns or knives, can be detected moments before an attack is carried out. Security and law enforcement can then be alerted in real-time of the location and nature of the incident, so that action can be taken immediately.

The future of technology

In addition, there are other AI-driven technologies that can be covertly deployed across a range of environments to protect the citizenry. These AI technologies takes multiple different forms depending on the environment it is trying to protect.

For example, and as highlighted earlier, video systems enhanced by AI-powered object recognition software can be deployed to identify and flag forbidden objects in a wide range of public spaces. These include schools, hospitals, sport stadiums, event venues and transport, so that threat objects or suspicious behaviours can be identified and flagged instantaneously.

Targeted magnetic sensors, concealed in everyday objects like planter, scan individuals and bags for catalogued threat items and large mass casualty threat objects. With this advanced magnetic solution, it becomes possible to discover a knife or weapon on a person body before it appears in their hand, allowing for immediate notification for onsite security. The hidden technology empowers security staff to intercept threats before they evolve into a wider scale attack.

Either video object recognition or smart metal detection, the benefit

of using data-driven algorithms to identify threat objects is that it removes human bias in identifying suspicious individuals. AI-enabled technologies can be completely objective in a way that is innately difficult. The benefits of this should come as a welcome relief for today's law enforcement who face constant scrutiny for profiling.

Furthermore, by combining these covertly deployed technologies today's security can be alerted for both hidden and visible weapons without the need for invasive measures, such as stop and search procedures which disproportionately target the minority.

Implementing a proactive security model is the most effective way to safeguard the public without causing a mass obstruction and disruption, and new AI-driven technologies can aid in this effort.

By Martin Cronin, CEO, Patriot One

Italian Critical Infrastructure Secretariat's guidance for the continuity of critical infrastructures during the COVID-19 pandemic

It is a fact that Italy is one of the countries that has been most severely hit by the spreading of the COVID-19. Such condition has triggered an unprecedented response by all of the governmental offices and public authorities with the aim of reducing the diffusion of the virus, guaranteeing public health and supporting the continuity of critical infrastructures. Starting from the 11th of March 2020 and onwards, the Italian Government has called for a lock-down which has begun from the Lombardy region and has later been progressively extended to the entire territory of the Country.

At the moment this article is written, Italy is still in a complete lock-down, due to the need to contain the spread of the virus and reduce the pressure on the healthcare system, which is overwhelmed because of the large number of affected citizens that require intensive care or similar treatments.

In this context, an important role in keeping the Country up and running, is the one of critical infrastructures and essential services. During these challenging times, in fact, the role of critical infrastructures is even more important, since the Country, more than ever, needs stable services. With all of the forces

focused on the containment of the virus, it is a basic requirement that critical infrastructures need to ensure stability, since any failure or accident and the potential consequences across the interdependency-chain, can lead to further complications. The loss of service needs to be avoided at all costs, the more if considering that cyber-attacks have improved, as attackers are willing to exploit and take advantage of the current situation and of the citizens' feelings of vulnerability and uncertainty (circumstance that makes them an easy target for social engineering and other attacking techniques).

Even though "prevention" is not a new item on the agenda, both at national and European level, the pandemic scenario has found the modern society partially unprepared and lessons have mainly been drawn from experiences of those countries that have been first in line in the fight against COVID-19. At the same time, it's necessary to point out that the pandemic threat wasn't among the ones properly addressed by critical infrastructures' business continuity plans, in consideration of the fact that they were surely recognized as high impact events, but with a low probability occurrence. Such perception of the phenomenon has led to light or nonexistent prevention mechanisms which have then resulted in a lack of measures or alternative plans in the following areas:

- HR continuity and resilience (e.g. no people scenarios – segregation of personnel);
- availability of protection supplies, such as masks and suits for employees engaged in critical tasks (e.g. oversight of control rooms) or on field duties (e.g. maintenance);
- difficulties in the execution of planned/extraordinary maintenance to machinery and plants, due to the two points above and also in case of reliance on foreign suppliers which have encountered limitations in the movement of qualified personnel and/or in the shipment of goods, because of the lock-downs and the consequent shortage of certain supplies.

The infrastructure operators in the subsectors of electricity and gas transmission, including bigger multi-utilities, which have more structured and proactive approaches in the areas of prevention and preparedness (since they're even more vital in such extraordinary conditions), have had to stress their adaptation capabilities, in order to face the challenges posed by the pandemics to the continuity of their business. Their efforts have led to the preliminary exploration of potential ways to tackle most common issues, since they often had a solid base in their business continuity plans that could be partially repurposed to address new challenges posed by COVID-19.

Given the need to provide very direct and promptly implementable measures to all of the critical infrastructures and the SMEs that belong to their supply chain constellation, the Critical Infrastructure Secretariat of the Presidency of the Council of Ministries , on the 26th of March 2020, has released a set of guiding principles in order to ensure the continuity of critical services which are of public interest.

The released guidance provides recommendations to the operators of critical infrastructures for the "containment and fight against the spreading of the virus, while ensuring the continuity of essential services, the infrastructures' operation and the safety of the workforce".

The guidance can be summarized as follows:

- operators are invited to sanitize the premises, tools and workstations which are daily used for the business and operations of CIs and such operation should be repeated at every turnover;
- anti-contagion equipment to be distributed to employees that cannot operate in smart working;

- for all the personnel that can operate in remote working, the adoption of all of the measures for ensuring a good level of cybersecurity, including the provision of a specific guidance for smart workers;
- the review of the operational plans, so to minimize the physical presence of employees, including the execution of maintenance which should be limited to tasks that cannot be postponed;
- for those employees whose duties require the physical presence on premise, organize the teams and their turnover by including the minimum number of people who have to operate wearing all safety equipment. On this point, the guidance suggests the teams to always rely on the same pool of employees, in order to reduce the risk of cross-contagion.

Apart from these horizontal recommendations, the guidance also provides two specific measures to be applied to "control rooms" and "essential maintenance".

On these matters, the guidance recalls the need to apply measures that should be as close as possible to "zero-tolerance", in order to avoid that personnel operating in control rooms is exposed to the risk of contagion. For this reason, the guidance suggests the adoption of a voluntary segregation, which entails that one team is hosted in a temporary accommodation for at least 14 days, with a complete limitation of all social contacts for such period; while the second one observes the same measures from home. In the cases when the voluntary segregation is not a viable option, the guidance suggests the use of different premises, in order to avoid social contacts among the teams that are in charge of the control rooms (e.g. using the disaster recovery sites), including the enforcement of the previously described horizontal measures regarding the reiterated sanitization and the adoption of safety equipment.

In regards of the "necessary maintenance for ensuring the continuous operation of essential services", the guidance stresses again the need to adopt smart working and in all the cases this is not feasible, to provide technicians engaged on field with the necessary safety equipment and allow them to reach the sites, where the maintenance has to be performed, directly from their homes, avoiding unneeded physical presence in headquarters or operation premises.

Finally, the guidance draws the attention to the need to prepare lists of active and quiescent personnel, including personnel available in external contractors, that have cross-capabilities (e.g. control room operation and maintenance), in order to call them in service to substitute qualified staff that is temporarily unavailable for any reason.

For the purpose of the efficient handling of the COVID-19 crisis, the Secretariat has provided operators with an institutional email address in order to receive updates "from the field" and also prompt reporting of disruptions or difficulties that operators may face in these challenging conditions, so to activate all sort of support.

As said, even though business continuity methodologies and plans are usually well known and implemented in critical infrastructures, the release of this guidance, which have been released in similar format from other governments worldwide, provides an important support to operators that haven't properly considered the pandemic scenario, so to trigger their prompt, efficient and harmonized response.

In these very delicate circumstances, while the crisis is still ongoing, it's maybe too early to draw comprehensive lessons learned on the evolution of the Covid-19 phenomenon. In a later stage, when the "wartime" will be over, further lessons will be drawn, not only in the dimension of pandemic scenarios in the context of critical infrastructures, but also in the domain of hybrid threats. In addition to the challenges posed by the COVID-19, in fact, many countries have experienced all sort of ever-growing cyber-attacks, together with an increasing spreading of fake news which have led to disruptions and contributed to social unrest and unjustified panic. These last arguments confirm the need to keep addressing the matter of CIPR with a multidisciplinary and harmonized approach, circumstance that in the EU will have an impact on the ongoing negotiations of the next phase of the European Programme for Critical Infrastructure Protection (EPCIP), including the new European Critical Infrastructure Directive that should be promulgated as part of the programme.

By Alessandro Lazari – Director for the Mediterranean Region – IACIPP

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.

Registration Today

and save with Early Bird Rates

All Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and security of their respective internal critical infrastructure that supports primary mission essential functions. Such infrastructure need to be addressed in the plans and executed to the requirements of the National Continuity Policy.

Join us in New Orleans, LA for the premier event for operator/owners of CI, government establishments and agencies and the CI industry tasked with the regions Critical Infrastructure Protection and Resilience.

The conference will look at developing on the theme of previous events in helping to create better understanding of the issues and the threats, to help facilitate the work to develop frameworks, good risk management, strategic planning and implementation.

For more information and online registration visit www.ciprna-expo.com

The premier discussion for securing America's critical infrastructure

Confirmed speakers include:

- ***Keynote Speaker:*** Brian Harrell, Assistant Secretary for Infrastructure Protection, US Department of Homeland Security (DHS)
- Leslie Millet, Safety Agency Risk Manager / FSO Workgroup Chairman, Port of South Louisiana & Infragard Louisiana President
- Harrison Andrew Pierce, Head of Operational Compliance and Security, Aerial Systems, San Diego Homeland Security Office
- Dr. Christopher Rodriguez, Director of Homeland Security and Emergency Management for the city of Washington, DC, USA
- Stephanie Murphy, Assistant Vice President, Resiliency and Critical Infrastructure Programs, Tidal Basin Government Consulting
- Jeff Gaynor, President, American Resilience
- Sam Cohen, Cybersecurity Consultant – Risk Group, Deloitte Canada
- Alessandro Lazari, Regional Director – Mediterranean, International Association of CIP Professionals & KPMG Advisory, Italy
- Steve Povolny, Head of Advanced Threat Research, McAfee
- Tim Klett, Cybersecurity Researcher, Idaho National Laboratory
- Frédéric Petit, Principal Infrastructure Analyst, Argonne National Laboratory
- Ben Eazzetta, CEO , ARES Security Corporation

For speaker line-up visit www.ciprna-expo.com

Supporting Organisations:

Media Partners:

Cyber Security at Ports

For years, ports have been undergoing a digital transformation, due to the ever emerging challenges brought about by the optimisation of existing processes and the introduction of many new capabilities. Digital transformation is pushing the maritime industry beyond its traditional limits to provide opportunities and to improve productivity, efficiency and sustainability.

Such digital transformation has come about from the advancements in the interconnectivity of IT and the introduction of cloud computing, big data and Internet of Things (IoT). However, for ports, transitioning with the digital transformation brings along cyber security challenges that need to be met in order for future ports to fully unlock the potential of these new technologies. As a result, ports have discovered that there is a price to pay for modern technological marvels. Cyber criminals are attracted to the centralised systems which ports have that provide fraudsters with a wealth of target information.

The need for increased cyber security in ports is evident by the proliferation of cybersecurity incidents that have occured in ports over the past few years. For example: in 2011, the Belgian port

of Antwerp experienced a cyber attack by where drug traffickers recruited hackers to breach IT systems to control the movement and location of containers in order to intercept and smuggle drugs. This particular cyber attack was regarded as a multi stage attack as it occured over a period of 2 years. Furthermore, Maersk experienced a NotPetya ransomware attack which infected 50,000 endpoints and thousands of applications and servers across 600 sites in 130 countries. During the 2019 Association of Bulk Terminal Operator's annual conference, Ian Adam, chief executive said: "both physical and cyber security remain to be a particularly weak spot for the ship to shore interface," further highlighting the need for stronger cyber security for ports.

Increasingly, ports are seen as key targets for those who are looking to disrupt national infrastructure and hostile governments. Many insiders have viewed ports as being underprepared for the likes of these cyber threats, even though major players in the industry have recognised and acted on the risks posed by cyber threats. However, the majority of the major players have been very slow to recognise the need for cyber security. There are a number of key reasons and challenges ports face as to why there are lacking effective cyber security.

1. Lack of digital culture in ports, some stakeholders are still very conservative. Traditional stakeholders do not consider cyber security to be a priority over technology adoption.
2. Lack of awareness and training regarding cyber security
3. Lack of an understanding of what time and budget should be allocated to cybersecurity
4. Lack of qualified IT and OT human resources regarding security matters, skills shortage.
5. The ability to find a balance between business efficiency, digital transformation and cyber security.
6. Difficult to stay up to date with the latest cyber threats and therefore lack of cyber security against these
7. The convergence and interconnection of OT and IT systems, greatly exposes OT systems to higher risks.
8. Supply chain challenges: the lack of control over the cyber security level of suppliers presents cyber security challenges for ports.
9. Strong interdependencies between port systems and external services from other sectors (such as energy) that introduce interdependency cyber security risks.
10. New cyber risks resulting from digital transformation of ports.

It is important that cybersecurity becomes a top priority for ports, in order to ensure the safety, security, compliance and commercial competitiveness, while also ensuring they have the full capabilities for a digital transformation. Port operation is very complex because of the nature of the services provided, the number of processes taking place in the infrastructure and the large number of workers involved in the operation, which includes land, sea and economic activities, so there are many reasons for cyber security. With all the new and modern systems and equipment, ports are exposing themselves more to the risk of cyber attacks.

Ports can be found vulnerable to a number of types of cyber attacks due to the vast quantities of data that is stored and transmitted in port infrastructure, this is a key attraction for cyber criminals. Due to the automated navigation, logistics systems and ports fleet management software, all are presented as being a rich source for criminal activity. It is more and more evident that the incorporation of digital tools in the day to day activities of ports has not removed the threat of crime, but rather shifted criminals focus to digitally enabled activities. There are a number of cyber attacks ports can potentially face:

- The theft of sensitive and

critical port data, such as: location of content of containers or competitive know-how, along with the ability to delete and alter such data.

• Hackers can intercept the communications between the port and different stakeholders, also referred to as 'man in the middle attack' that relays and alters communications between 2 parties who believe they are directly communicating with each other.

• The scanning of port systems to intercept data for corporate or state espionage or criminal crime and privacy espionage.

• Session hijacking- the exploitation of system vulnerabilities to gain the same access rights than the targeted clients (such as authentication cookies).

• Network reconnaissance and traffic manipulation- an attack scans the network until he finds an entry door which reveals internal port network information, to therefore compromise the targeted systems.

• The use of phishing attacks to compromise networks with inadequate security.

• The illegal smuggling of people and drugs due to organised crimes viewing ports as a nexus point for smuggling

• The ability to shut down the entire port by compromising port systems

• Other examples of cyber crime on ports is: fraud, sabotage, vandalism, theft, unauthorised access, terrorism and corruption,

Therefore, there is an increased call for cyber security at ports due to the impact cyber crime can have on the port itself. Cyber attacks have the ability impact to how a port safely carries out operations,

they also have the ability to reduce the speed and efficiency a port operates at. There is the risk of damage to ships and crews, if, for example, a ship collision occurred due to a hacking of e-navigation. The overall port business could be disrupted and damaged, resulting in a tarnished reputation. There is the risk of huge losses, be it in regards to, physical assets, the loss of cargo or the loss of personal data of employees or customers. These are only to name a few of the impacts that a lack of cybersecurity can do to ports.

What can ports do to increase their cyber security? It is important to implement security measures to identify and manage the continuous risks and threats to a port system.

• Define a clear governance, objectives and strategic guidelines around cyber security at port level.

• Identify all potential external and internal cyberthreats and the vulnerabilities associated with these.

• Involve all stakeholders involved in port operations

• Raise awareness of cyber security matters at port level

• Infuse a cyber security culture

• Adopt a secure and controllable communications system

• Adopt a risk-based approach to build a port cybersecurity strategy

• Ensure that all identified risks are under control and properly identified in a timely manner.

• Conduct and regularly update security risk analysis

• Enforce detection and response capabilities at port level to react as fast as possible to any cyber attack.

• Strictly control access of third parties to the port system

• Develop specific and mandatory cybersecurity training courses

With the recent growth of cyberattacks and increased awareness of cybersecurity, it appears that ports have been somewhat neglected. It is evident that with the world rapidly becoming digitalized and dependent on efficient communication systems, cyber security has been identified as a top-level priority among policymakers and scholars. The gap of knowledge on cybersecurity in ports is a key issue, as it makes them more and more vulnerable

to cyberattacks which will prove a major problem in years to come. The limited amount of information and guidance available about cybersecurity related practices in ports and maritime as a while, indicates the essential need for increased cybersecurity protocols. Traditionally ports were only concerned with physical security and safety, it is now more important to integrate cybersecurity into a global strategy.

About SaltDNA

SaltDNA, ranked in the top half in the Cybersecurity 500, provides a fully enterprise-managed software solution that enables absolute privacy in mobile communications. It is easy to deploy and uses multi-layered encryption techniques to meet the highest security standards. The SaltDNA Desktop and Mobile apps are intuitive and easy to install and use. The SaltDNA Communication Manager provides a console for tight management of users and can be configured for the management of regulatory compliance. SaltDNA is headquartered in Belfast, Ireland, for more information visit saltdna.com.

A word from the Chairman

John Donlon
Chairman
International Association of CIP Professionals
(IACIPP)

Emergencies are a fact of life throughout the world and can take many forms.

Since the 9/11 attacks nearly 20 years ago, national security has been dominated by terrorism and we should not forget, at this time of an international emergency that terrorism remains a significant threat. As does the threat from sophisticated hostile intelligence right through to that of low-level criminals. However, as countries across the globe are currently focused on trying to manage a way through the spread of an infectious respiratory virus which is killing thousands and impacting on billions of people, there will be those who will take advantage at a time when governments, organisations and the national workforce are distracted.

The scale of the current situation seems to have caught us all by surprise, but should it have done? From a UK perspective, looking at the most recent National Risk Register, there is a clear statement about the unpredictability of emerging infectious diseases linking the same to such factors as: climate change; the increase in world travel; greater movement and displacement of people resulting from war; the global transport of food; intensive food production methods and humans encroaching on the habitat of wild animals.

Under the last review in the UK, an international pandemic was classed as a Tier 1 national security risk in the UK - meaning it was judged to be of the highest priority (but was interpreted almost entirely as risk of a type of flu, rather than a SARS-type virus) – but some would now question as to how, both the resources and the preparatory acts, have been addressed when compared with other threats at a similar level, such as terrorism and cyber-attacks. This is not the time to delve into that detail or to point fingers at governments and institutions, there is too much else to be done. In the end, citizens will judge a government by that intangible sense of whether they think it has had a plan to manage the disease. They will look at whether a government remained as in control as possible, and took decisions that were in the spirit both of what the public said it wanted at the time and what it thought the country needed in the emergency and beyond.

The IACIPP Poll

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

Q. How prepared do you feel for a cyber attack?

- Very well prepared - 22%
- Well prepared - 11%
- We are preparing but not yet there - 56%
- We have just started preparations - 0%
- We are not prepared but have started - 0%
- We have not made any preparations and unprepared - 11%

This is, however, the time to start considering and understanding the numerous lessons that will emerge from this situation and to ensure, at a global level they are both shared and acted upon. Unfortunately, dealing with coronavirus has not, so far, been a model showcase for global coordination.

Those of us who are involved within the world of protection and resilience of our national infrastructure have, I believe, often taken a wider view of the threat factors that could seriously impact on our day to day operations. This has been particularly so when we consider the evidence, we have seen following natural type hazards such as earthquakes and flooding. We have often been too slow to pick up on what has or hasn't worked and then turn that into actionable plans to better prepare, respond and recover from such tragic events.

We cannot allow that to happen this time. Functioning critical infrastructure is imperative during the response to the COVID-19 or a similar style pandemic emergency for both public health and safety as well as community well-being. Certain critical infrastructure industries have a special

responsibility in these times to continue operations and to do so they need strong support and clear guidance from the government. There is also a need for evolving good practice, new ideas and innovation to be shared across sectors, regions and countries in a timely way.

Within the IACIPP our Regional Directors are linked into their respective governments, infrastructure operators and academia and are ideally placed to communicate such good practise and innovation as it relates to national infrastructure. Some examples of government activity (not including the obvious financial support that is required) that has been highlighted includes:

- The Centre for the Protection of National Infrastructure (CPNI) in the UK providing advice on Personal Security Behaviours during a pandemic and promulgating the National Cyber Security Centre advice on home working. This is particularly relevant as the COVID-19 outbreak is forcing millions of employees to work from home. This means countless organisations are faced with a unique challenge: how to keep as many business-critical functions running as possible whilst maintaining adequate security. All this alongside an unprecedented rise of 667 per cent in Phishing attacks in the UK compared to just a few weeks ago, as malicious actors trick users via fake coronavirus alerts.
- The Cybersecurity and Infrastructure Security Agency (CISA) in the USA has been taking part in government and industry coordination calls, issuing guidance and working with critical infrastructure partners to prepare for, respond to, and mitigate effects in the U.S. They have produced an excellent document – 'Guidance on the Essential Critical Infrastructure Workforce: Ensuring Community and National Resilience in COVID-19 Response'. This sets out considerations for government and business identifying those who are classed as essential critical infrastructure workers and provides sector by sector guidance. This includes workers who support crucial supply chains and enable functions for critical infrastructure.
- The Lombardi region in Italy has, as we all know, had an extremely difficult time and from that starting point the virus rapidly spread across the whole of the country. The Critical Infrastructure Secretariat of the Presidency of the Council of Ministries has, with the assistance of our– Director for the Mediterranean Region – Alessandro Lazari, released a set of guiding principles in order to ensure the continuity of critical services which are of public interest. Within this they recognize that a pandemic threat wasn't among the ones properly addressed by critical infrastructures' business continuity plans, in consideration of the fact that they were surely recognized as high impact events, but with a low probability occurrence. A fact which appears to be replicated right across both the public and private sectors. The released guidance provides recommendations to the operators of critical infrastructures for the "containment and fight against the spreading of the virus, while ensuring the continuity of essential services, the infrastructures' operation and the safety of the workforce". An article by Alessandro which details the specifics of this guidance can be found within this edition of the World Security Report.

Video of the Month

Some great resources are available on the IACIPP website, and this months featured video presentation comes from Paolo Trucco, Professor – Risk and Resilience Management of Complex Systems research group at Politecnico di Milano.

Paolo Trucco's presentation 'Simulating the resilience of key resource supply chains upon Critical Infrastructure disruptions: the case of Italian FMCG' was presented at Critical Infrastructure Protection & Resilience Europe in Milan in October 2019 and can be viewed at www.cip-association.org.

These are just a 'snapshot' of what some governments are doing. There are obviously others areas of good practise emerging all the time and let's hope as they are identified they are communicated to help us all manage our way through these challenging times.

There are still many things that are unclear and uncertain, whether globally, nationally or in our own lives. However, this shall pass, and in the meantime, we need to continue to observe government guidelines, stay busy and get ready for the recovery that will come.

I hope that you and yours stay safe and healthy, and wish you all the best for these troubled times.

John Donlon QPM FSyI
Chairman IACIPP

World Border Security Congress

24th-26th November 2020

ATHENS, GREECE

www.world-border-congress.com

Building Trust and Co-operation through Discussion and Dialogue

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

NSeRC

Media Partners:

BORDER SECURITY REPORT

WORLD SECURITY REPORT

World Security-index.com

A new normality in security screening?

The Coronavirus crisis is one of the most disruptive events since the Second World War. Whilst governments around the globe strive to get to grips with the situation and plan for a return to normality it is interesting to reflect on exactly what normality will look like. It's almost certainly going to be different to normality as we understand it today.

Whether or not we'll experience anything like it again in the near future is a moot point but what is for sure is that we have to learn the lessons of the current situation and make sure that we do all that we can to prevent creating the conditions for such a pandemic to grip the world in this way again. The security community can make a contribution to this by ensuring that it delivers technology and operational concepts that respect some of the mitigation measures adopted during the recent crisis.

In particular, concepts that result in creating queues and congestion, thereby placing people in close proximity to each other for prolonged periods, need to be avoided. Likewise approaches that expose staff and the public alike to a high level of personal physical contact or that require multiple people to handle pieces of equipment need to be reconsidered. Nowhere is this more applicable than in security screening scenarios involving the protection of crowded places. The Daily

Telegraph , quoting a University of Nottingham and the Finnish National Institute for Health and Welfare study, concluded that whilst travelling by public transport was a significant health risk in general, security checks are thought to be the highest risk areas.

Securing crowded places from the threat of terrorism has been a clear requirement for many years. However, implementing such measures in a proportionate way that is effective, practical and affordable without disrupting daily life is extremely challenging. Whilst the natural response to the mass casualty attacks, that hit Europe from the early 2000s, was to adopt security regimes that were in existence at the time, these regimes were never designed for crowded public places and high throughputs; we need to move on.

Intrusive approaches that originated in aviation security are of little practical use (slow, designed for aviation threats and requiring a high level of staffing) and are disproportionately expensive to deliver at a scale large enough to meet the required throughput of people when it comes to crowded places. The large queues associated with these types of security approaches that often build up outside of the venue are attractive targets in their own right. With reference to the current crisis, they are high density, high contact environments and at odds with the health lessons identified and mitigation measures implemented to date.

In recent years, great effort, much of it driven by governments and international defence and security bodies (NATO in particular), has been put into developing practical means of screening large numbers of people for the most serious terrorist threats. These efforts have been rewarded and technologies have been introduced to the market that offer a proportionate, efficient and cost-effective solution. A range of technologies, some passive others active, some narrow beam standoff devices and others wide angle devices offer a choice for the end user to meet various scenarios and requirements. An example of these high throughput systems is Apstec's Human Security Radar (HSR), which is a wide angle, real time and autonomous active system.

HSR is a free flow technology that enables the security screening of thousands of people an hour. The system uses active centimetre wave to detect the presence of explosive threats carried on the body or in body worn bags, and detects metallic and non-metallic fragmentation associated with IEDs. Metal detection technologies offer the opportunity to detect firearms and bladed weapons, and, where the operational need exists, options allow more stringent requirements relating to smaller threat items to be met.

The inspection zone of HSR is several meters wide and up to 6 metres deep, allowing the free flow of people through the system. The free flow nature of the system and the large inspection zone allows for social distancing between people, where the requirement exists. People can adopt their own personal space as they see fit or as directed as part of strategy to manage health risk. The whole operation requires only a handful of security staff but may deliver the throughput and security effect of 10-15 conventional security lanes, or more, where a manual screening or traditional approach is used.

Although HSR is unique in some ways, there are several technologies that offer robust and mature capabilities that are designed specifically for protecting crowded places. There's no single technology that appears a perfect fit for every case but the technologies that exist meet a wide range of scenarios. In many instances, it is conceivable that a number of different but complementary screening technologies may be used to contribute to an effective operational concept. What these technologies all have in common is that they aim to deliver as high a throughput as the technology allows in a way that is simple to operate and that minimises the disruption to people passing through the systems.

Of course, it's not all about high throughput, security systems such as HSR also offer a much-improved personal experience for those passing through them. No divestment is required, personal contact is avoided for the vast majority of people and high value clients are offered a service that is more consistent with their expectations.

As high throughput systems allow for several people at a time to pass through them, they lend themselves to behavioural detection where abnormal behaviour can be identified in direct comparison with others. These types of system are considered to be a good triggers for behavioural detection and

many security regimes draw heavily upon the integration of the technology and an operational concept that incorporates behavioural detection.

Further opportunities exist to integrate high throughput systems with other technologies such as video tracking, biometric identification systems, and, for some, thermal cameras that could provide a health monitoring capability. Of course, the integration of these technologies would need to be done sensitively and there's a risk that the responder becomes overwhelmed. It is also clear that in some cases different alerts will require different responses but integrating biometrics with high throughput security screening is becoming a common request. Combining biometric technologies with a technology like HSR not only allows people of interest to be detected but also offers the prospect of implementing access control and security screening in a single seamless operation. These are interesting developments and provide a means of doing all of this in a way that minimises health risks.

To cap it all, high throughput systems offer a cost-effective solution. Whilst capital expenditure on security screening is a significant factor, the cost of people will almost always outweigh the cost of equipment over the life of a system, and generally do so many times over. Being able to deliver so much security effect with such a small work force is great and cost effectiveness a significant advantage with these systems.

When confronted by mass casualty scenarios the security world adopted what seemed a sensible approach at the time and used aviation type security. That this approach wasn't well suited to securing crowded places was outweighed by the imperative of just doing something in the face of a changing threat environment. However, high throughput security screening technologies that have spent years in development are available and offer a bespoke approach to securing the most attractive targets. They are cost effective, respect the public's right to

get on with day to day life with the minimum of disruption and offer a simple and agile approach. In light of the lessons of the Coronavirus crisis, these systems can deliver an operation that is low contact thereby, minimising health risks, and which has the scope for further technology integration to provide a more comprehensive security outcome. They have the ability to significantly reduce costs and, for once, have the prospect of contributing to the bottom line of the business.

Now is a good time to move on from an historical security approach and to consider how state of the art high throughput security screening systems can help mitigate terrorist and health risks, and do so in a way that offers considerable cost benefit. For governments, businesses and for the reassurance of the general public, there should be an expectation that security contributes to the fight against terrorism in a way that also embraces best practice identified during the Coronavirus crisis. If so, it is highly likely that this will become the new normality.

By Stephen Cooper, OBE, COO Apstec Systems

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

Securing Prison's with next generation Motion Detection Technology

On the 26th June 2019 James Bartholomew escaped from Grays Harbor County Jail, USA by hiding in a large rubbish bin, which was taken outside the walls of the jail by another prisoner. He was preparing to plea to a drug and a weapon offense and was facing a lengthy prison sentence.

After being on the run for nearly a month, he was finally apprehended on July 19th found to be carrying substances believed to be heroin and methamphetamine. He now adds various charges including escape and drug charges to his original offenses.

And this is not the first time using this method. In 2018 in Kentucky two prisoners escaped jail by hiding in wheelie bins. They were soon apprehended but their escape was caught on cctv footage and soon went viral causing acute embarrassment to the authorities.

Richard Lee McNair an infamous prison "escape artist" mailed himself out of prison in a crate in April 2006 – he was captured in October 2007 and is now back in jail. McNair previously used lip balm to squeeze out of handcuffs to escape, and on another occasion slipped through a ventilation shaft.

In 2001 Joaquín Guzmán Loera (El Chapo) the notorious drug

lord, thought to be the most powerful drug smuggler in the world, escaped a federal maximum security jail in a laundry cart that was rolled through several doors and security checkpoints and eventually out the front door. He was then transported in the boot of a car.

The desire to escape for inmates serving life or very long sentences is never going to go away and every avenue has been tried and will be tried again. Even prisoners serving shorter sentences can be tempted to try to escape if they feel that they have some pressing business in the outside world.

If we have learnt anything from history it is that "Where there is a will, there is a way."

With thousands of vehicles and other containers coming and going from our prison and correctional facilities every day, it is vital to have a quick, safe and reliable way of checking that they are not being used to smuggle out inmates.

However unlikely a scenario it may seem, we must assume that any vehicle or container that could possible carry a human, regardless of size, should always be inspected in some way before leaving any prison or correctional establishment.

Different technology types have been tried over the years, albeit with limited success. For example, 'sniffer' technology cannot be deployed on all types of large vehicles. While X-Ray technology is also limited in being deployed only on certain types of trucks, in addition to the fact that there are health and safety concerns, for both the operator and any hidden fugitive.

Motion Detection Technology (sometimes called Human Presence Detection or Heartbeat Detection Systems) has been in use in some prisons, as well as border crossings, for a number of years. However, the early adaptations of this technology were deployed with very limited success, many being turned off permanently and decommissioned shortly after installation.

For example, they were not able to operate in busy noisy environments, simply because they could not determine which vibrations were coming from within a truck and which were coming from the surrounding area. These systems were also subject to breakages and fragile, i.e. unable to withstand the real world dirty, dusty, damp environments of prison compounds, nor able to endure the operational input from prison security staff, as opposed to office administration staff.

ClanTect's 2nd Generation of Motion Detection Technology has radically upgraded the performance, flexibility and durability of these systems, bringing huge operational benefits for the prison services.

ClanTect is able to effectively filter out all environmental disturbances. So regardless of any passing traffic, road works, nearby building works or machinery, turbines and engines, ClanTect can isolate the component of vibration emanating from within any vehicle. So there really is 'no hiding place' for any prisoner.

The ClanTect system is based upon one single enclosed unit (certified to Mil spec IP65), which provides for a very rugged device, designed to handle the harsh reality of operations in a prison compound.

The system is also easy and quick to operate, and there's no requirement for any technical or specialist skills. The sensors are simply attached to the frame of the truck or container, it literally takes seconds. The operator then presses a button, and the system then automatically executes an 'electronic search' of the vehicle, which is completed in just over a minute. There is practically zero operator intervention.

The system is also built to operate on a 24 x 7 basis, thereby ensuring that any container whether leaving or entering the prison compound during day or night hours can be searched. ClanTect's systems have been searching tens of thousands of vehicles, for years, without breaking down, this technology really is built to last.

ClanTect have added an integrated ANPR (Automatic Number Plate Recognition) camera, which automatically captures the plate details of every vehicle entering and leaving the prison. This eliminates any human error and speeds up the throughput of vehicles through the Prison gate.

Clantect also provide an optional secure high-speed communications gateway. This enables online communications between the terminals installed at the prison gate area and the prison control centre, or even at a regional or national control centre. Equally data can be securely and rapidly downloaded from the terminal to the central operations centres, which gives instant access about every truck and every search.

As a result of this technology refresh, ClanTect's new generation Motion Detection Technology is being successfully deployed in prisons and border control areas, and most tellingly they have replaced many out-dated and now redundant systems. This 2nd Generation technology is truly a key component in maintaining the integrity of Europe's borders and is providing far more effective security for Prisons.

Colin Summers – Sales and Marketing Director, ClanTect Ltd.

Alert and Protocols Next Stage of the Security Situation (Convid-19)

Multi-national corporate companies may have globally located partners or branches therefore dictating that what happens in one country will impact another. There are some countries that are within days be in a state of anarchy which will deliver unimaginable consequential collateral damage. Using the term 'unimaginable' is because, now more so than ever, desperate people will do desperate things which they would never think of doing before.

There are many slum cities besides poor people living in villages, towns and cities. These people are massed together that live, eat, and transport together. They are inter-dependent on each other besides dependant on menial jobs paying them daily or weekly. It would be impossible for them to lockdown for 21 days and starve to death. Their situation would drive them to acts of desperation.

Also, there are also invisible people working in high-risk sites who are the foundation of support services that keep the system alive. For example, people applaud the surgeons, doctors and nurses but what about the cleaners, cooks and maintained that keep the hospitals running? When one or more get ill, the entire chain of support may need to be re-manned, but the re-training time impacts the smooth running of the system.

The following may sound not applicable to practitioners in some countries however, the situation would be time dependant on finding of a cure.

Situation

- Increased numbers of starving people due to loss of jobs
- People desperate for medicines, protection clothing and equipment
- Many will be desperate for protection gear depending on their location for security

Implications

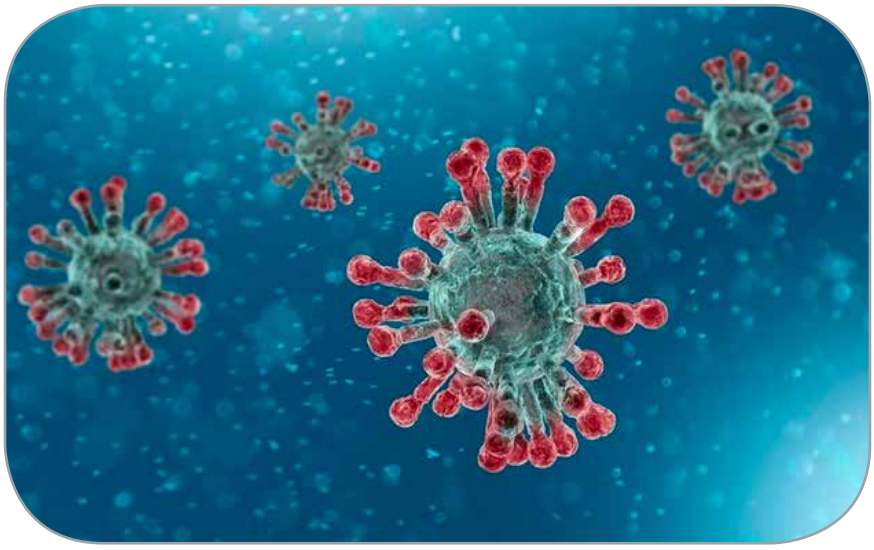
- Increased theft and shoplifting
- Mob attacks on warehouses stocking food and medicines or outlets for such be located in malls shops hospitals, pharmacies or old-aged nursing homes or even shops on the streets.
- Attacks of logical supply chain of food and medicine
- Increased home invasions
- Many more weaponized people without training
- Increased perimeter protection equipment and manpower
- Many more people suffering from emotional or mental disorders

Problems

- It is doubtful that countries can afford to mass feed or house the many. Once people starve specially their children would starve, then, their reaction would be hostile
- The covid-19 pandemic is similar to the previous SARS threat but, the SARS was easier to cure. Even though some human trials have begun, it when an antidote will be discovered, obtain approval, manufacture and distribute.

Limiting the collateral damage

Considering the term that security



success to limit the collateral damage of the virus on people and assets will depend on the level of situational awareness of the people on the ground and their reaction speed

Situational Awareness: the knowledge to identify a person of interest or a group working in concert. One must heighten situational awareness using equipment, technology and manpower.

- Technology and Equipment

Temperature/Fever detection using CCTV or Handheld thermometers will detect an infected person

One cannot bank on facial recognition as people will wear masks . Some facial recognition technology is deriving disappointing results because of the masks (https://ipvm.com/reports/face-masks). The combination of both temperature/fever and facial would be best for certain applications if one does not have handheld thermometers.

People on the ground making decisions

- Manpower: It is vital that manpower must be quickly trained with skills that are relevant to the new threat. Comprehending the narrative, it is possible that the manpower on the ground could be dealing with volatile behaviour.

The officers on the ground must have the character traits that are balanced with empathy and ego drive. A highly aggressive and reactive person is not a good choice for first interaction with the public. This threat also dictates that the people on the ground will experience issues that they know and that they do not know. For example, they may have been trained not to take action but, to summon their superiors. Making decisions and reaction speed for pandemic security demands fast decision making and actions to be taken. Scenario, the temperature/fever detection identifies a person of interest. What should they do? There is quite a bit more to this… (get the answers from ISIO (find later in this work)

- The Manpower must be able to identify a person of interest and to determine if they are working in concert with others either voluntarily or under duress to mitigate loss prevention. Therefore, lie, deception detection and critical situational interviewing are the relevant skills
- Subsequently, some practitioners may need to be familiar with crime culture, criminal methods and

critical infrastructure PROTECTION AND RESILIENCE EUROPE

6th-8th October 2020

Bucharest, Romania

www.cipre-expo.com

REGISTRATION NOW OPEN

Early Bird Rates currently apply - Register Today!

Securing the Inter-Connected Society

UN Member States need "to share information [...] to prevent, protect, mitigate, investigate, respond to and recover from damage from terrorist attacks on critical infrastructure facilities, including through joint training, and use or establishment of relevant communication or emergency warning networks."

The 7th Critical Infrastructure Protection and Resilience Europe brings together leading stakeholders from industry, operators, agencies and governments to debate and collaborate on securing Europe's critical infrastructure.

Register online today at www.cipre-expo.com/onlinereg.

To discuss sponsorship opportunities contact:

Paul Gloc
(UK and Rest of World)
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

Leading the debate for securing Europe's critical infrastructure

Owned & Organised by:

TORCH

Supporting Organisations:

International Association of CIP Professionals

ICI

NS&RC

SPF

ISIO

Media Partners:

World Security-index.com

WORLD SECURITY REPORT

behaviour

• Bias impacting decision-making. Bias towards any size, colour, religion of a person could be misinterpreted which could add fuel to the fire of violent behaviour.

• Psychological Considerations

Practitioners could handle emotionally distraught or mentally unwell people. This calls for practitioners on the ground now must be even more socially aware to comprehend that some people (determine if they are normal, emotional or mentally challenged) may be over-reacting and becoming highly sensitive and must be understood before physical intervention is used.

• Cultural Considerations

A person that is bias will naturally display their emotions in their tone of voice and body language which will instinctively obtain a negative reaction by another person to the extent of a hostile and physical reaction. This could also lead to a person misinterpreting or being misunderstood by another culture and providing an unreliable reading to the practitioner. This calls for practitioners to be properly trained with lie, deception detection using critical situational interviewing taking cultural behaviour into account. For handling conflict or violent behaviour, the practitioner must be culturally aware (conduct and behaviour) so that they do not over-react or make decisions based on bias

Reaction Speed

Reacting to late will invite collateral damage. It is recommended that when a person that has been flagged with a high temperature then the protocols mentioned below must be used. As a matter of fact, unlike investigation scenarios where reaction speed must be purposely timeous, for pandemic security reaction speed is paramount from the person in charge down to the practitioner on the ground.

• Physical Considerations

We must consider that people are now perhaps 'weaponized' with covid19 and therefore, precautions must be considered

Protocols for Action

When identifying the Person-of-interest using temperature/Fever detection

1. We must consider that people are now perhaps 'weaponized' with covid19 and therefore, precautions must be considered

2. Approaching the person must only be by properly protected trained staff

• Consider that the person that is infected could affect others within 1.5m (+3ft) to 2m (6ft) and, also know that the eyes and mouth could be entry points for the virus. Subsequently, staff must use eye-goggles or face shields with masks when approaching a person of interest.

• If there is resistance by a person-of-concern, then the practitioner may consider if correctly trained to detain the person of concern and must alert the authorities as soon as possible (Each sector has its own recommended protocols. Contact HIM for discussion)

Incident Management

The validity of the narrative will depend on the quality of the data captured, either by deception detection critical situational interviews or by physically testing people for the virus. Yes, it is possible to locate a person of interesting depending on the stage of infection when they display a temperature/fever which could be captured on cctv or by handheld devices, but, at the end of the day, the data must be accurately reported.

A skilled practitioner with investigation management and critical thinking abilities would be able follow certain bits of information that will present an understanding and overall interpretation of the complete picture.

By following the data, the practitioner would then be able to see the movement and tempo of an emerging threat. The reaction speed must be timeously applied to limit or mitigate the collateral damage but again in regarding pandemics, quick reaction speed is vital. There is no room for procrastination – response time must be quick.

Presented by ISIO |International Security Industry Organization for HIM | Human Investigation Management

Criminals Profiting from Covid-19 Pandemic

During this unprecedented crisis, governments across Europe are intensifying their efforts to combat the global spread of the coronavirus by enacting various measures to support public health systems, safeguard the economy and to ensure public order and safety.

A number of these measures have a significant impact on the serious and organised crime landscape. Criminals have been quick to seize opportunities to exploit the crisis by adapting their modi operandi or engaging in new criminal activities. Factors that prompt changes in crime and terrorism include:

High demand for certain goods, protective gear and pharmaceutical products;

Decreased mobility and flow of people across and into the EU;

Citizens remain at home and are increasingly teleworking, relying on digital solutions;

Limitations to public life will make some criminal activities less visible and displace them to home or online settings;

Increased anxiety and fear that may create vulnerability to exploitation;

Decreased supply of certain illicit goods in the EU.

Building upon information provided by EU Member States and in-house expertise, Europol has published today a situational report analysing the current developments which fall into four main crime areas:

CYBERCRIME

The number of cyberattacks against organisations and individuals is significant and is expected to increase. Criminals have used the COVID-19 crisis to carry out social engineering attacks themed around the pandemic to distribute various malware packages.

Cybercriminals are also likely to seek to exploit an increasing number of attack vectors as a greater number of employers institute telework and allow connections to their organisations' systems.

Example: The Czech Republic reported a cyberattack on Brno University Hospital which forced the hospital to shut down its entire IT network, postpone urgent surgical interventions and re-route new acute patients to a nearby hospital.

FRAUD

Fraudsters have been very quick to adapt well-known fraud schemes to capitalise on the anxieties and fears of victims throughout the crisis. These include various types of adapted versions of telephone fraud schemes, supply scams and decontamination scams. A large number of new or adapted fraud schemes can be expected to emerge over the coming weeks are fraudsters will attempt to capitalise further on the anxieties of people across Europe.

Example: An investigation supported by Europol focuses on the transfer of €6.6 million by a company to a company in Singapore in order to purchase alcohol gels and FFP3/2 masks. The goods were never received.

COUNTERFEIT AND SUBSTANDARD GOODS

The sale of counterfeit healthcare and sanitary products as well as personal protective equipment and counterfeit pharmaceutical products has increased manifold since the outbreak of the crisis. There is a risk that counterfeiters will use shortages in the supply of some goods to increasingly provide counterfeit alternatives both on- and offline.

Example: Between 3-10 March 2020, over 34 000 counterfeit surgical masks were seized by law enforcement authorities worldwide as part of Operation PANGEA supported by Europol.

ORGANISED PROPERTY CRIME

Various types of schemes involving thefts \have been adapted by criminals to exploit the current situation. This includes the well-known scams involving the impersonation of representatives of public authorities. Commercial premises and medical facilities are expected to be increasingly targeted for organised burglaries.

Despite the introduction of further quarantine measures throughout Europe, the crime threat remains dynamic and new or adapted types of criminal activities will continue to emerge during the crisis and in its aftermath.

Newly declared states of emergency must include a time limit and parliamentary oversight, OSCE human rights head says

Emergency legislation being adopted by governments across the OSCE region must include a time limit and guarantee parliamentary oversight, said the Director of the OSCE Office for Democratic Institutions and Human Rights (ODIHR) ahead of a vote in Hungary to extend emergency measures earlier adopted in the EU member state.

Global operation sees a rise in fake medical products related to COVID-19

Counterfeit facemasks, substandard hand sanitizers and unauthorized antiviral medication were all seized under Operation Pangea XIII, which saw police, customs and health regulatory authorities from 90 countries take part in collective action against the illicit online sale of medicines and medical products.

The operation resulted in 121 arrests worldwide and the seizure of potentially dangerous pharmaceuticals worth more than USD 14 million.

Criminals are cashing in on COVID-19

The outbreak of the coronavirus disease has offered an opportunity for fast cash, as criminals take advantage of the high market demand for personal protection and hygiene products.

Law enforcement agencies taking part in Operation Pangea found 2,000 online links advertising items related to COVID-19. Of these, counterfeit surgical masks were the medical device most commonly sold online, accounting for around 600 cases during the week of action.

The seizure of more than 34,000 counterfeit and substandard masks, "corona spray", "coronavirus packages" or "coronavirus medicine" reveals only the tip of the iceberg regarding this new trend in counterfeiting.

"Once again, Operation Pangea shows that criminals will stop at nothing to make a profit. The illicit trade in such counterfeit medical items during a public health crisis shows their total disregard for people's wellbeing, or their lives," said Jürgen Stock, INTERPOL's Secretary General.

Compared to the week of action in 2018, this latest edition of the operation reported an increase of about 18 per cent in seizures of unauthorized antiviral medication, and an increase of more than 100 per cent in seizures of unauthorized chloroquine (an antimalarial medication), which could also be connected to the COVID-19 outbreak.

Seizures and website closures

During the week of action (3 - 10 March 2020) authorities in participating INTERPOL countries inspected more than 326,000 packages of which more than 48,000 were seized by customs and regulatory authorities.

Overall, authorities seized around 4.4 million units of illicit pharmaceuticals worldwide.

More than 37,000 unauthorized and counterfeit medical devices were also seized, the vast majority of which were surgical masks and self-testing kits (HIV and glucose), but also various surgical instruments.

Information received from the participating countries during the operation points to a considerable decrease in international shipments of small parcels (by about 40 per cent), probably due to the coronavirus outbreak.

The operation has already closed down more than 2,500 web links, including websites, social media pages, online marketplaces and online adverts for illicit pharmaceuticals with a similar number in the process of being closed down. The combined efforts of the authorities disrupted the activities of 37 organized crime groups.

INTERPOL

International Day of Forests: protecting Earth's most biologically diverse ecosystems

INTERPOL marks International Forest Day by highlighting how the global police community tackles forestry crime as part of steps to make the world a safer place.

INTERPOL operations to date have resulted in the seizure of more than 1 million cubic metres of illicit timber (worth in excess of USD 1.5 billion) across Africa, Asia, Europe and Latin America.

Training of financial intelligence units has led to millions of dollars in assets being seized from illegal logging networks and returned to state budgets.

Vacant workplaces and buildings are places for perpetrators

As the potentially deadly COVID-19 virus continues to spread, many offices, retail operations, manufacturing facilities and other businesses close and send employees home to work. Those empty facilities ' contents can become easy targets for criminals.

Most companies are secured by conventional plastic access cards or access control schemes. Yet, by themselves, they may not be enough. Commonly used forms of cards-mag stripe, proximity, even MIFARE or iCLASS-may be cloned by an accomplished hacker within minutes. Which will produce two equivalent cards but the disparity will not be recognized by the device program.

Imagine server rooms, storage of equipment and many other places which are all readily available to unauthorized people. That is why it has become so necessary to provide two-factor authentication using a biometric technology. Cloning fingerprints, facial expressions, and iris patterns is hard, almost difficult.

But what betters one biometric device than the others? Readers needing fingerprint touch. The COVID-19 virus has been demonstrated to live for as long as three days on stainless steel and plastics. Facial recognition is contactless; but the systems are not the most reliable. And many people wearing protective masks today merely decrease the accuracy.

Recognition of iris is highly precise, able to recognize a person wearing gloves, masks, goggles, glasses and lenses. It's likewise contactless. There is also no need to reenroll workers into the security program as the iris pattern of a individual is set at birth.

Installing iris recognition readers at building entrances provides a vital second layer of protection at insecure premises as they remain vacant during this global health crisis.

By Mohammed Murad is vice president global sales and business development, Iris ID

New South Wales Police Force and IDEMIA Extend Partnership to Strengthen Criminal Identification System

IDEMIA has renewed its partnership with the New South Wales Police Force, the largest police force in Australia. Under the six-year contract, IDEMIA will support and maintain the LiveScan solution, a powerful biometric identification solution to process and book criminals' biometric data in 142 police stations across New South Wales.

IDEMIA's LiveScan technology provides law enforcement jurisdictions with a flexible workflow-based application to capture criminals' biometric information and demographics. LiveScan ensures that the biometric solution can be deployed across the state efficiently while meeting the highest quality and safety requirements.

The New South Wales Police Force is serving more than 7.5 million people over an area of 800,000 sq. km. IDEMIA is the leader on the Australian market for biometric enrolment and authentication as LiveScan is being used across the states of New South Wales, Queensland, Victoria and the Northern Territory.

"This contract strengthens a long-term partnership that we have had with the New South Wales Police Force for over two decades", said Tim Ferris, Asia Pacific President and Senior Vice President for Public Security and Identity at IDEMIA. "This collaboration proves IDEMIA's capacity to provide critical support and maintenance when it comes to integrating multiple biometrics technology to increase national security and support efficient police services. It is a great honour to be supporting the biggest police organization in Australia."

Canadian tech company has announced a product that allows governments to analyse the patterns and movement in public spaces to support emergency response strategies and social distancing programs

InnerSpace has announced its product capabilities to support all levels of government to analyse the patterns and movement in public spaces using existing WiFi networks. The platform is ideally suited to understand the movement of people inside public spaces and can support emergency response strategies, social distancing programs, and help Smart Cities implement effective security and public safety measures.

"In response to the global COVID-19 pandemic, we have accelerated the delivery of our public safety solution inFORCE," said James Wu, CEO, InnerSpace. "Our platform processes RSSI data in real-time and returns the industry's most accurate location data available today. By using public WiFi access points, municipalities have a way to quickly roll out new solutions at city-wide scale."

InnerSpace inFORCE, was selected in a competitive process by the Department of Homeland Security, for its ability to use WiFi to locate citizens and track emergency responders in an active shooter scenario.

The same platform can be used in a wide variety of emergency situations such as the current COVID-19 pandemic. In addition to the company's tracking capabilities, it's analytics dashboard gives public safety offices an unprecedented view into how people leverage public spaces.

"In times of emergency, it is reasonable to prioritize safety and public health to minimize the loss of human life," said Cerys Goodall, President & COO, InnerSpace. "By providing municipalities with a system that can deliver line-of-sight into how people move in public spaces, we can inform response strategies, improve rescue efforts, and create an infrastructure to support better outcomes."

InnerSpace inFORCE ingests RSSI data and returns accurate anonymous indoor locations. The information can be connected directly into emergency response communications systems, building management and security systems, or analysed by InnerSpace to identify critical patterns and trends in people's movements.

3DX-Ray Secures New Contract for Asian Customer

3DX-Ray have announced a sale of its ThreatScan®- LS3 lightweight, x-ray scanner system to an undisclosed government agency in Asia.

After initial operator training provided by 3DX-Ray, the system will be deployed in co-operation with the United Nations on mine and EOD clearance peace keeping missions in the Middle East and Africa.

ThreatScan®- LS3 is a compact, yet powerful x-ray scanning system that can penetrate 34mm steel at 120kV as standard. The 305mm x 256mm imaging area enables typical bags and packages to be scanned in one scan. The complete system fits securely into a backpack, ideal for operations in remote locations.

Designed for rapid deployment and ease of use, ThreatScan® systems operate with the intuitive and user-friendly ThreatSpect software to produce high quality, sub-millimetre resolution images.

The ThreatScan®- LS3 is designed so that the operative can achieve accurate high-quality images quickly and efficiently.

Protecting Prisoners, Prison Staff and Visitors from COVID-19

The world is currently facing an unprecedented challenge in dealing with the coronavirus (COVID-19) pandemic. The World Health Organization's prevention advice is simple; wash your hands, cough into your elbow, avoid touching your face, distance yourself at least one metre from another person and if you feel unwell, stay at home. Above all, keep away from other people, or what is now termed 'social distancing'.

For the general public, in theory, these measures should be relatively easy to adhere to, although they are proving challenging enough, 'social distancing' in a prison environment is almost impossible, leaving prison staff, prisoners and visitors vulnerable.

Prison Reform International (PRI) in their recent briefing note, said "The difficulties in containing a large outbreak in detention facilities are clear. People in prison and the personnel who work with them are in close proximity and in many cases in overcrowded, cramped conditions with little fresh air. People in detention also have common demographic characteristics with generally poorer health than the rest of the population, often with underlying health conditions. Hygiene standards are often below that found in the community, and sometimes security or infrastructural factors reduce opportunities

to wash hands or access to hand sanitizer – the key prevention measures recommended by the World Health Organization."

If luxurious cruise ships were described during the initial outbreak of COVID-19, as a "Floating Petri Dishes", then it is not difficult to imagine the challenges facing prisons.

The numbers of infected prisoners around the world are increasing daily - A scary proposition for authorities to handle.

Most Countries have issued their own standards for their prisons.

The Government of Iran temporarily released 70,000 prisons. Each prisoner had to test negative for COVID-19 and post bail before being released.

The automatic first step taken by prison/detention authorities to prevent an outbreak of a disease is to limit contact with the outside world; generally, to stop visitations.

In Italy, riots and protests erupted in 27 prisons when visiting rights were stopped, killing and injuring many prisoners and staff.

In Colombia, riots broke out across 13 prisons, killing at least 23 prisoners and staff and injuring many more.

These incidents and others around the world were triggered by fear of the unknown and the perceived helplessness of the prisoners.

The World Health Organizations interim guidance on how to deal with COVID-19 in Prisons,

"Preparedness, prevention and control of COVID-19 in prisons and other places of detention" - lists advice concerning the risk of; communicating the disease, personal protection measures, use of masks, environmental measures, physical distancing measures, and staff returning to work. In all instances, the necessity of being closer than one meter from a prisoner, i.e. arrest, restraint or interviewing, the minimum staff should wear are disposable gloves, medical mask, long-sleeved gown, and eye protection, i.e. face shield or goggles.

During this time of crisis the safety of the prisons is paramount and the typical day to day running of the prison needs to continue unhindered, and this includes checking inmates, staff and visitors for any contraband; be that drugs, weapons, cell phones, or any other illegal items.

One of the main benefits of the Soter RS scanner is its ability to scan a person, internally and externally, remotely, even from another room, thereby alleviating the need for close contact, protecting operators, prisoners and visitors alike.

The Soter RS is the worlds most advanced security X-ray system. It is a person X-ray system which combines ultra-low radiation with maximum visibility, revealing everything hidden inside human cavities or inside the human body.

It is already used successfully in many prisons worldwide for scanning visitors, inmates, and prison staff.

The Soter RS body scanner can detect any contraband. Indeed, to date, it has identified; drugs/narcotics, weapons, cell phones, plastic items, metals, cash, gemstones and other contraband. If it is hidden, the Soter RS can detect it; whether it is on, or in, the body being scanned.

Integrated counter UAV solution led by FREQUENTIS and HENSOLDT

Frequentis and HENSOLDT sign Memorandum of Understanding (MoU) to intensify collaboration on integrated counter drone solutions for airports

Frequentis, the leading Air Traffic Management (ATM) solution provider, and defence and security sensor specialist HENSOLDT are combing strengths to support the creation of next generation integrated counter unmanned aerial vehicle (UAV) solutions. Both companies are already combining their respective strengths and competences on the FALKE research project, which aims to develop the blueprint solution for the airport environment.

The formation of this MoU further reinforces our intention to create effective solutions to differentiate cooperative and non-cooperative flying objects, ensure shared situational awareness across all organisations

and interoperability with existing airport surveillance infrastructures and available UAV traffic management (UTM) systems. We are pleased to be working on this common goal with HENSOLDT, combining our strengths." says Günter Graf, Frequentis Head of Business Development.

The Frequentis Group is providing mature components in the areas of UTM/ATM/drone detection, data fusion and exchange (MosaiX SWIM), shared situational awareness and ATM-grade surveillance data automation (SDDS-NG, MSDF, PRISMA), cross-agency incident management (ICM), as well as operational requirement analysis (Control Room Consulting). HENSOLDT will provide detection, identification and mitigation modules from their own Xpeller CUAV system.

"Together with Frequentis, we will create a modular counter-UAV system optimised for the specific needs of airports", added Markus Wolf, Head of Sales and Business Development at HENSOLDT Ventures. "Xpeller demonstrates HENSOLDT's innovative capabilities, answering our customer's needs to detect and act against unmanned threats. Due to its versatility, Xpeller is able to offer maximum protection under a variety of conditions and ranges. While available as a fully functional stand-alone system, its modular approach enables us to easily join forces with partners like Frequentis."

Both companies already work together on the FALKE project, developing the ability to intercept small UAV that enter restricted airspaces at airports. The integrated solution will enable airports to deal with incidents, like those that took place at British airport Gatwick and German airport Frankfurt, swiftly and effectively. Hamburg Airport will be the model for the resulting blue-print solution, with the partners demonstrating a technical and organisational concept to defend against illegally operating drones.

Herta launches a new technology that allows facial identification even with a mask

Herta is launching this week a new version of its facial recognition algorithms that can correctly identify people who wear facial masks. The company had been working on the issue of partial occlusions for some time and, following the worldwide outbreak of coronavirus (CoVid19), development has been accelerated to launch a version of the software that helps provide an accurate identification under these conditions.

Based on Deep Learning technology, Herta's algorithms provide very high identification rates, especially in identity verification tasks and their reliability is very high, even when people hide a large part of their face. It is important to remember that the most differential part of the human face is in the eye area.

The launch of this software is key for the identification in automatic passenger control systems with documentation, such as border control with the passport. This way it will not be necessary for the person to remove the mask, avoiding possible contagion or long waiting times. Its application, in general, extends to any type of access control or identity verification system.

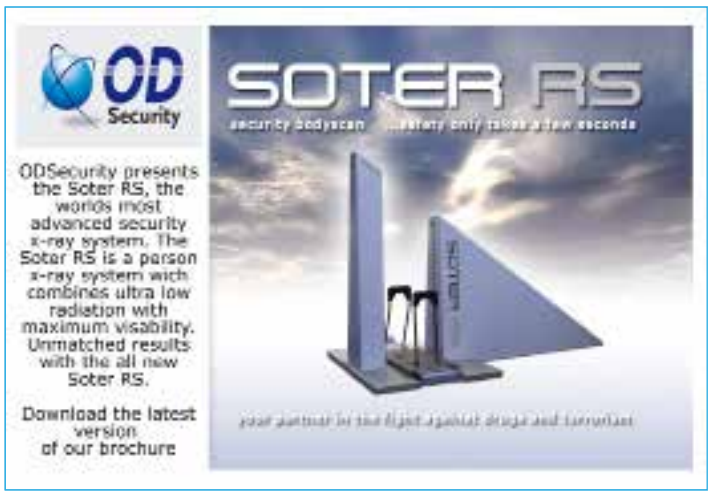
Herta expects that the impact of this new technology in the market will be very important worldwide and that it will be used massively in environments such as transportation, health, government, events, sports stadiums or in the gaming sector.

World Security Report

World Security Report is a bi-monthly electronic, fully accessible e-news service distributed to over 130,000 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.

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 20,000 border agencies, agencies at the borders and industry professionals, policymakers and practitioners, worldwide.



June 2020

2-4
InfoSecurity Europe
London, UK

2-4
National Cyber Summit
Huntsville, AL, USA

29 June-2 July
National Homeland Security Conference
Chicago, IL, USA

July 2020

6-8
SECON 2020
Seoul, Korea

September 2020

2-3
The 15th International Conference on Critical Information Infrastructures Security 2020
Bristol, UK

8-10
IFSEC
London, UK

22-23
The Security Event
Birmingham, UK

22-25
Security Essen 2020
Essen, Germany

27 Sept - 2 Oct
GITEX Global
Dubai, UAE

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

October 2020

6-8
Critical Infrastructure Protection & Resilience Europe
Bucharest, Romania
www.cipre-expo.com

27-29
Critical Infrastructure Protection & Resilience North America
New Orleans, LA, USA
www.ciprna-expo.com

November 2020

24-26
World Border Security Congress
Athens, Greece
www.world-border-congress.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