INCORPORATING BORDER SECURITY REPORT

# WORLD SECURITY REPORT

Official Magazine of International Association of CIP Professionals

MARCH / APRIL 2018
www.worldsecurity-index.com

## COVER STORY

## SECURING COMMUNICATIONS AT A TIME OF ‘EXTREME EVENTS’

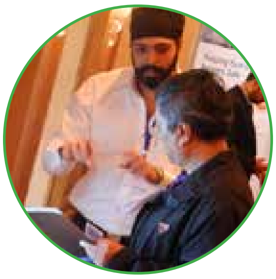
# critical infrastructure PROTECTION & RESILIENCE ASIA

Strategic Partner:

NACSA

In Partnership With:

CyberSecurity MALAYSIA
An agency under MOSTI



## 17th-19th July 2018

Sarawak, Malaysia

www.cip-asia.com

## *Developing resilient infrastructure for a secure future*

# Register Today

**The 3rd Critical Infrastructure Protection and Resilience Asia will bring together leading stakeholders from industry, operators, agencies and governments to collaborate on securing Asia.**

Southeast Asia has seen a rise in insurgency-related attacks and terrorist activities, creating uncertainty and insecurity on critical national infrastructure.

Climate change has also seen more extreme weather patterns, creating additional hazardous, unseasonal and unpredictable conditions and a severe strain on infrastructure.

**The conference will look at developing existing national or international legal and technical frameworks, integrating good risk management, strategic planning and implementation.**

***Be part of the discussion - and solution!***

**Register online at www.cip-asia.com**

***Gain access to leading decision makers from corporate and government establishments tasked with Critical Infrastructure Protection and Resilience.***

### Latest Confirmed Speakers include:

- Ir. Md Shah Nuri Md Zain, Chief Executive, National Cyber Security Agency (NACSA), Malaysia
- Dato Dr Chai Khin Chung, Director, State Security Unit, Sarawak, Malaysia
- Franz-Josef Schneiders, Head of Division, Federal Ministry of Transport and Digital Infrastructure, Germany
- Oliver Carlos G. Odulio, VP, Head of Asset Protection & Risk Management, PLDT Inc, Philippines
- Elli Pagourtzi, Project Manager, Security for Security Studies (KEMEA), Hellenic Ministry of Interior, Greece
- Bill Hutchison, Honorary Professor, Security Research Institute, Edith Cowan University, Australia
- Dato' Dr. Haji Amirudin Bin Abdul Wahab, Chief Executive Officer, CyberSecurity Malaysia
- Bill Bailey, Regional Director Australasia, International Association of CIP Professionals (IACIPP), Australia
- Nur Iylia Roslan, Researcher, Cybersecurity Malaysia
- Senior Representative, Cyber Security Centre, Universiti Pertahanan Nasional Malaysia
- Senior Representative, Sarawak Energy, Malaysia
- Norhamadi bin Ja'affar, Senior Executive, CyberSecurity Malaysia

For full conference programme visit www.cip-asia.com

Owned & Organised by:

TORCH KNM MEDIA

Media Partners:

World Security-index.com WORLD SECURITY REPORT

Supporting Organisations:

KeTTHA KEMENTERIAN TENAGA, TEKNOLOGI HIJAU DAN AIR
International Association of CIP Professionals
sains Envision. Innovate. Advance
NS&RC
SPF

# FLORIDA: WHAT PRICE TOO HIGH?

As another US school suffers the appalling human tragedy of a mass shooting, it would be strange if I were not to mention it in this month's issue. But the reality is, much of what I would say on the subject has already been said after previous shootings and nothing's changed.

One can only wonder at the useless platitudes offered by President Trump and other politicians, who talk about "no teacher, no child should ever be in danger in an American school" and that "no child is alone, we will protect you" but then in an astonishing piece of deflection, switches the conversation and blame to the need to tackle mental health issues in the US. As if it is mental health that killed 17 people and injured 15 others and not a 'troubled' individual armed with a legally obtained AR-15 assault rifle, one of the world's most efficient killing machines.

In a sort of 'Emperors new clothes' moment politicians and gun supporters alike indulge in a mass self-delusion, where they ignore all statistics and kid themselves that it is not the availability of guns that's the problem, but that it is a social problem.

They say that if we put the proper checks in place and monitor properly individuals that are showing signs of mental health issues, then the problem will be solved. After all, Cruz was flagged up as a risk on numerous occasions.

They ignore that fact that every society around the world has problems with mental health issues, but they do not have the same problem with mass shootings. The missing element in the equation is that the mentally ill are not usually armed with assault rifles.

It also quietly ignores that fact that next year and every year after that, tens of thousands of gun owners in the US will be affected by previously undiagnosed mental health issues that may not be immediately apparent to family, friends and colleagues. Other gun owners will be angry, stressed out, jealous, fanatical or just plum mad!

The reality is that those people in the US that like their guns, will continue to come up with arguments to support gun ownership, aided by politicians that want their votes, and the mass killings continue. Only when the price becomes too high will something change, but nobody knows yet what constitutes 'too high'?

Tony Kingham
Editor

## READ THE FULL VERSION

The full version of World Security Report is available as a digital download at www.torchmarketing.co.uk/WSRMar18

www.worldsecurity-index.com

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

**Contributing Editorial:**
Neil Walker
E: neilw@torchmarketing.co.uk

**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.

K·N·M MEDIA TORCH

# Securing communications at a time of 'extreme events'

The first duty of any government is to provide for the security and safety of its citizens!

In historically, that would mean defending the population against aggressive neighbouring tribes and nations. Not much if anything would or could have been done to protect the population against natural disasters, like earthquakes, floods, famine or disease. These would be seen as acts of god, punishment for some imagined or real wrongdoings!

Today, in the technological age we have changed our view of what's possible and therefore what we expect from our governments. We now expect governments to protect us from any hazard, whether it is from this world and beyond!

Natural disasters still pose the greatest threat to life and property and sadly the world seems to have experienced plenty of those in recent years including tsunamis, floods, hurricanes galore, volcano's, volcanic ash clouds, earthquakes and pandemics.

But then of course there are what seem like more remote possibilities of 'extreme events', which could result in major global disasters that could affect everyone on the planet. They may seem more remote, but they are in fact, inevitable!

So, what are we talking about when we talk about 'extreme events'?

Meteor strikes, such as the so-called Tunguska event in Russia in 1908 that caused an explosion that knocked over an estimated 80 million trees covering 2,150 square kilometres.

More recently, in 2013 150-foot asteroid (designated D14) hurtled past the earth coming within 17,150 miles, closer than some of our own satellites. A near miss by space standards.

Whilst not big enough to cause an extinction event, had D14 hit the earth, weighing in at 143,000-ton, it would have done incredible damage, releasing the energy equivalent of 2.4 million tons of TNT and wiping out 750 square miles of territory (1,942 square kilometres).

Caught on camera and only a few hours apart from D14's fly-by, a meteor exploded spectacularly above Russia's Ural Mountains. The experts say it was a co-incidence. And we have no reason to doubt it but the real issue is that we were powerless to prevent either of them.

The most disturbing thing about Asteroid D14 is that the was only identified one year prior to it buzzing the planet. So, what other unexpected and unwelcome guest could already be on their way?

Another extreme event are so-called supervolcano's. Supervolcano's are those volcano's that have in their history had eruptions that measure 8 on the Volcanic Explosivity Index, (VEI). They are not typically the single volcanic cone, instead are usually characterized by a large caldera, or depression, that was formed during past explosive eruptions. Should they erupt they have the potential to throw in excess of one thousand cubic kilometers of volcanic debris up into the atmosphere causing massive destruction, not just in the immediate locality, but regionally and possibly even globally.

Yellowstone in the US is probably the most well-known example and is still extremely active as millions of tourists can tell you. Some scientists believe Yellowstone has been on a regular eruption cycle of around 600,000 years. The last eruption was 640,000 years ago.

VEI7 eruptions are not quite supervolcano's but are still massive and but more frequent. The Mount Tambora eruption took place in Indonesia in 1815, and as a result, 1816 became known as the 'Year Without a Summer'. Again, in Indonesia, Mount Rinjani erupted in 1257 possibly triggering a little ice age.

Then there's Campi Flegrei, under the Bay of Naples, which is the bookies favourite as the most likely to erupt. Whilst not as big as some of the others the entire caldera keeps swelling and deflating, and scientists are really not sure why. What this activity does indicate is that an active magmatic system exists and a recent scientists report in the journal Nature Communications said it could be ready for an eruption. No one can say with any certainty that it will erupt, but it's likely that it will.

That brings us neatly to tsunami's. Tsunami's are caused by events such as earthquakes like the one on 26 December 2014 killing between 230,000–280,000 people in 14 countries. The third-largest earthquake ever recorded. Other causes can be volcanic eruptions, landslides, glacier calving, meteorite impacts and other disturbances above or below water. Whilst some argue that tsunami's are not considered extreme events in themselves, but are in fact the consequence of other events….but that's just semantics. The death toll indicates otherwise.

Another scenario, is the solar flare and its big brother, a coronal mass ejection (CME).

On September 6th of this year the sun unleashed two monster solar storms, the second of which was the most powerful we've seen in more than a decade. The burst of radiation was so intense, it caused high-frequency radio blackouts across the daytime side of earth that lasted for about an hour. These solar storms can release as much energy as a billion hydrogen bombs.

But there is something that will have even more impact for us here on earth, which is the coronal mass ejection. These solar explosions propel bursts of particles and electromagnetic fluctuations into earth's atmosphere. Those fluctuations are something like an Electro Magnetic Pulse, causing electric fluctuations at ground level that could fuse conductive wires, down communications and blow out transformers in power grids. A CME's particles also have the potential to take out satellites and aircraft.

Then of course in addition to natural disasters, there's man kinds ability to create its own disasters.

Although the threat of conventional war in the developed world has receded (though not disappeared),

other threats have emerged.
As we have witnessed recently, rogue states like North Korea now poses the ability to deliver nuclear attacks via inter-continental ballistic missiles.

Global terrorists like ISIS and al-Qaeda have potential to deliver mass destruction through the use of modern technology like dirty bombs, chemical attacks, cyber-attacks, WMD and maybe one-day nuclear weapons.

Industrial disasters such as the those at Bhopal in India and Chernobyl in Russia are also obvious examples of unexpected home-grown disasters that can strike us at any time.

Then there's the cascade effect of a natural disaster causing a man-made disaster, like the earthquake that caused the tsunami that caused the Fukushima nuclear disaster.

Whatever the threat or disaster, it is the ability of the authorities to organise and move the available resources to the point of most need that is the key to managing the disaster effectively. Whether it's for search and rescue, medical assistance, shelter, sustenance or law and order; fundamental to the principle of good organisation is good reliable and resilient communications.

Good communications are taken for granted and we are increasingly dependent on them for the necessities of life, from our livelihoods to the weekly shopping delivery.

Most of those communications are being relayed over the existing Public Switched Telephone System (PSTN) infrastructure. Quite apart from all landline telephone calls, virtually all computer information is already relayed via the PSTN and the proliferation of technologies like Voice over Internet Protocol (VoIP) as a first choice for individuals and businesses will only increase our dependence on the existing infrastructure.

Few communications systems are completely reliable, they rely on a whole load of interconnections and interdependencies, as well as a power source. Communications tend to rely on other infrastructure, such as road, rail and bridges. So, flooding can cause a bridge collapse and that can cause local communications failures. These potential points of failure are often unidentified until it is too late.

In the event of a major disaster, although a complete national failure of the telecommunications system is unlikely, local communications failure or serious degradation of service within the disaster area is probable, due to damage to infrastructure, loss of power or simple overload. Mobile systems are particularly vulnerable to overload.

So here are 3 good examples of what has been done to keep the phones ringing.

Researchers then from the University of the Philippines, Electrical and Electronics Engineering Institute (UP EEEI), with support from the Department of Science and Technology (DOST), addressed this problem by developing a technology that restores basic communication services in the aftermath of disasters. The 'ROGER' System or RObust and Rapidly Deployable GSM Based Stations and Backhaul for Emergency Response System is an intervention that aims to provide emergency responders and affected communities with a reliable communication system during relief, rescue, and recovery efforts in case conventional communication channels (i.e. commercial telecommunications companies) go down. This technology is in "standby mode" in disaster-stricken area, and can be "unpacked" on site after the disaster. It is expected to provide a canopy of 2G coverage that will allow early responders with ROGER SIM cards to communicate and coordinate with one another.

The main components of the ROGER System are the IP Backhaul, the Base Station, and the Power Supply. The IP Backhaul is a point-to-point, long range wireless backhaul that links the GSM cell hoisted in the disaster-stricken area to the disaster command centre by utilizing IEEE 802.11 WiFi and TV white space (TVWS). The TVWS is an underutilized spectrum of the existing communication channel. The GSM Base Station, on hand, contains the so-called heart of the ROGER System, which is a software-defined radio (SDR) that runs on open source software and an IP-based network. It mimics the functionality of a traditional cellular/GSM base station. Simply put, the GSM Base Station provides cellular phone signal to allow calls and texts for phones with provided ROGER SIM cards. Within the ROGER network, authorized users can use their regular mobile phones to place calls to one another or to an emergency hotline. If interconnection to the commercial phone and cellular networks are still in place, users may call other people outside the ROGER network. The entire ROGER system is designed to be solar-powered, but a generator set is also set up as backup power source in case there is no enough solar energy for approximately three consecutive days. The ROGER System will be dismantled immediately once conventional GSM communication services have been restored.

Satellite communication, already used routinely by the military, is another obvious option.

To this end the Luxembourg government launched emergency.lu a Rapid Response Kit satellite communications system. The system consists of satellite infrastructure and capacity, broadband and voice communication and satellite ground terminals as well as transportation equipment. The system has already been widely deployed effectively after natural disasters around the world including during the aftermath of Hurricane Irma earlier this year. This system has been designed primarily for use in disasters overseas, but presumably could just as easily be deployed for a local disaster, if enough kits are available? However, it is not pre-positioned, so relies on the transport infrastructure to be deployed.

The UK Government believes the most likely of extreme event is in fact the solar flare or coronal mass ejection, which has the potential to damage or degrade existing terrestrial telecommunication and commercial satellite communications.

To guard against this eventuality and ensure that the UK

Government and emergency services are able to effectively respond to the situation, the UK has developed the High Integrity Telecommunications System or HITS.

HITS was developed by the UK Government's, Civil Contingencies Secretariat (CCS) in a partnership with Astrium and the UK Ministry of Defence (MOD).

The CCS is part of the UK Government's Cabinet Office and works across Government and industry to improve the ability of the UK to respond to and recover from significant emergency events.

Astrium is the prime contractor for the Skynet 5 contract with the UK Ministry of Defence. This program provides all secure voice, data, video, internet and broadcast communications for UK armed forces operating anywhere overseas.

They own and operate military hardened satellites that are resistant to any known attack and have both onboard and ground based technology to overcome the interference threat posed by high solar flare activity.

So, what is it? HITS is a secure and resilient satellite-based communications system capable of delivering secure data and telecommunications completely independently from the main UK telephone network.

The system is designed to provide telephone and internet communications to the emergency services and related agencies in the event of a national emergency when the existing landline or mobile networks are either down or seriously degraded.

It is however completely interoperable with those parts of the regular networks that are still functioning so will facilitate the break-out of calls onto other networks such as mobile phones.

It is installed at the Central Government Crisis Management Facilities, COBR, and at each of the UK's Devolved Administrations Crisis Management Centres. It is deployed at fixed sites across the UK, mainly in Police Strategic Command Centres (SCCs) because the Police usually the lead service in times of emergency.

Every HITS installation comes with a number of phones and laptops, usually three of each, as well as at least one networked printer.

In addition to the core network sites, each Police Force Area will also have at least one pre-determined fall-back location, where HITS Transportable Terminals are deployed. These fall-back locations are designed as an extra level of communication security should any of the main HITS installations be within the disaster area and so be unavailable as a result.

These Transportable Terminals can be deployed anywhere in England and Wales and will usually be driven to the relevant location although they can be carried by whatever transport is available.

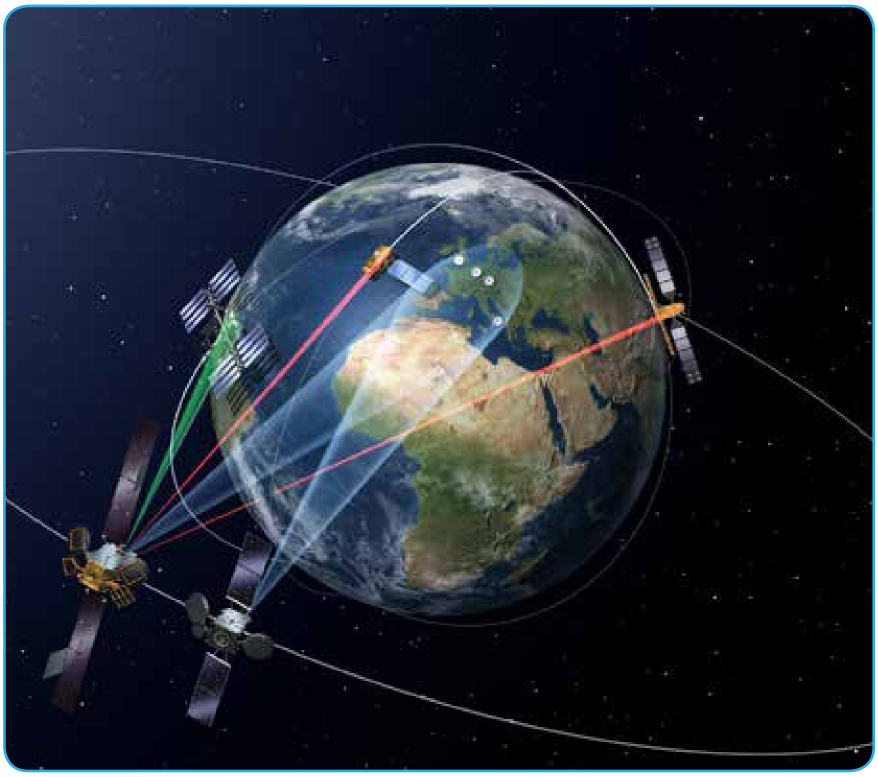
They are on call 24/7 and can be on the road within 6 hours of an emergency call out by the Cabinet Office.

Each transportable unit comes with up to 10 digital phones and laptops, so that they can effectively act as a mobile command centre wherever it's needed. They are equipped with their own generators and fuel, so are able to operate fully autonomously for up to seven days. Each of them has trained Astrium personnel on hand to support the emergency services throughout the deployment.

Whether it is satellite or GSM communication, in an 'extreme event' pre-positioning of communications equipment (and other supplies) as much as is practicable, is the key to effectiveness.

After all, if you rely on a system that depends on the transport infrastructure to get to the point of most need, haven't you already set it up to fail?

*Tony Kingham*
*Editor*



# Making Our Critical Infrastructures More Resilient: Best Practices

Today, our national critical infrastructures (CI) are more vulnerable than ever before and high-impact disruptions are no more rare or and low-probability events. In that regard, CIP (Critical Infrastructure Protection) discipline has already became one of the leading topics in the policy makers' agenda and any threats against our CI systems, which could be considered as the "lifelines" of the nations, are perceived as '"threats to national security". In that sense, with respect to evolving and sophisticating dynamics of natural and man-made threats, it is undeniable that almost every state has started to implement its national CIP policies.

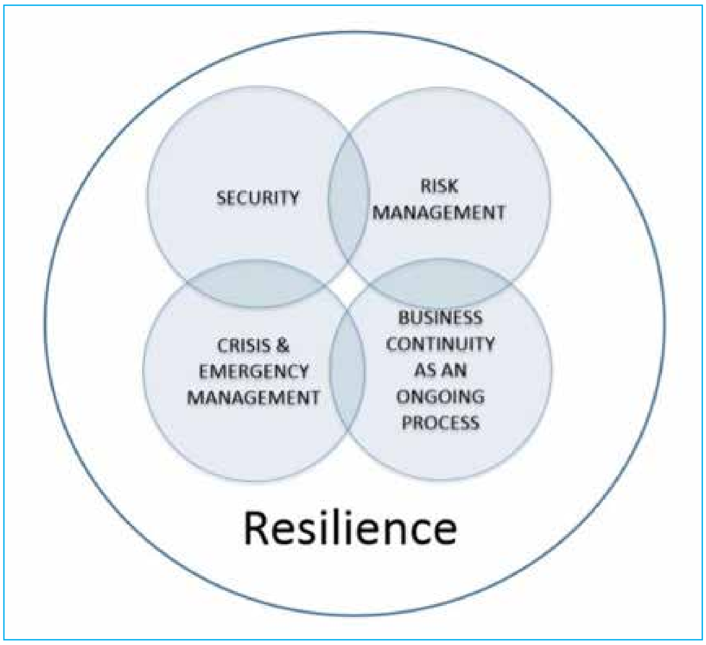
Despite its criticality, the concept of "Critical Infrastructure Resilience" (CIR) had been mostly underestimated and only in the last five years it gained much more attention especially in the field of homeland security and civil protection practices. Especially as a response to the new emerging threats in the "age of uncertainty", it is possible to observe that many national security strategies have already adopted risk based "all hazards" approach with a special focus on the concept of "resiliency".

Nonetheless, it is possible to observe that in general infrastructure planning requirements little references to resilience was made and there is a lack of supporting guidelines which provides a holistic overview how to achieve "more resilient critical infrastructures". Besides, governments and policy makers generally facing challenges regarding the complex bureaucratic and cross-jurisdictional processes, intensive data requirements, limited technical capacity in planning and investing to the infrastructure resiliency improvement plans.

## Two Distinct Concepts: CIR and CIP

It shall be highlighted that even though both CIP and CIR policies are parts of integrated risk management approaches and strategies, these two concepts are distinct. According to the policy paper released by Italian Association of Critical Infrastructures Experts (AIIC), since there is the tendency to confuse the concepts like security, resilience or risk management, resiliency could be imagined as a "multifaceted problem"

Figure-1: All Influences All Perspective- A Multifaceted Problem


SECURITY
RISK MANAGEMENT
CRISIS & EMERGENCY MANAGEMENT
BUSINESS CONTINUITY AS AN ONGOING PROCESS
Resilience

### Defining "Resilience"

Resiliency shall be firstly handled as a process not a single outcome. Additionally, since there has been no consensus how to "measure the resiliency", the concept has also various definitions and it is generally associated with "the ability to bounce or spring back into shape after being pressed or stretched." In other words, it refers to the ability of a system to resist, absorb, recover from a negative affect and successfully adapt to changing environment. In general, when this definition and understanding is handled with CIP policies, being resilient could be considered with "the capability to cope with severe disruptions which would have negatively impact CI that the CIR framework should operate in a multidisciplinary nature and address technical (logical and physical), organizational, social and economic dimensions of the infrastructures."

According to the experts, similar to CIP policies, CIR policies also vary according to nations. For instance, in US, PPD-21 (Presidential Policy Directive -- Critical Infrastructure Security and Resilience) defines resiliency as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incident." On the other hand, in UK's Sector Resilience Plan for Critical Infrastructure 2010 document defines the resilience as: "the ability of a system or organization to withstand and recover from adversary." Another point could be added that for example, while the national policies in US and Australia recognize CIP as an enabler of CIR by considering "resilience" alongside with the protection and put a special emphasis on the "voluntary" approach, European policies mostly focus on regulatory measures. (1)

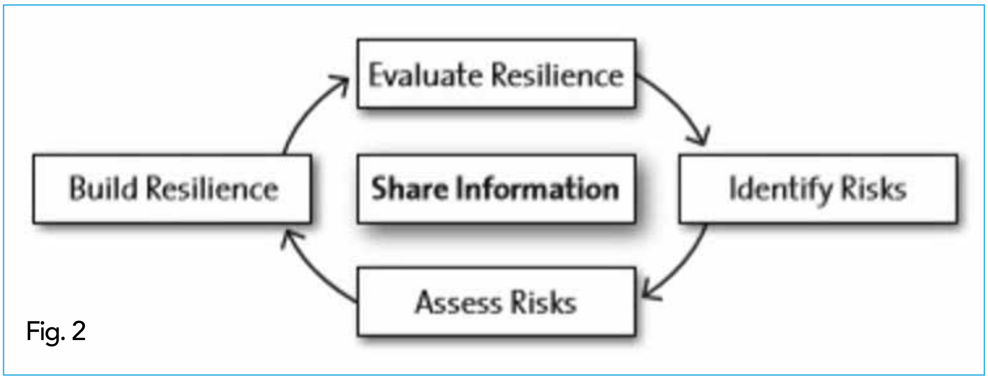


Fig. 2

Figure-2: Resilience Cycle for the Infrastructure Owner

### Designing the Framework

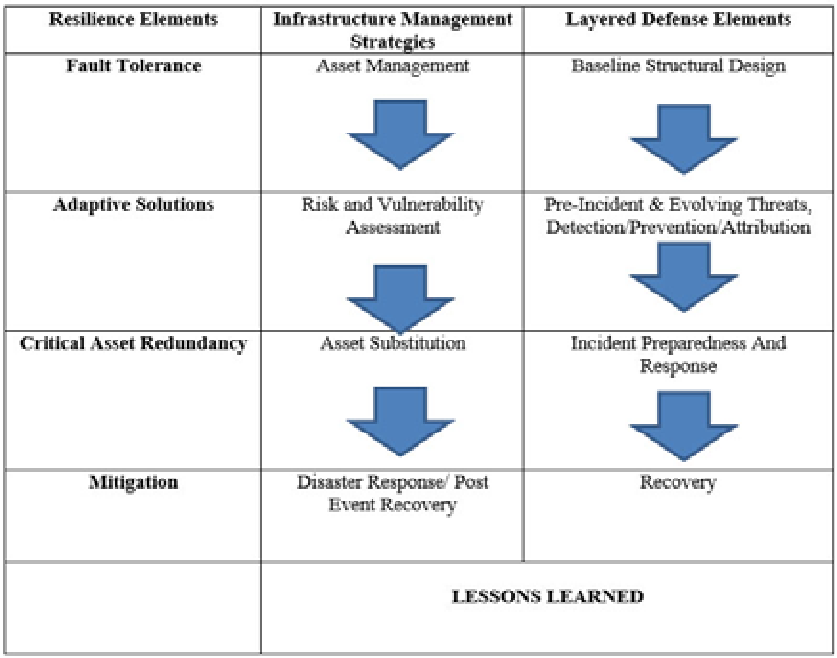
According to the experts, since resiliency is not a static concept and derived from principals of multi-layered defense and risk mitigation, the resiliency framework should be based on an "adaptive approach" which is capable to respond today's complex and dynamic risk environment. According to a well-known resilience specialist Stephen Flynn, resiliency consists of four outcomes: Robustness, resourcefulness, rapid recoverability and adaptability. Very similarly, Volpa's white paper (Figure-3) about the "Infrastructure Resiliency: A Risk-Based Framework" states that a resilient infrastructure should be/have:

- Robust and Fault-tolerant

- Adaptable, aware and resourceful

- Functional flexibility and layers of redundant safeguards

- Response and recovery capability for mitigation of event consequences



| Resilience Elements | Infrastructure Management Strategies | Layered Defense Elements |
|---|---|---|
| Fault Tolerance | Asset Management<br>↓ | Baseline Structural Design<br>↓ |
| Adaptive Solutions | Risk and Vulnerability Assessment<br>↓ | Pre-Incident & Evolving Threats, Detection/Prevention/Attribution<br>↓ |
| Critical Asset Redundancy | Asset Substitution<br>↓ | Incident Preparedness And Response<br>↓ |
| Mitigation | Disaster Response/ Post Event Recovery | Recovery |
| | LESSONS LEARNED | |

Fig. 3

Resource: Volpa, Infrastructure Resiliency: A Risk-Based Framework, Access

Figure-3: Infrastructure Resiliency Framework

### Best Practices and Recommendations for CIR policies

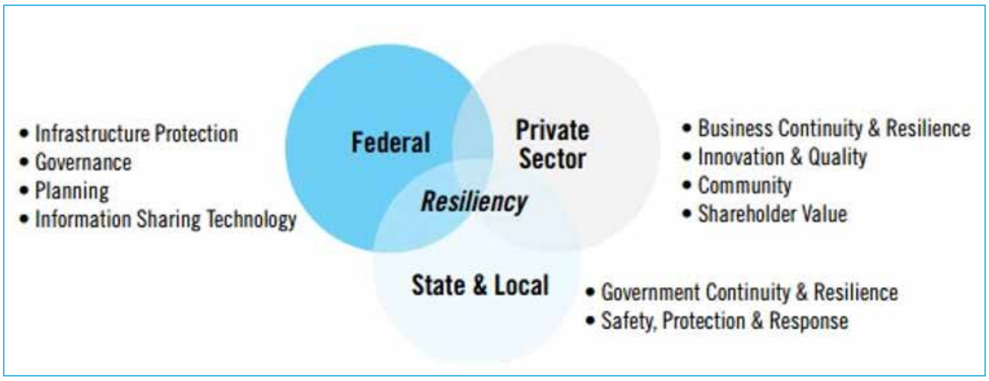
As it was discussed previously, the most challenging part regarding the planning and investing for more resilient critical infrastructures is to identify a comprehensive and globally accepted guideline for implementing best practices. Nonetheless, it is possible to illustrate some recommendations and practical guidelines based on the current approaches.

For instance, a set of five principals were introduced by Deloitte's report on "Building Resilient Infrastructure" for infrastructure planning as: Identifying the disaster risks, applying robust methodologies for Cost and Benefit Analysis, coordinating-centralizing and

making the available data for critical data and information, strengthening approval processes and embedding ongoing monitoring of resilience. (2) Besides a few other key points and actionable items in improving the CIR policies are worth to be mentioned:

- Establishing an Effective Public Private Partnership (PPP): In most of the states strengthening the resiliency of critical infrastructure is seemed to be a shared responsibility among public and private sector authorities. In that sense, the business-government partnership remains to be an effective platform especially for exchanging information. In some countries like US or in the European Union level, effective platforms for PPP's have already initiated. For example, in the European Union level, European Public Private Partnership for Resilience (EP3R) which is engaging with National PPP's in building CIR policies can be illustrated.

Figure 4- : Diagram of Infrastructure Stakeholders Involved in Resilience


• Infrastructure Protection
• Governance
• Planning
• Information Sharing Technology
Federal
Private Sector
Resiliency
State & Local
• Business Continuity & Resilience
• Innovation & Quality
• Community
• Shareholder Value
• Government Continuity & Resilience
• Safety, Protection & Response

- Encouraging Information Sharing: As being a useful outcome and the principal value of the PPP's, information sharing is a crucial component of CIR policies which facilitates more informed decision making on how best to protect CI.

Besides, in defending CI, by sharing useful information which shall be distributed in a proper methodology (for ex: traffic light protocols), it is possible to identify critical trends and incidents which could be transform into the actionable recommendations for all actors. Nevertheless, the opportunities and challenges of information sharing process shall be calculated and its "using guideline" should be introduced by policy makers. For instance, establishing ground rules for information exchange and identifying what information could not be shared outside of the partnership shall be determined in advance. Like PPP structure, some countries like US have already implemented information sharing platforms and methodologies. For instance, The Trusted Information Sharing Network (TISN) for CIR policies was established by Australian Government in 2003.

Finally, in addition to all technical and technological aspects, it shall be kept in mind "cultural" aspects play a crucial role in building national CIR policies and infrastructure problems are also "social". Thus, policy makers should calculate cultural and social dynamics in building CIR policies whether for example they will be voluntary or regulatory to participate. Besides, understanding the networks and going beyond the theoretical aspect by practicing operational resilience should be considered as the cornerstones for achieving a future resilient infrastructure.

*Ms.Ayhan Gücüyener is a Researcher and Regional Director of the International Association of CIP Professionals (IACIPP)*

# Business interruption and cyber incidents dominate risk landscape for companies of all sizes and sectors in 2018

They take aim at the backbone of the connected economy and, when they strike, can jeopardize the success, or even the existence, of companies of every size and sector. Business interruption (# 1 with 42% of responses / # 1 in 2017) and Cyber incidents (# 2 with 40% of responses, up from # 3 in 2017) are this year's top business risks globally, according to the Allianz Risk Barometer 2018.

Larger losses from natural catastrophes (# 3 with 30% of responses, up from # 4 in 2017) are also a rising concern for businesses, with the record-breaking 2017 disaster year also ensuring Climate change and increasing volatility of weather (# 10) appears in the top 10 most important risks for the first time. Meanwhile, the risk impact of New technologies (# 7 2018 / # 10 2017) is one of the biggest climbers, as companies recognize innovations such as artificial intelligence or autonomous mobility could create new liabilities and larger-scale losses, as well as opportunities, in future. Conversely, businesses are less worried about Market developments (# 4 2018 / # 2 2017) than 12 months ago.

These are the key findings of the seventh Allianz Risk Barometer, which is published annually by Allianz Global Corporate & Specialty (AGCS).The 2018 report is based on the insight of a record 1,911 risk experts from 80 countries.

"For the first time, business interruption and cyber risk are neck-and-neck in the Allianz Risk Barometer and these risks are increasingly interlinked," says Chris Fischer Hirs, Chief Executive Officer, AGCS. "Whether resulting from attacks such as WannaCry, or more frequently, system failures, cyber incidents are now a major cause of business interruption for today's networked companies whose primary assets are often data, service platforms or their groups of customers and suppliers. However, last year's severe natural disasters remind us that the impact of perennial perils shouldn't be underestimated either. Risk managers face a highly complex and volatile environment of both traditional business risks and new technology challenges in future."

## New business interruption triggers emerging

Business interruption (BI) is the most important risk for the sixth year in a row, ranking top in 13 countries and the Europe, Asia Pacific, and Africa & Middle East regions. No business is too small to be impacted. Companies face an increasing number of scenarios, ranging from traditional exposures, such as fire, natural disasters and supply chain disruption, to new triggers stemming from digitalization and interconnectedness that typically come without physical damage, but with high financial loss. Breakdown of core IT systems, terrorism or political violence events, product quality incidents or an unexpected regulatory change can bring businesses to a temporary or prolonged standstill with a devastating effect on revenues.

For the first time, cyber incidents also rank as the most feared BI trigger, according to businesses and risk experts, with BI also considered the largest loss driver after a cyber incident. Cyber risk modeler Cyence, which partners with AGCS and is now part of Guidewire Software, estimates that the average cost impact of a cloud outage lasting more than 12 hours for companies in the financial, healthcare and retail sectors could total $850 mn in North America and $700 mn in Europe.

BI also ranks as the second most underestimated risk in the Allianz Risk Barometer. "Businesses can be surprised about the actual cause, scope and financial impact of a disruption and underestimate the complexity of 'getting back to business'. They should continuously fine tune their emergency and business continuity plans to reflect the new BI environment and adequately consider the rising cyber BI threat," says Volker Muench, Global Property and BI expert, AGCS.

### Cyber risks continue to evolve

Cyber incidents continues its upward trend in the Allianz Risk Barometer. Five years ago it ranked # 15. In 2018 it is # 2. Multiple threats such as data breaches, network liability, hacker attacks or cyber BI, ensure it is the top business risk in 11 surveyed countries and the Americas region and # 2 in Europe and Asia Pacific. It also ranks as the most underestimated risk and the major long-term peril.

Recent events such as the WannaCry and Petya ransomware attacks brought significant financial losses to a large number of businesses. Others, such as the Mirai botnet, the largest-ever distributed denial of service (DDoS) attack on major internet platforms and services in Europe and North America, at the end of 2016, demonstrate the interconnectedness of risks and shared reliance on common internet infrastructure and service providers. On an individual level, recently identified security flaws in computer chips in nearly every modern device reveal the cyber vulnerability of modern societies. The potential for so-called "cyber hurricane" events to occur, where hackers disrupt larger numbers of companies by targeting common infrastructure dependencies, will continue to grow in 2018.

Meanwhile, privacy risk is back in the spotlight following huge data breaches in the US. The introduction of the General Data Protection Regulation (GDPR) across Europe in May 2018 will intensify scrutiny further, bringing the prospect of more, and larger, fines for businesses who do not comply. Time is running out to be GDPR-ready. "Compared to the US where privacy laws have been strict for decades and cyber security and privacy regulation is continuously evolving, firms in Europe now also have to prepare for tougher liabilities and notification requirements. Many businesses will quickly realize that privacy issues can create hard costs once the GDPR is fully implemented," says AGCS's Global Head of Cyber, Emy Donavan. "Past experience has shown that a company's response to a cyber crisis, such as a breach, has a direct impact on the cost, as well as on a company's reputation and market value. This will become even more the case under the GDPR."

Cyber threats also vary according to company size or industry. "Small companies are likely to be crippled if hit with a ransomware attack, while larger firms are targets of a greater range of threats, such as the DDoS attacks which can overwhelm systems," says Donavan.

Allianz Risk Barometer results show that awareness of the cyber threat is soaring among small- and medium-sized businesses, with a significant jump from # 6 to # 2 for small companies and from # 3 to # 1 for medium-sized companies. With regard to sector exposure, cyber incidents rank top in the Entertainment & Media, Financial Services, Technology and Telecommunications industries.

### Weather and technology risk on the rise

After a record-breaking $135 bn in insured losses from natural catastrophes alone in 2017[1] – the highest ever – driven by hurricanes Harvey, Irma and Maria in the United States and the Caribbean, Natural catastrophes returns to the top three business risks globally. "The impact of natural catastrophes goes far beyond the physical damage to structures in the affected areas. As industries become leaner and more connected, natural catastrophes can disrupt a large variety of sectors that might not seem directly affected at first glance around the world," says Ali Shahkarami, Head of Catastrophe Risk Research, AGCS.

Respondents fear 2017 could be a harbinger of increasing intensity and frequency of natural hazards. Climate change/increasing weather volatility is a new entrant in the Risk Barometer top 10 in 2018 and the loss potential for businesses is further exacerbated by rapid urbanization in coastal areas.

Meanwhile, the risk impact of New technologies is one of the big movers in the Allianz Risk Barometer, up to # 7 from # 10. It also ranks as the second top risk for the long-term future after cyber incidents, with which it is closely interlinked. Vulnerability of automated or even autonomous or self-learning machines to failure or malicious cyber acts, such as extortion or espionage, will increase in future and could have a significant impact if critical infrastructure, such as IT networks or power supply, are involved.

"Although there may be fewer smaller losses due to automation and monitoring minimizing the human error factor, this may be replaced by the potential for large-scale losses, once an incident happens," explains Michael Bruch, Head of Emerging Trends, AGCS. "Businesses also have to prepare for new risks and liabilities as responsibilities shift from human to machine, and therefore to the manufacturer or software supplier. Assignment and coverage of liability will become much more challenging in future."

# ‘What has been’ and what the future may hold?

John Donlon
Chairman
International Association of CIP Professionals
(IACIPP)

2018 is well underway and hopefully will be a year where we will all see a dramatic reduction in the use of extreme violence carried out through terrorist activity.

The start of a New Year is obviously a good time to reflect on ‘what has been’ and what the future may hold both professionally and personally and this is something that we within the IACIPP have been considering in the context of Critical Infrastructure and Information. What will be the new challenges to be faced and what might we see in terms of new innovations, from both a public and private perspective?

The CIPRNA conference held in December at the Kennedy Space Center in Orlando hosted a broad range of presenters from Government Agencies, Academia and the Private Sector all providing an insight into the complexities of future challenges whether they be from developing physical security, natural disasters or cyber activity.

The threat of physical attacks is unlikely to subside but as may have been expected, the topic generating the most significant debates were those around cyber and it’s use as a disruptive and destructive tool against our infrastructure and information.

Cyber is already becoming increasingly attractive as such attacks know no borders, physical or virtual, and as we all know are capable of causing serious harm.  By way of example, in May 2017 a strain of ransomware called Wannacry spread around the world, breaching the defences of numerous targets (It is estimated that over 200,000 computers in 150 countries were attacked) including public utilities and large corporations. Notably, the attack temporarily crippled National Health Service hospitals and facilities in the United Kingdom, disabling emergency rooms, delaying vital medical procedures and creating chaos for many British patients.

2018 is predicted to see even more sophisticated types of ransomware attacks and the Defence Secretary for the United Kingdom, Gavin Williamson, has warned recently that State actors such as Russia could launch a cyberattack targeting the UK’s critical energy infrastructure. The Foreign minister for UK cyber security, Lord Ahmed of Wimbledon, has also spoken out about the involvement of Russian military in malicious cyber activity alluding to the fact that UK intelligence agencies have discovered evidence indicating their involvement (UK Media February 2018).

State actors are obviously not the only concern. Recent press reports clearly show that as Islamic State continues to lose physical territory, the group’s supporters are taking the battlefield to cyberspace, targeting critical infrastructure and online Western websites. During 2017, many Western websites, and especially government sites, were hacked by Caliphate Cyber Ghosts, a pro-Islamic State hacktivist group. While it is believed that this group and others still have poor technical skills, they are continually struggling to improve their cyber capabilities

Such are the concerns of governments internationally that we have seen a call for those operating our critical infrastructure to continue to develop robust safeguards to protect themselves from cyberattacks. In the UK those involved in critical industry and essential services have been warned that they may face fines and sanctions if their cybersecurity preparations are not up to standard as the government implements the Network and Information Systems (NIS) Directive.

It is likely that making organisations pay up for failing to meet cybersecurity standards would only be a “last resort” and the expectation is voluntary uptake of the new rules before they come into effect on the 10th May. To help support industry the UK’s National Cyber Security Centre (NCSC) has also published detailed guidance on the security measures which will assist organisations to meet the compliance standard.

The bottom line here is, that on a global scale, we want our essential services and infrastructure to be primed and ready to tackle cyberattacks and be resilient against major disruption to services. If that means a more robust stance from governments then that, in my opinion, is not a bad thing.

# To Protect and Protect Again

Vehicle Security Barriers are becoming a recognised sight in our cities around the world.

In January 2018, the Mayor of New York, Bill de Blasio and the City's Security Infrastructure Working Group announced plans to bring permanent perimeter barriers, or bollards, to high-profile sites and to create a process to streamline their design and construction. With funds exceeding $14 million for permanent bollards in Time Square and in excess of $50 million to commence the broader rollout of new protective measures in phases.

Mayor de Blasio said, "In 2017, New Yorkers witnessed the horrible capacity of people willing to do us harm, whether it was in our subways, on our bike paths or in Times Square. But we will not be cowed and our expanded investment today in barriers and bollards in our public spaces underscores our resolve in keeping New York City safe from future attacks. In this new year, we can and will protect our iconic public spaces while New Yorkers go on living our lives, including by hosting a record number of tourists."

"These additional safety bollards will allow New Yorkers and visitors to be more secure at landmark locations and other sites throughout our City," said Police Commissioner James P. O'Neill.

And with vehicles seemingly becoming the weapon of choice for terrorists, the need to protect citizens from "people willing to do us harm" has dawned on most large cities, leaving many still trying to find the best way to protect their citizens.

Admittedly in many cases, it seems to be "after the horse has bolted" so to speak.

In 2016 a lorry was driven into crowds celebrating Bastille Day in Nice, killing 87 people and injuring 458. This was an awful, cowardly and devastating attack that had a huge impact on so many lives. The stark reality is however, after two previous vehicle attacks in France, if there had had been tougher security measures in place, rather than an increased police presence, and a plastic temporary barrier, then many of those citizens would still be alive today.

Reacting to these devastating events, Metropolis Nice Côte d'Azur decided to install a safety barrier along the

Promenade des Anglais.

The new barrier, or vehicle incursion prevention system, MacSafe, was tailor-made for the Promenade des Anglais by Maccaferri and J&S Franklin. It was inaugurated in July 2017. It is crash test rated to stop a 19-tonne truck travelling at 50km/h and impacting at 20°, equivalent to the vehicle used by the terrorist in Nice in 2016 and can withstand two successive impacts. The system is also accredited by the UIAU (University of Venice).

The MacSafe system consists of two high tensile steel cables supported on tubular steel posts and anchored at each end with our patented energy dissipation system. The posts are secured to ground foundations and all external fixings are designed to prevent them being easily removed.

The force of the vehicle impact is distributed through the cables and posts and absorbed within the patented energy dissipaters. The energy is absorbed through compressive deformation and not by friction. This ensures better and more reliable performance throughout the long-life of the barrier.

On the 19th December 2016, a truck was deliberately driven into the Christmas market next to the Kaiser Wilhelm Memorial Church at Breitscheidplatz in Berlin,killing 12 people and injuring 56 others. One year on, and the Christmas Market in Berlin is protected by large concrete barriers, armed police patrols and stop and search checks.

January 2017 – In Melbourne, 6 people were killed and 37 injured when a car sped down a footpath crashing into pedestrians, by June 2017 $10 million had been allocated, and temporary concrete barricades and bollards had been installed around the City of Sydney.

In January 2018, the City of Gold Coast began installing heavy duty retractable bollards capable of repelling the force of a large heavy goods vehicle. They had previously resolved to spend $515,000 on bollards which met the Australian standard, but on the advice of the QPS Commonwealth Games security adviser, it was recommended that the bollards comply with a European standard bringing the cost of the project to $1.095 million.

Las Vegas, plan to have their existing 800 bollards, updated to some 7,000 by the end of 2018, in an effort to increase the safety of those walking The Strip in Sin City.

However, some Cities are still concerned about the aesthetics of concrete bollards on their historic cities, a case of balancing security over protecting tourism.

Take for instance, Barcelona in Spain.

On the 17th August 2017, a van was driven into pedestrians strolling along Las Ramblas, in Barcelona, killing 13 people and injuring at least another 130. Advice was given that bollards were needed, warnings of impeding threats were given, and yet, the action taken was to increase policing levels on the streets. Now, thankfully, there are a few bollards and increased police on the streets, and going forward they are "studying the possibility of installing physical barriers to prevent further attacks with vehicles"

In London on 22nd March, 2017, a car was driven into pedestrians on Westminster Bridge, killing 5 people and injuring 49 others. The driver also stabbed a policeman to death. Again, in London, on 3rd June 2017, a van was driven at pedestrians in the London Bridge Area. Three attackers began stabbing people, before being shot by police. 8 people died. 48 were injured, 21 critically. Controversially previously installed "Guard Rails" had been removed from London's Streets in an effort to protect cyclists and make the Capital more "attractive". Although Guard Rails would not have stopped either London attack they could have limited the results. However, today, protective barriers are erected on Thames bridges and from London's experience of previous terrorist activities (IRA) there are very few buildings or indeed public spaces that don't have "counter-terrorism" design inbuilt.

The UK Government has produced

*Mayor de Blasio Announces Extensive Plan to Install Security Bollards to Protect New Yorkers, Tourists and City's Infrastructure*

a 174 page guide, Crowded Places Guidance, that highlights the threat as a vehicle being used as a weapon, but also highlights that these threats can be "mitigated by installing physical measures (including blending into the landscape or streetscape) which may be passive (static) or active (security controlled). These measures can be installed either on a permanent or temporary basis. All such measures should meet appropriate standards in terms of their vehicle impact performance, design and installation."

Vehicle Security Barriers, need not be ugly concrete monstrosities. Nor do they need to be concrete lumps that need huge lifting gear to place them. They can be totally inconspicuous, letting everyday life continue and forgetting they are there, or full on "in your face" shouting a warning to would be terrorists that this area is safe.

They come in many guises;

Active Retractable Bollard, like the Avon SB970CR Scimitar Security Bollard which provides a high level of security against unauthorised vehicle access without the need for an outwardly aggressive appearance.

The PAS 68 impact tested bollard is an active bollard that is hydraulically operated, it stands 1000mm in its fully raised position and retracts to road level to allow authorised vehicles access.

Passive Static Bollard, like The Heald Mantis from Ross Technology. Their PAS 68 shallow mount fixed bollards are designed with a unique shape for contemporary style and architectural appeal. It offers a high crash rating, while still providing a shallow excavation depth of only 10" and structural frame with integrated rebar.

Planters, like the PAS68 Street Planters from Securiscape, which have an attractive floral display whilst cleverly acting as a security barrier. These planters can be installed quickly and are sited to allow pedestrians to pass through while vehicles can't, but due to intelligent design, incorporating a surface mounted, reinforced structure which can stop a vehicle if it is used as a battering ram.

Street Furniture, like the Monoscape Igneo PAS rated seat, by Marshals. The Igneo seat has been successfully crash tested in accordance with PAS 68 using a 7.5 tonne vehicle travelling at 40mph. It can be specified in any length, using any number of modules. It is manufactured from Marshalls' fibre reinforced precast concrete and further strengthened by RhinoGuard technology, which is cast into the individual modules.

But if none of that appeals, then there are many Landscaping options, including, ditches, bunds and berms.

DefenCell by J&S Franklin, is a lightweight geotextile welded mesh gabion that once filled with locally available materials, can be incorporated into security measures for public places and protection. Filled and stacked, these gabions can be covered and planted, maintaining the aesthetic and environmental considerations of high profile or sensitive locations.

Sadly, people with "evil intent" are a fact of life. Which makes Vehicle Security Barriers a permanent part of ourcity landscapes. So whether hidden or in plain sight they will be there be to Protect and Protect again.

Europol’s European Cybercrime Centre (EC3) supported the countries in their efforts to identify EU citizens by providing analytical support and by facilitating information exchange in the framework of the Joint Cybercrime Action Taskforce, hosted at Europol’s headquarters in The Hague.

The OSCE, because of its comprehensive approach to security, is well positioned to support States on their national Security Sector Governance and Reform programmes, said speakers at today’s joint meeting of the Forum for Security Co-operation and Permanent Council in Vienna.

The discussions focused on what the OSCE can do to continue to strengthen the effectiveness and coherence of its approach in assisting participating States in their nationally-led governance and reform efforts in the security sector.

The joint meeting was opened by Ambassador Alessandro Azzoni, Chairperson of the OSCE Permanent Council and Italy’s Permanent Representative to the OSCE, and Ambassador Radomír Boháč, Chairperson of the Forum for Security Co-operation and Slovakia’s Permanent Representative to the OSCE.

Azzoni highlighted Italy’s involvement in the OSCE Group of Friends of Security Sector Governance and Reform, a topic which is receiving particular attention by Italy’s current OSCE Chairmanship.

OSCE Secretary Thomas Greminger said that the concept of Security Sector Governance and Reform has much to offer when it comes to strengthening the OSCE’s ability to effectively prevent and respond to complex and interconnected modern-day challenges.

## EU plans to create a data base to enable EU countries to exchange non-EU citizens’ criminal records faster

The Civil Liberties Committee approved plans on Thursday to create a new centralised data base on third country nationals to complement the European Criminal Records Information System (ECRIS), which EU countries already use to exchange information on previous convictions of EU citizens.

The ECRIS Third Country National (TCN) system, will:

- enable national authorities to establish quickly whether any EU member state holds criminal records on a non-EU citizen,

- contain data such as names, addresses, fingerprints and facial images (which, however, may only be used to confirm the identity of a non-EU national who has been identified based on other data), and comply with EU data security and data protection rules.

MEPs stressed that, in addition to judges and prosecutors, Europol, Eurojust and the future European Public Prosecutor’s Office should also have access to the ECRIS-TCN system.

MEPs see this system an important cross-border crime fighting tool for European prosecutors, judges and police forces, who currently often rely solely on data available from their own national criminal record systems.

Rapporteur Daniel Dalton (ECR, UK) said: “The fast, reliable exchange of information is key in the fight against crime at all levels. This measure will close the loophole allowing third country nationals to hide their criminal records, while protecting peoples’ rights and information.”

These negotiations, which can start as soon as Parliament as a whole gives its green light, will also include talks on a related directive for which Parliament has already given its negotiators a mandate.

ECRIS was put in place in 2012 to exchange information on criminal convictions in the EU. However, using the current system to check the criminal records of a non-EU citizen is cumbersome and inefficient. According to the European Commission, national authorities have used information available in other countries’ criminal records only in less than five percent of conviction cases of third country nationals, between 2010 and 2014.

## INTERPOL and UN chiefs address global security issues

With an increased risk of foreign fighters returning home or joining other conflicts following the liberation of Da’esh-held territories transforming the global threat landscape, international security was high on the agenda during discussions between the heads of the United Nations (UN) and INTERPOL.

In their first meeting, Secretaries General António Guterres and Jürgen Stock addressed areas of common concern where the two organizations can further streamline and strengthen their cooperation for the benefit of their member countries.

Areas for enhanced collaboration have been identified in a number of UN resolutions, including protecting critical infrastructure, preventing foreign terrorist fighter travel as well as combating all forms of transnational crime such as maritime piracy, human trafficking and drug smuggling.

In addition, there are currently nearly 600 valid INTERPOL-UN Special Notices for entities and individuals who are the targets of UN Security Council Sanctions Committees.

Secretary General Stock said today’s complex security landscape combined with increased pressure on resources highlighted the value of INTERPOL’s communications system and databases as a ‘global early warning system’.

“We are all too well aware of the threats which face us, and indeed for the foreseeable future, these threats are increasing rather than diminishing.

“The partnership between INTERPOL and the UN provides a unified response in supporting law enforcement and the maintenance of international peace and security,” said Mr Stock.

Among the tens of millions of pieces of data held in INTERPOL’s global databases accessible to law enforcement across its 192 member countries, are more than 43,000 foreign terrorist profiles.

In 2017, law enforcement officers around the world conducted some 4.5 billion searches against INTERPOL’s databases resulting in one million ‘hits’, with each match potentially a key piece in an investigation.

INTERPOL has a long history of cooperation with the UN which was  formalized in a 1997 agreement.  The Office of the Special Representative of INTERPOL to the United Nations in New York was opened in 2004, which has further strengthened the relationship between the two organizations.

## INTERPOL facial recognition nets most wanted murder fugitive

Police in Buenos Aires have arrested an internationally wanted murder suspect after his image was identified as a likely match by INTERPOL’s facial recognition unit.

Kristian Danev, a Slovak national aged 33, is wanted internationally by Czech authorities under an INTERPOL Red Notice following a murder ten years ago.

As part of an investigation by police in Argentina, INTERPOL’s National Central Bureau in Buenos Aires submitted images of the suspect to INTERPOL’s General Secretariat headquarters for comparison against records in its facial recognition database.

After the search result came up as a potential match, police in Argentina detained the suspect for further questioning, resulting in the suspect confirming his identity.

“In less than 48 hours, INTERPOL’s global police cooperation platform helped locate, identify and arrest an international fugitive who had evaded justice for a decade,” said Harald Arm, Director of Operational Support and Analysis at INTERPOL.

“This illustrates the fundamental role of INTERPOL’s policing capabilities and forensic data in international police investigations. We need to ensure that vital information moves faster than fugitives,” added Mr Arm.

INTERPOL’s Fugitive Investigative Support unit was supported by its Command and Coordination Centre and its Regional Bureau in Buenos Aires. They worked closely together with the INTERPOL National Central Bureaus in Bratislava, Buenos Aires and Prague to ensure the quick exchange of information on the case.

Authorities in Argentina are now holding Kristian Danev subject to his extradition to the Czech Republic.

INTERPOL launched its facial recognition biometric service in November 2016. It already contains more than 44,000 images from 137 countries.

Police forces across the globe use INTERPOL’s facial recognition tool daily to make connections between criminals and crime scenes, identify fugitives and missing persons or to compare mugshots.

## Europol, Thomson Reuters and the World Economic Forum Launch Coalition to Fight Financial Crime and Modern Slavery

The fight against financial crime and modern slavery has been given fresh impetus at the Annual Meeting of the World Economic Forum with the launch of a new public/private coalition comprising Europol, Thomson Reuters and the World Economic Forum. The perpetration of financial crimes has a devastating socio-economic impact on individuals and communities around the world. Every year, the estimated $2.4 trillion in proceeds from this and other causes of human misery such as forced prostitution, terrorism and drug trafficking will be laundered through the world's financial markets and banking systems. Despite substantial amounts of human and economic capital deployed at stopping financial crime, less than 1% is detected and confiscated via existing mechanisms.

The amount of money laundered globally in one year is estimated by the United Nations to account for 2-5% of global GDP (around $2 trillion). Criminal networks are becoming increasingly connected, global and technologically sophisticated. Against this backdrop, additional collective action must be brought to bear to combat financial crime in order to achieve the Sustainable Development Goals target 8.7 to eradicate forced labour, end modern slavery and human trafficking, and secure the prohibition and elimination of the worst forms of child labour. Public-private cooperation is key for the identification and implementation of innovative strategies that address this challenge while avoiding unintended consequences, such as a further retrenchment in access to the global financial system for individuals and institutions. The coalition, which is seeking additional members, will work to mobilise and influence decisions-makers at the highest levels to achieve the following objectives:

- raise awareness among global leaders on the topic of financial crime as a critical challenge with grave financial and human consequences
- promote more effective information sharing between public and private entities on a coordinated, global level
- establish enhanced processes to share compliance best practice and approaches to more robust customer due diligence

Rob Wainwright, Executive Director of EUROPOL, said: "Europol launched in December 2017 the first transnational financial information sharing mechanism, the Europol Financial Intelligence Public Private Partnership. All the members of this partnership, comprising experts from financial institutions and competent authorities, have actively started to share financial intelligence in a trusted environment. Ultimately, our objective is to facilitate, in accordance with the applicable domestic legal frameworks, the exchange of operational or tactical intelligence associated with on-going investigations. We also aim to identify ways in which the regulations for information sharing could be improved. Europol welcomes any idea of a complimentary public-private sector coalition to encourage more policy commitment for a more efficient fight against financial crime."

David Craig, President of Financial & Risk at Thomson Reuters said: "In 2011, the UN report estimated that less than 1% of criminal funds flowing through the international financial system every year are believed to be frozen and confiscated by law enforcement. Move forward six years and those of us dealing with this issue day in day out expect to find a similarly low percentage. The fragmentation we witness across global political, regulatory, economic and social spheres is creating barriers to our success. Meanwhile criminal networks are becoming more connected, more global and more technologically sophisticated. Now more than ever there is a pressing need for public and private organizations to work together across borders to secure our future by developing new strategies for sharing data and adopting new technologies in the fight against financial crime. We must not accept being one step from failure – it's time for a fresh approach."

## International Crackdown on Anti-Spyware Malware

A hacking tool allowing cybercriminals to remotely and surreptitiously gain complete control over a victim's computer is no longer available as a result of an UK-led operation targeting hackers linked to the Remote Access Trojan (RAT) Luminosity Link. This case was investigated by the South West Regional Organised Crime Unit and coordinated by the UK National Crime Agency with the support of Europol, this operation saw the involvement of over a dozen law enforcement agencies in Europe, Australia and North America.

Once installed upon a victim's computer, a user of the Luminosity Link RAT was free to access and view documents, photographs and other files, record all the keystrokes entered and even activate the webcam on the victim's computer – all of which could be done without the victim's knowledge.

Europol's European Cybercrime Centre (EC3) supported the countries in their efforts to identify EU citizens by providing analytical support and by facilitating information exchange in the framework of the Joint Cybercrime Action Taskforce, hosted at Europol's headquarters in The Hague.

# The True Cost of Flooding

In 2016, worldwide, there were 342 reported natural disasters

- The total number of Hydrological disasters in 2016 was 177 (164 floods and 13 landslides)
- The total number of peopled affected by Hydrological disasters in 2016 was 78.1 million
- The total number of deaths from Hydrological disasters in 2016 was 5,092*

Insurance company Munich Re, released their Natural Catastrophe Review which shows that 2017 had the highest insured losses, ever, at 330 billion USD, (the second highest figure ever recorded for natural disasters.)

In 2017, worldwide, there were 710 reported natural disasters.

The figures of people affected, and the number of deaths has not yet been reported, but it is estimated to be substantially higher than 2016

Each year scientists gather information to predict global weather forecast. They study historical weather patterns, the behaviour of the atmosphere, effects of climate change, the oceans movement, watching radars, and satellites all to forecast when and where natural disasters may occur.

And yet each year, more and more people are being affected by flooding in some way, be that the loss of livelihoods, homes or indeed lives.

Torsten Jeworrek of Munich Re said, “For me, a key point is that some of the catastrophic events, such as the series of three extremely damaging hurricanes, or the very severe flooding in South Asia after extraordinarily heavy monsoon rains, are giving us a foretaste of what is to come. Because even though individual events cannot be directly traced to climate change, our experts expect such extreme weather to occur more often in future.”

If the extreme weather that we are witnessing is to continue to occur more often, then solutions need to be found to minimize the effect of flooding on communities.

One such solution currently operational, with notable success is DefenCell, an effective and easily installed Flood Protection Barrier.

DefenCell Barriers are a cellular textile containment system that can be filled with various materials; soil, sand, gravel or small rocks whilst the heavy-duty geotextile fabric construction adapts to the terrain, offering excellent structural strength and durability. The easy-to-deploy cellular confinement system is well suited for irregular terrain and the addition of an integral or external impervious layer makes an effective flood barrier for temporary or permanent installation.

DefenCell has been proven in action and undergone thorough testing.  DefenCell can be used to build new defences, enhance existing protection measures or reinforce weakened levees ensuring that communities, towns and farms are protected.

A simple one metre high (or just 0.50m) wall will be sufficient to stop all but the most extreme flooding. Adding this to an existing levee or embankment is a quick and easy solution and many times faster than installing the equivalent barrier using sandbags and much faster and easier to remove when the threat has passed. DefenCell proved its operational capabilities on two flood prevention deployments on the Ohio River in the US and in Ontario, Canada.

In 2017, J&S Franklins DefenCell products were installed in two separate areas in South Australia for environmental applications including Ground Stabilisation, Flood Protection and Erosion Control with great success.

Andrew Cole, Chief Executive Officer, ↱ District Council of Barunga West, South Australia, said, “Whilst its normal use is military protection, security and flood/erosion barriers, we saw DefenCell as a flexible, cost-effective solution in front of the caravan park.  We ran a coastal trial and monitored DefenCell’s performance in tidal sea movement including high tides.”

“DefenCell maintained its integrity and we are very confident moving to a full deployment of DefenCell along the caravan park foreshore.  It is an easy product to use and there is potential for us to use it elsewhere on Council tasks.”

## Changi Airport's new Terminal 4 has already processed more than 1.5 million departing passengers using facial recognition systems from IDEMIA

In the context of soaring world airport passenger numbers (2016: up 6.3% to 3.7 billion and 700 new routes), the need for passenger identification coupled with demanding safety standards is becoming ever more critical.

In October last year Changi Airport's latest Terminal - Terminal 4 opened its doors to the travelling public and has already processed more than 1.5 million departing passengers. Passengers are processed using a system based on facial recognition from IDEMIA, enjoying a secure and innovative seamless experience as part of Changi's FAST and Seamless Travel program.

Selected by Changi Airport in 2015, IDEMIA has deployed its MorphoPass Airport Solution to automated passenger ID checks using facial recognition at all departure control points. The system includes a centralized platform used by airlines and the airport to manage the various steps required for passenger authentication and identification, MorphoFace and MorphoWay (a fully automated gate for both border control and smart boarding).

Changi Airport was ranked the world's top airport for the fifth year in a row in 2017, and for the eighth time since the award was first introduced in 2000. T4 has been created to be its most innovate terminal and can handle up to 16 million passengers per year increasing Changi's overall annual capacity to 82 million passengers.

Philippe BARREAU, Group Executive Vice President, Citizen Identity & Public Security, spokesperson for IDEMIA said "IDEMIA is thrilled that it has already helped more than 1.5 million passengers enjoy the best customer experience for travellers in the world at Terminal 4. IDEMIA strives to protect passengers so they travel in complete safety, backed by novel and convenient solutions to ensure there is no let-up in security standards while increasing convenience."

## Tanzania is using Facial Recognition to expedite cross-border mobility

The solution by Vision-Box is being used by Tanzania Immigration Services at some of the largest airports of the country

Dubai, 25th January 2018 – The Tanzania Immigration Services Department (TISD) has started using new Facial Matching Systems (FMS) to improve border control procedures end of last year.

The purpose of the integration of Vision-Box advanced technology was to enhance border security in Tanzania. How? By strengthening the capacity of immigration authorities at both land and air entry points in the country to detect irregular migration, while adhering to data protection best standards.

The new desktop automated immigration control solutions integrate advanced document authentication and biometric recognition features. They are capable of identifying fraudulent travel documents such as passports, visas and identity cards, as well as detect identity fraud by travelers trying to enter or stay in the country irregularly. The solution matches the information contained in the travel document against the live face image capture of the traveler to guarantee a reliable traveler identification.

The Vision-Box-developed solutions are at use at two of the busiest Tanzania airports, the Kilimanjaro International Airport, in northern Tanzania serving the cities of Arusha and Moshi, and Julius Nyerere International Airport in the largest city Dar es Salaam.

Commissioner Samuel Magweiga received the equipment on behalf of the Commissioner General of Immigration and advanced "we need more of its kind for all our land, air and maritime entry points to combat irregular Migration which is becoming rampant along our borders".

## Automated, Driverless Security Robot to Help Protect the World's Highest Capacity Sports Venue

Sharp INTELLOS A-UGV provides an added layer of safety and security protection for what is known as the "highest capacity sports venue in the world."

"Technological innovation is in our DNA," says IMS President, J. Douglas Boles. "Dating back to the very first Indy 500 where the rearview mirror was pioneered, IMS values, invests, and nurtures high-tech advancements in all aspects of our operations. Evolving our security force to include automated, robotic integration enables us to better safeguard patrons, drivers, and staff."

"Sharp Electronics' outdoor security robot is ideally suited to help safeguard the Indianapolis Motor Speedway's expansive, fenced property," states Cliff Quiroga, Vice President for Sharp Robotics Business Development. "The Sharp INTELLOS A-UGV is a multi-terrain, mobile sensor, data-gathering robot that can capture video, audio, and environmental information, while providing a visible deterrent without the aid of a human driver. It utilizes a navigation surveillance platform to patrol predefined routes, extending the property coverage and impact of a traditional security force, while keeping manpower safely protected from direct threats. The Sharp INTELLOS A-UGV can also act as a sentry, monitoring in a stationary position, for an extra layer of protection and has a semi-autonomous mode for incident response. Included are standard information gathering tools, plus optional observation and sensor equipment configurable to meet the Indianapolis Motor Speedway's changing safety needs."

## International Crackdown on Anti-Spyware Malware

A hacking tool allowing cybercriminals to remotely and surreptitiously gain complete control over a victim's computer is no longer available as a result of an UK-led operation targeting hackers linked to the Remote Access Trojan (RAT) Luminosity Link. Coordinated by the UK National Crime Agency with the support of Europol, this operation saw the involvement of over a dozen law enforcement agencies in Europe, Australia and North America.

Once installed upon a victim's computer, a user of the Luminosity Link RAT was free to access and view documents, photographs and other files, record all the keystrokes entered and even activate the webcam on the victim's computer – all of which could be done without the victim's knowledge.

These joint actions were carried out back in September 2017, the details of which can now only be released due to operational reasons.

Europol's European Cybercrime Centre (EC3) supported the countries in their efforts to identify EU citizens by providing analytical support and by facilitating information exchange in the framework of the Joint Cybercrime Action Taskforce, hosted at Europol's headquarters in The Hague.

### Victims across the world

The investigation uncovered a network of individuals who supported the distribution and use of the RAT across 78 countries and sold it to more than 8 600 buyers via a website dedicated to hacking and the use of criminal malware. Luminosity Link cost as little as EUR 40.00 and required little technical knowledge to be deployed.

Victims are believed to be in the thousands, with investigators having already identified evidence of stolen personal details, passwords, private photographs, video footage and data. Forensic analysis on the large number of computers and internet accounts seized continues.

Steven Wilson, Head of Europol's European Cybercrime Centre, said: "Through such strong, coordinated actions across national boundaries, criminals across the world are finding out that committing crimes remotely offers no protection from arrests. Nobody wants their personal details or photographs of loved ones to be stolen by criminals. We continue to urge everybody to ensure their operating systems and security software are up to date".

# Banning Smoking in Prisons

As Prison Authorities the world over are considering the damage of second hand smoke within our jails, a blanket ban on smoking within our Prison systems is gradually being introduced. There is an overshadowing worry of litigation and compensation claims coming down the track of health damage caused by second hand smoke.

However, the Prisoners themselves are none too happy.

In the United States, 24 states prohibit indoor smoking and 4 prohibit smoking on the entire prison grounds. And in the UK, around 66 prisons have introduced a smoking ban, but plans to make all 136 prisons in England and Wales are well underway.

According to the World Health Organisation (WHO) "Tobacco use is the single most preventable cause of death and disease claiming over 100 million lives worldwide in the 20th Century." They also claim that tobacco is the psychoactive substance most widely used by prisoners, with phenomenal usage rates ranging from 64% to more than 90% depending on the country and the setting.

But, tobacco use is so totally entrenched in prison life; it helps cope with boredom, deprivation, stress, anxiety and tension. It is a source of pleasure, and of course not to mention the monetary value in an environment without currency. Introducing a tobacco ban is not going too easy nor welcome in prison communities.

In the UK, riots have occurred within prisons over newly enforced smoking bans.

Prisoners caught with tobacco products or smoking can face disciplinary measures, such as loss of privileges as well as potentially extra time added on to a sentence. However, a couple of days added on to a 5, 10 or maybe lifetime sentence, is neither here nor there, and worth risking for a daily cigarette.

All of this makes cigarettes, big business creating an underground trade in tobacco products.

In the US, just one whole cigarettes worth of tobacco, rolled in toilet paper covering can make 5 or 6 "pinners" (small hand rolled cigarettes), this can net the seller $30. Whilst in the UK, prisoners pay £20 for a single cigarette, and a small pouch of rolling tobacco can cost £200

Of course, it's not just tobacco that is banned, any associated accoutrements, like lighters and matches are also banned. However, prisoners can make their own fire sources, with simply 2 AA batteries and a strip of foil!

And, where there is a will, there is a way.

Which is why, stopping contraband items before they get into the prison system is all the more imperative. Items as small as AA batteries, or foil, or even one cigarette, all need to be detected.

One system that is currently operational in prisons in over 30 countries is the SOTER RS Body Scanner. This ultra-low radiation full body scanner can find contraband that has been hidden on a person, and more frequently, in, a person.

Jan Steven Van Wingerden, CEO of ODSecurity, manufacturers of the SOTER RS Body Scanner said, "One of the strengths of our system is that regardless of how small an item is, and whether it has been ingested or inserted, the SOTER will find it. We pride ourselves on our products ability to find items that cannot be detected by conventional metal detectors or strip searches."

He continued, "It is important when searching for contraband that you can differentiate between human and other materials, to limit false positives, and wasted time. SOTER RS comes with its own software, and any hidden object, regardless of what material it is made from is found within 10 seconds!"

## City of Leon Continue to Build Their Sepura Network Rollout.

Following the successful implementation of a Sepura TETRA network in the Mexican State of Guanajuato, the city of Leon has added another 757 Sepura radios to its existing stock of more than 800 terminals through Sepura's in-region partner Jomtel. Following a successful implementation in December 2017, the city of Leon has now achieved its goal of upgrading its communications capability for 2018.

The Municipal Public Security Secretariat of the city of Leon purchased the radios to further enhance public safety communications for officers in the field. One of its focus points is to streamline the portfolio of radios in use within the force, thus reducing training costs.

Sepura are pleased to be selected to support the Mexican Government in this process through our partner Jomtel.

Sepura's TETRA STP9000 radios have an IP67 environmental rating - ensuring the radio remains operational even after submersion in water. Powerful audio, exceptional battery life and haptic feedback enable officers to physically feel when actions are registered on the device.

## Optim Awarded Five Year Contract from Department of Homeland Security Customs and Border Patrol division

Optim has announced it has been awarded a five-year, sole-source contract to supply its FreedomView Videoscope to the United States Customs and Border Patrol ("CPB") division. The FreedomView provides law enforcement agents the ability to search for illegal contraband, such as drugs, people, and weapons of mass effect hidden in hard-to-reach-and-see areas of vehicles, containers, and other conveyances.

"We believe the FreedomView Videoscope is the best-in-class for contraband detection" stated Paul Joyce, President and CEO of Optim. "We are extremely excited that Department of Homeland Security and the CPB selected our cutting-edge equipment to enable agents to effectively police, maintain, and protect our nation's borders. This continues the long, exclusive relationship we've had with CBP that dates back to 2010. The FreedomView is about enabling effective search and seizure in vehicles and hazardous environments, while still offering simplicity and safety to the agents using the equipment."

The CPB is tasked with utilizing small-scale detection systems like the FreedomView Videoscope to further their mission of preventing illegal contraband from entering the United States. The FreedomView is designed for easy, portable use and feature state-of-the-art optical quality. A robust, durable construction of the videoscope enables field agents operating at ports of entry and checkpoints to conduct searches safely and efficiently.

Optim's pioneering FreedomView line for contraband detection features a one-handed operation, outstanding image quality, and made-in-America craftmanship and durability. The FreedomView line is UL-certified for use in hazardous environments such as gas tanks and incorporates one-touch image/video capture for reference and evidence usage. Empowered for highly protected use, the FreedomView includes AES 256-bit hardware encryption with FIPS 140-2 Level 3 validation – enabling file transfer with secure USB drives. Intended for the rigors of every day law enforcement, the video systems can sustain the harsh elements with its water, dust, and high temperature resistant design.

## MARSS announce Middle East contract for its RADiRguard smart perimeter surveillance system

MARSS have announced an important contract for its RADiRguard smart perimeter surveillance system. The contract, with an unspecified Middle Eastern Government, is for a critical national infrastructure installation and provides for the protection of a 12km high security perimeter.

RADiRguard is a smart perimeter surveillance system combining multiple sensors and complementary technologies inside a single intelligent unit.

It is the first, all-in-one perimeter surveillance solution, which can reliably detect and classify objects in advance of reaching a perimeter, thanks to its combination of a built-in radar, video imaging and radio frequency detection. It is then able to intelligently classify the threats and issue notifications using its integral behavioural analysis software.

RADiRguard is a cost effective, easy to deploy and scalable solution which can be configured to a wide variety of surveillance scenarios such as; airports, ports, borders, fuel storage facilities, power stations, water treatment plants, nuclear facilities, bridges and high value buildings.

RADiRguard coverage shape and extension is highly adaptable by changing the number and configuration of sensors installed. In a typical configuration, a single RADiRguard unit provides 400m x 100m of coverage along a perimeter wall or fence. The system can detect and track multiple known and unknown objects including humans, animals and vehicles.

The initial detection and tracking is achieved by compact micro-radar. Behavioural algorithms provide the first level of classification. Camera footage is then analysed by Artificial Intelligence for object recognition to provide additional and more precise classification, and this classification is further augmented by analysing GSM/Wi-Fi/VHF signals emitted by object and other intelligence data bases.

This provides a risk level for each tracked object and if the object is deemed a risk then the system automatically notifies security personnel with the exact location and a live video feed supporting interception.

This layered decision hierarchy reduces the instances of false alarms.

RADiRguard operates autonomously 24/7 and is a robust, stand alone, modular and scalable system which is low maintenance and as such is extremely cost effective.

RADiRguard can be integrated into an existing security system or as part of the MARSS NiDAR advanced long-range surveillance system for protecting borders, coastal and land-based critical infrastructure from air, surface and underwater threats.

## Radiflow has revealed the first documented cryptocurrency malware attack on a SCADA network of a critical infrastructure operator

Radiflow has revealed the first documented cryptocurrency malware attack on a SCADA network of a critical infrastructure operator

Radiflow discovered this cryptocurrency malware attack as part of routine and ongoing monitoring of the OT network of a water utility customer. The company reports that this attack infected several servers in the OT network in order to mine the Monero cryptocurrency.

A cryptocurrency malware attack increases device CPU and network bandwidth consumption, causing the response times of tools used to monitor physical changes on an OT network, such as HMI and SCADA servers, to be severely impaired. This, in turn, reduces the control a critical infrastructure operator has over its operations and slows down its response times to operational problems.

Radiflow's research team uncovered that this cryptocurrency malware was designed to run in a stealth mode on a computer or device and even disable its security tools in order to operate undetected and maximize its mining processes for as long as possible.

## IPS Announce Firmware Update for OSCOR Spectrum Analyzer

The new Firmware update is a free download available on the REI website, for existing OSCOR operators. In addition to performance improvements in the new Firmware update, two file and data operations have been added:

When generating a signal list, the OSCOR will automatically populate the comments field with information about the frequency band that a signal might be a part of for the currently selected ITU region. This information contains known regulatory or other uses of given frequency bands. Depending on the frequency there may be multiple allocations given. The frequency allocation information is also provided anytime that a signal is added to an existing signal list.

The file dialogs on the OSCOR, such as the file open and file save dialogs, now contain Cut, Copy, Paste, Delete, and Rename operations which allow users to copy or move files from a compact flash card to a USB flash drive, as well as other file operations within the OSCOR firmware.

OSCOR Blue is a portable spectrum analyzer with a rapid sweep speed and functionality suited for detecting unknown, illegal, disruptive, and anomalous rogue transmissions across a wide frequency range. The OSCOR Blue Spectrum Analyzer is designed to detect illicit eavesdropping signals, perform site surveys for communication systems, conduct radio frequency (RF) emissions analysis, and investigate misuse of the RF spectrum.

OSCOR Green Spectrum Analyzer is designed to detect illicit eavesdropping signals, perform site surveys for communication systems, conduct radio frequency (RF) emissions analysis, and investigate misuse of the RF spectrum. The OSCOR Green is a portable spectrum analyzer that sweeps 24 GHz in one second to quickly detect transmitting electronic surveillance devices and ensure that spectrum activity is captured.

## L3 WESCAM Launches Smarter, More Accurate Imaging and Processing Technologies

L3 WESCAM announced that it has created smarter, more technologically advanced electro-optical and infrared (EO/IR) systems by incorporating high-performing imaging and processing technologies into its MXTM-Series product line. These new technologies will enable MX operators to conduct missions with enhanced image processing and greater visual capabilities than ever before.

"Today's environments are more complex, and missions need to be executed with more assurance," said Paul Jennison, Senior Vice President of Strategy and Business Development for L3 WESCAM. "L3's newly incorporated smart technologies provide a portfolio of capabilities that will help operators succeed though a combination of ease-of-use and robust performance."

Newly launched imaging technologies include the addition of higher-sensitivity cameras that offer advanced imaging capabilities across a much wider range of illumination conditions, thereby advancing operator capabilities in low-visibility and no-visibility environments.

Advancements to L3's MX image processing technologies include WESCAM's embedded Advanced Video Engine (WAVE) and a newly embedded Graphics Processing Unit (GPU). L3 WESCAM's new Automated Video Tracker (AVT) and embedded Moving Target Indicator (MTI) technologies are supported by this new architecture and provide automatic target acquisition of multiple targets with significantly improved target lock performance in challenging mission scenarios.

L3's significant investment in its image processing technologies has made the MX product line smarter, as the WAVE's architecture supports future growth and allows for the rapid deployment of future image processing techniques.

L3 has more than 40 years of experience in the design and delivery of stabilized imaging and targeting solutions. Systems range in size from 8 to 25 inches in diameter, portray clear sighting capabilities across the visible and infrared spectrums, and operate with outstanding stabilization and leading range performance.

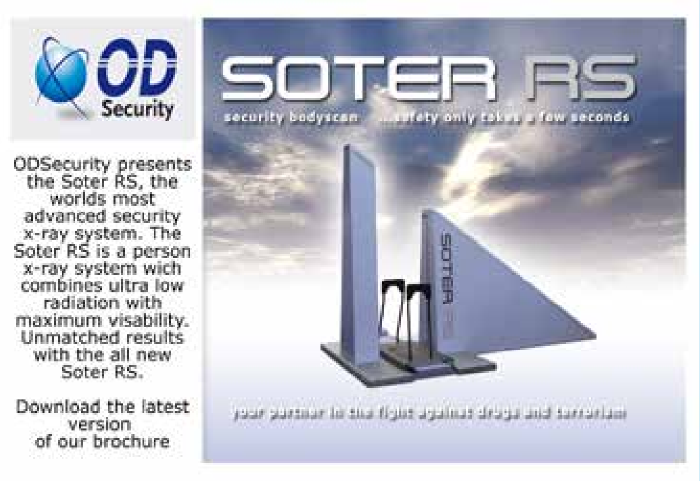
## World Security Report

World Security Report is a bi-monthly electronic, fully accessible e-news service distributed to over 150,000 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.

HIDDEN TECHNOLOGY
systems international ltd.
Discrete tracking devices for personal protection and vehicle security.
Fast, accurate locations using 3G, GPRS, SMS and RF.
In use by Police, Military and Government organizations worldwide.
www.hiddentec.com

## Border Security Report

Border Security Report is the bi-monthly border management industry magazine delivering agency and industry news and developments, as well as more in-depth features and analysis to over 20,000 border agencies, agencies at the borders and industry professionals, policymakers and practitioners, worldwide.


OD Security
ODSecurity presents the Soter RS, the worlds most advanced security x-ray system. The Soter RS is a person x-ray system wich combines ultra low radiation with maximum visability. Unmatched results with the all new Soter RS.
Download the latest version of our brochure
SOTER RS
security bodyscan ....safety only takes a few seconds
your partner in the fight against drugs and terrorism

2003-2013
WAGTAIL
UK LIMITED
SPECIALIST DOG SERVICES
10 YEARS
Wagtail International
leading specialists in detection dogs and dog handler training
Click here to view our profile

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

## March 2018

5-6
Defence Logistics Eastern Europe
Prague, Czech Republic
www.defence-logistics.eu

6-7
Security & Policing
London, UK
www.securityandpolicing.co.uk

6-7
Security & Counter Terror Expo
London, UK
www.counterterrorexpo.com

6-8
Major Events Safety & Security Summit (ME3S)
Dubai, UAE
www.isnrabudhabi.com/ME3S

14-15
Behavioural Analysis
Cardiff, Wales, UK
www.behaviouralanalysis.com

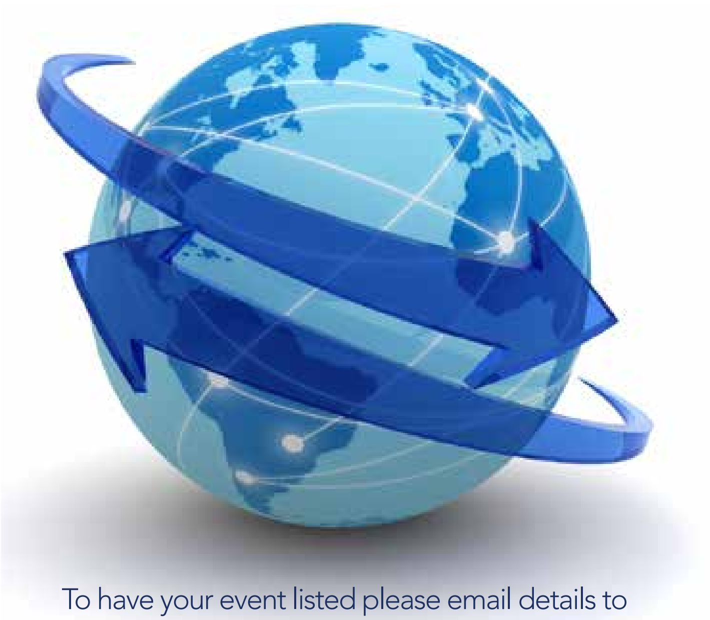
20-22
World Border Security Congress
Madrid, Spain
www.world-border-congress.com

## April 2018

5-7
Secutech India 2018
Mumbai, India
www.secutechexpo.com

10-12
LAAD Security 2018
Sao Paulo, Brazil
www.laadsecurity.com.br/en

11-13
International Security Conference West
Las Vegas, NV, USA
www.iscwest.com



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

18-19
IoT Tech Expo Global 2018
London, UK
www.iotevents.org

## May 2018

1-3
Civil Security Congress & Expo 2018
Melbourne, Australia
www.civsec.com.au

## July 2018

17-19
Critical Infrastructure Protection & Resilience Asia
Sarawak, Malaysia
www.cip-asia.com

## September 2018

25-27
Critical Infrastructure Protection & Resilience Europe
The Hague, Netherlands
www.cipre-expo.com

## December 2018

4-6
Critical Infrastructure Protection & Resilience North America
Florida, USA
www.ciprna-expo.com