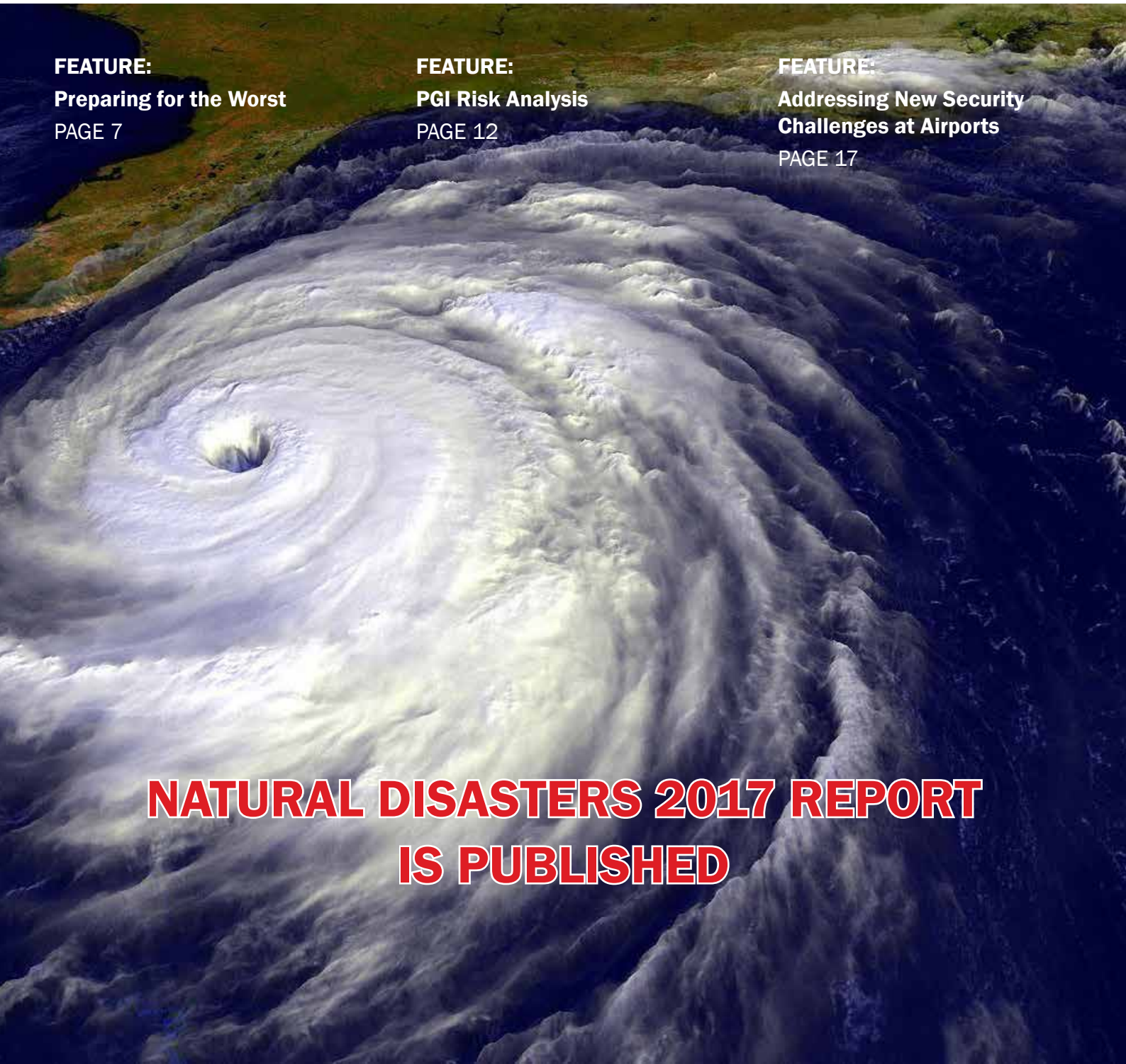
INCORPORATING BORDER SECURITY REPORT

WORLD SECURITY REPORT

Official Magazine of
International Association of CIP Professionals

SEPTEMBER / OCTOBER 2018
www.worldsecurity-index.com



NATURAL DISASTERS 2017 REPORT IS PUBLISHED

critical infrastructure PROTECTION AND RESILIENCE EUROPE

2nd-4th October 2018

The Hague, Netherlands

www.cipre-expo.com

REGISTER ONLINE TODAY

Working together for enhancing security

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

Critical Infrastructure Protection and Resilience Europe launches Preliminary Conference Programme

Delivering an outstanding conference programme of international expert speakers contributing to the valuable discussion on protecting Europe's critical infrastructure.

Part of the City of The Hague's 2018 **Cyber Security Week**, Critical Infrastructure Protection and Resilience Europe will include topics of discussion such as:
• Risk and Resilience in CIP and CIIP • PPP Role in CIP • Emergency Preparedness and Response in CNI • Cyber Security Legislation, Best Practice & Standards • Cyber Defence Strategies • Cyber Technologies to Prevent and Protect • SCADA Systems and IT/OT Integration • Emerging and Future Threats on CNI • Space Based CNI • Human Factors, Organisation Risk and Management Culture • Risk Management in Transport, Telecoms and Energy CIP

Download the Prelminary Conference Programme guide at www.cipre-expo.com/PSG

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

Further details and Online Registration at www.cipre-expo.com

Confirmed Speaker include:

- Silvio Mascagna, Member of the Security Union Cabinet, European Commission
- Andrew Palmer, Border Security Lead, Gatwick Airport
- Bharat Thakrar, Head of Business / Cyber Security Resilience, BT Global Services
- Mirjam van Burgel, Researcher Tele-Vulnerability, Radiocommunications Agency Netherlands
- Catherine Piana, Director General, CoESS – Confederation of European Security Services
- Mia Wannewitz, Research Associate, United Nations University, Institute for Environment and Human Security (UNU-EHS)
- Eva Stock, Research Consultant, German Federal Office of Civil Protection and Disaster Assistance
- Ivana Cesarec, Senior Advisor for Prevention Activities National Protection and Rescue Directorate Republic of Croatia
- Alexandru Georgescu, Researcher, ROMSPACE
- Assistant Professor Robert Mikac, Faculty of Political Sciences, University of Zagreb, Croatia

For further details and speaker line up visit **www.cipre-expo.com**

Leading the debate for securing Europe's critical infrastructure

Hosted by:

Supporting Organisations:

Media Partners:

CONTENTS

WORLD SECURITY REPORT


» p.5


» p.12


» p.17


» p.19

WHERE US GUN CONTROL LAWS AND INTERNATIONAL SECURITY COLLIDE

As this magazine went to press, once again we have witnessed the awesome power of nature wreak havoc across vast areas of the US and Asia.

In the US, 17 people are so far believed to have been killed and tens of thousands left stranded in rescue centres around the Carolina's. Historic flood levels have caused power outages and have left at least 650,000 homes without electricity.

In Asia, Typhoon Mangkhut smashed first into the northern tip of the Philippines and north-eastern Luzon, leaving a large swathe of destruction of roads and bridges and shutting down electricity in at least eight provinces. It is one of the most powerful storms to hit the region in decades, killing 100 people or more in the Philippines and is now causing widespread death and destruction in China.

The long-term trend indicates that the length and intensity of storms worldwide will worsen over time, making it more important than ever that we secure vital infrastructure, not only from the threat of terrorism, but from the immediate threat posed by our changing weather patterns.

In an increasingly connected world, almost everything we do is dependent upon networks, and networks upon power. Whether it's foodstuffs in the shops or fuel at the pumps, almost everything we need is delivered on a "just-in-time" basis, which relies on networked communications. In our homes everything from our communications to the outside world, to the water in our taps are all dependent on a reliable and resilient power grid.

We can't do anything to stop natures annual show of strength, but surely when we can run power and communications under the oceans, we can certainly do more to secure the power grid from some of the worst effects?

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/WSR

www.worldsecurity-index.com

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

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

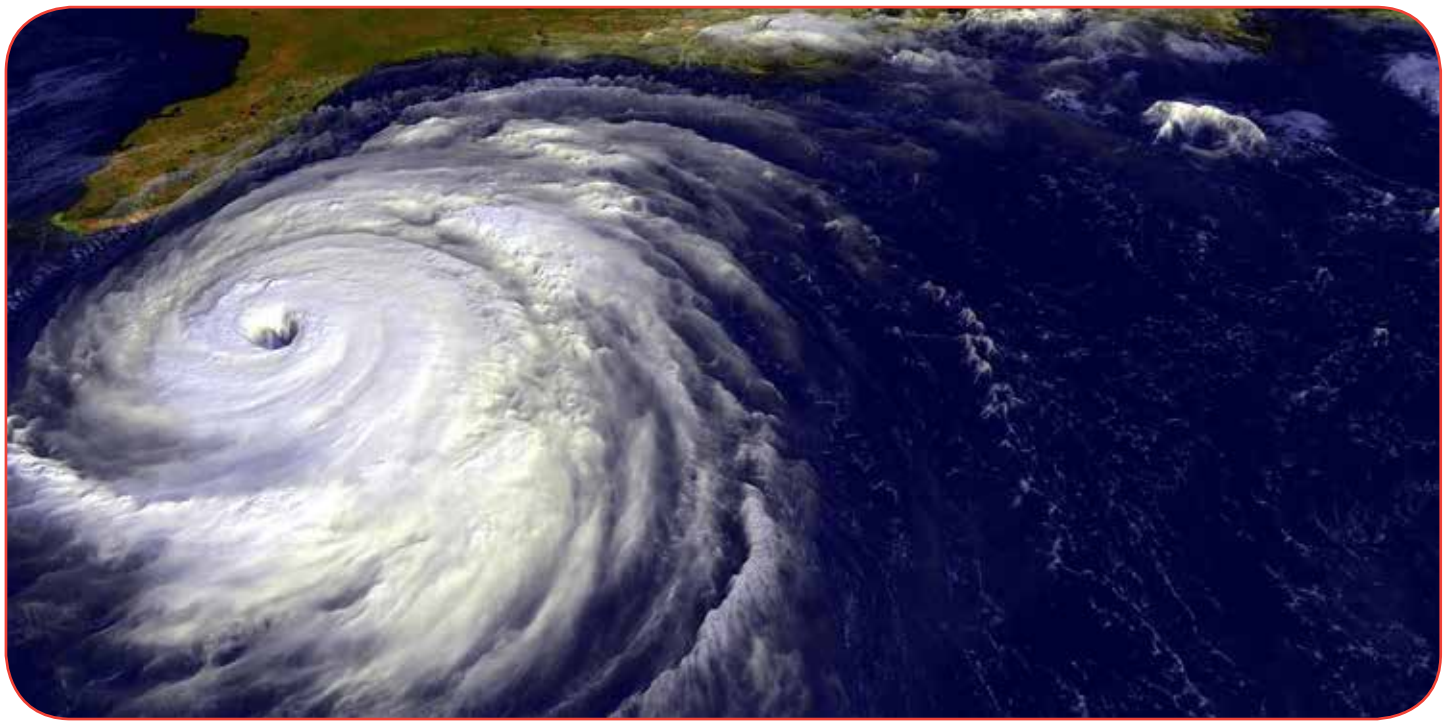
Features Editor:
Karen Kingham
E: karen.kingham@knmmedia.com

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

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

World Security Report is a bi-monthly electronic, fully accessible e-news service distributed to over 130,000 organisations globally. It tracks the full range of problems and threats faced by today's governments, armed and security forces and civilian services and looks at how they are dealing with them. It is a prime source of online information and analysis on security, counter-terrorism, international affairs, warfare and defence.

Natural Disasters 2017 Report has just been published



In 2017, 335 natural disasters affected over 95.6 million people, killing an additional 9,697 and costing a total of US $335 billion. This burden was not shared equally, as Asia seemed to be the most vulnerable continent for floods and storms, with 44% of all disaster events, 58% of the total deaths, and 70% of the total people affected.

Despite this, the Americas reported the highest economic losses, representing 88% of the total cost from 93 disasters. China, U.S., and India were the hardest hit countries in terms of occurrence with 25, 20, and 15 events respectively. Given the large land mass of each country, these results are not surprising.

Compared to the previous decade (2007-2016), there were fewer natural disasters, deaths, and total people affected in 2017, but with a higher price tag. Number of natural disasters in 2017 were similar to the annual average of 354 events, below the average of 68,273 killed per year, and well below the 210 million annual average people affected. In terms of economic losses however, there was a 49% increase than the previous average of $141 billion.1 After 2011, characterized by a devastating earthquake/ tsunami in Japan, 2017 was the most expensive year in the decade due to a series of powerful hurricanes across the U.S. and the Caribbean. These include Hurricane Harvey, Hurricane Irma, and Hurricane Maria, costing $95 billion, $80.7 billion, and $69.7 billion respectively. When looking at types of events, 2017 was characterized by a higher number of reported storms with 127 compared to the annual 98 average. Similar patterns were seen with wildfires, with 15 compared to the annual 9 average, and landslides, with 25 compares to the annual 17 average.

Mortality is quite low compared to the annual average of the last decade of 68,273. This is likely due to three events with very high mortality: the 2010 earthquake in Haiti (222,500 deaths); the 2008 Cyclone Nargis in Myanmar (138,000 deaths); and the 2008 Sichuan earthquake (87,000 deaths). The deadliest event in 2017 was the landslide in Sierra

Leone in August, with 1,102 reported dead or missing, followed by Cyclone Okchi in December with 884 reported dead or missing in India and 27 deaths in Sri Lanka. Notably, these two events are characterized by a high number of missing, representing over half of the total death toll.

Specifically for the African and American continents, the 2017 mortality is higher than the 10 years average due to the occurrence of the landslide, earthquake (mentioned below), and hurricanes. These figures do not consider the revised death toll of Hurricane Maria in Puerto Rico from 64 deaths to 4,645 excess deaths,2 or more recently 2,975 excess deaths.3 Additionally, although the total affected, 95.6 million, is well below the yearly average of the last decade of 210 million, Africa and the Americas have a greater proportion of people affected than the yearly average.

In terms of disaster events reported, the year was characterized by a record hurricane season with heavy losses, both economic and human, with at least 340 dead or missing for the 3 main hurricanes: Irma, Maria, and Harvey. In addition to hurricanes, losses were also seen as a result of two major earthquakes: one in September in Mexico with 369 fatalities and one in November in Iran/ Iraq with at least 450 fatalities. Additionally, two strong wildfires in Portugal contributed to the human cost, with 64 fatalities in June and 45 fatalities in October. A single flood killed 834 people and affected almost 27 million people in August in India, Nepal and Bangladesh, and in China, 12 million were affected by a flood during the Mei-Yu season.

The data reported above suggest an emerging trend in natural disaster events demonstrating lower mortality but higher cost.

Preparing for the Worst

When flood waters strike a community, be that in Europe, Asia, Africa, or the Americas a trail of devastation follows; lives are lost, livelihoods wrecked, homes are ruined, and critical infrastructure destroyed. The effects and damage to that community will remain long after the emergency services, relief efforts or international aid have patched up the damage and gone home.

Damage or disruption to any Critical Infrastructure whether it is water treatment plants, electricity substations, transportation networks, communication systems, or medical services will inevitably lead to other significant secondary consequences including; malfunctioning emergency services, lack of power to hospitals, stranded populace, contaminated food stocks, and water borne diseases.

With every will in the world, relief efforts, and international aid, are just that; relief and aid. Perhaps, now, it is time for us to find a way of instead of looking at how to get emergency aid to the areas affected once a disaster strikes, why not look at how help can be offered immediately that disaster strikes, by preparing for it before it happens!

It is a fact that our world's weather is changing.

The UN Office for Disaster Risk Reduction (UNISDR) 20-year review produced jointly with the Belgian-based Centre for Research on the Epidemiology of Disasters (CRED) demonstrated that since the first Climate Change Conference (COP1) in 1995 (until 2015), 606,000 lives have been lost and 4.1 billion people have been injured, left homeless or in need of emergency assistance because of weather-related disasters. With the USA, China, India Philippines and Indonesia recorded the most.

Floods accounted for 47% of all weather-related disasters from 1995-2015, affecting 2.3 billion people and killing 157,000. Storms were the deadliest type of weather-related disaster, accounting for 242,000 deaths or 40% of the global weather-related deaths, with 89% of these deaths occurring in lower-income countries.

Ms. Margareta Wahlström, United Nations Special Representative of the Secretary-General for Disaster

critical infrastructure PROTECTION AND RESILIENCE AMERICAS

December 4th-6th, 2018
Tampa, Florida, USA

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

Registration Now Open

Register today and benefit from Early Bird delegate fees

For further details visit www.ciprna-expo.com/registration

Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. This directive supersedes Homeland Security Presidential Directive 7.

We must be prepared!

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

Join us in Tampa, Florida for the premier event for operators and government establishments tasked with the regions Critical Infrastructure Protection and Resilience.

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

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

Confirmed speakers include:

- Chauncia Willis, Emergency Coordinator, City of Tampa
- Brian Harrell, Managing Director, Enterprise Protective Services, Duke Energy Corporation
- Fred Ruanavar, Chief DISA/DoDIN
- Michael Cotton, National Telecommunications and Information Administration (NTIA), Institute for Telecommunication Science (ITS)
- Jessica Yuzwa, Project Administrator, Franklin County Office of Homeland Security and Regional Communications, Ohio
- David Alania, International Expert/ Adviser, Georgia
- Jeff Gaynor, President, American Resilience
- Deborah Kobza, President, International Association of Certified ISAOs (IACI)
- Michael Hamilton, Founder and President, Critical Informatics
- Peter Murphy, Director and Co-founder, Noetic Corporation
- John Esquivel, Senior Director, AECOM
- Christian Morin, VP Cloud Services & CSO, Genetec

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

Leading the debate for securing Amercia's critical infrastructure

To discuss exhibiting and sponsorship contact:

Paul McPherson
Exhibit Sales Manager
E: paulm@torchmarketing.co.uk
T: +1-240-463-1700

Owned & Organised by:

Supporting Organisations:

Media Partners:

Risk Reduction said: *"Weather and climate are major drivers of disaster risk and this report demonstrates that the world is paying a high price in lives lost. Economic losses are a major development challenge for many least developed countries battling climate change and poverty."*

Throughout the world now we have amazing weather centres, providing forecasting the likes of which we have never seen.

We have access to reliable, recorded historical data now.

We know for instance that Bangladesh will be affected every year by the devastating effects from their annual monsoon season, which is exacerbated by the cyclones which cause coastal flooding, meltwater from the Himalayas, deforestation and increasing urban areas, and that the US will go through Hurricane season every year.

Even as I write this article the UNHCR (United Nations Refugee Agency) is continuing to deal with the effects from the continuing heavy monsoon rains that have hit Bangladesh with the heaviest monsoon rainfall so far this year being around 463mm on the 25th July 2018, the USA is preparing for Hurricane Florence to make landfall, with the prediction of life threatening storm surges of up to 12 foot along the coasts and up to 30 inches of rain, an estimated 1 million people are evacuating the east coast and a super typhoon Mangkhut is currently in the Pacific and heading to Hong Kong where latest Tropical Cyclone Warning Bulletin issued by the Hong Kong Observatory. The Standby Signal, No. 1 is in force. This means that a tropical cyclone now centred within about 800 kilometres of Hong Kong. The tropical cyclone warning

is however expected to reach Level 10 over the coming hours, and days.

Margareta Wahlström, United Nations Special Representative of the Secretary-General for Disaster Risk Reduction said, *"Access to information is critical to successful disaster risk management. You cannot manage what you cannot measure."*

In May this year, a ground-breaking new humanitarian fund designed to mitigate and even prevent the damage and trauma caused by natural disasters such as flooding was launched by the International Federation of Red Cross and Red Crescent Societies, (IFRC)

Forecast-based Action Fund uses a combination of weather predictions and historical data to fix triggers for the automatic release of money for pre-agreed early action plans. For example, a combination of forecast rainfall combined with the level of a river at a certain point can be used to activate funding for downstream evacuations and the distribution of shelter kits for the people who have been moved to safer ground. It is embedded within IFRC's Disaster Relief Emergency Fund (DREF), a 25-30 million Swiss franc annual fund which has been supporting Red Cross and Red Crescent emergency response efforts for more than three decades.

"We think this is a game-changer, not only for the Red Cross and Red Crescent, but for humanitarian action as a whole," said Pascale Meige, IFRC's Director of Disaster and Crisis Prevention, Response and Recovery. "Our new forecast-based action fund means that guaranteed money will be available to help communities prepare for a disaster before it strikes."

"For decades, humanitarians have been calling for a shift to proactive and preventative humanitarian action, but such action has so far been sporadic. For the first time, this fund, and the work we are doing to build country-level plans and agreements, can consistently deliver on this promise – turning promises into action."

"It means that life-saving action can now take place before anyone is in immediate danger, which will save lives and reduce the need for more costly emergency response and recovery efforts."

The Forecast-based financing approach – now being rolled out by IFRC at national level – has been piloted at community level since 2014, including in Peru, Togo, Uganda, Bangladesh,

Mozambique and Mongolia. In Bangladesh, predicted flooding of the Bramaputra river in 2017 triggered cash grants for people who were able to use this money to support their families during the emergency.

Whilst the Bangladeshi monsoon floods on the 25th July 2018, were the strongest test of the UNHCR monsoon mitigation measures and emergency response, including relocation, post disaster kits, shelters replaced, and new tarpaulins supplied. The Cox's Bazar settlements largely weathered the storms, proving the value of months of mitigation efforts, with no deaths reported in the refugee sites. 60 potentially life-threatening incidents and others averted through swift action.

Fifteen National Red Cross and Red Crescent Societies in Africa, Americas and Asia Pacific are currently developing Early Action Protocols for foreseeable and preventable natural disasters and are expected to access the fund in its first two years. However, the facility can be available for all 190 National Societies.

According to the International Federation of Red Cross and Red Crescent Societies (IFRC) in 2008 1.2 million people felt the impact when the Brahmaputra River of north eastern India and Bangladesh pushed over its banks

The National Disaster Reduction Centre of China (NDRCC) reports that as of 15th August 2017 and confirmed by the Bangladesh Red Crescent Society (BDRCS) own source; 3,917,184 people are affected following the 4th flood of 2017. Approximately 531,517 Houses have been damaged by this flood. There were 1,392 temporary shelters; where 282, 479 peoples have taken shelters. 309,542 hectares of crop at that date had already been damaged.

Floodgate's removable flood protection

Flood Forecasting in Bangladesh is done by the Flood Forecasting and Warning Centre (FFWC) under the ministry of Water Resources. The FFWC uses both deterministic and probabilistic forecasts and they cover about 60% of the flood affected areas. Including Bogra one of the FbF (Forecast based Financing) pilot sites.

The government of Bangladesh is working toward its 'Vision 2041,' which outlines plans to have a strong and developed economy and to generate 60,000MW of electricity (4 times its current capacity) by 2041. It aims to provide access to electricity for its population of around 165 million, by 2021, and has invested some 30million USD in its electricity infrastructure to meet vision.

Bangladesh obviously has a unique set of natural phenomena linked with effects of current lifestyles, that culminates in a worsening of effects with every passing year. But, there are many, many ways available to limit the devastating effects of flooding to communities and critical infrastructure alike with a little prior warning of a catastrophic event. A quick search of the internet will bring up many companies offering a range of flood protection products, from the tried and tested, to the weird and wonderful. The following companies all are tried and tested, and have a pedigree in their own right.

UK Company, Floodgate supply a completely removable, flood protection door barrier which can be used singly, or joined together. Floodgates comprise of a 25mm thick, boxed steel frame covered by a 7mm thick blue neoprene cover. A jacking mechanism attached to the rear of the frame allows both the frame and cover to expand telescopically widthways into the walled area (the reveal) immediately in front of the door. Four bolts situated along the bottom edge of the frame are then adjusted to provide a seal along the ground. Due to its unique

Van den Noort Innovations Self Closing Flood Barrier

Chemtex Grab & Go Flood Control Kit

expandable design, Floodgate does not normally need any permanent fittings to the property and does not require pre-drilling of the door frame, making it ideal for use on old and listed buildings.

The Self Closing Flood Barrier manufactured by Van den Noort Innovations, BV in the Netherlands provides, a unique effective flood defence system to protect people and property from inland waterway floods caused by heavy rainfall, gales or rapid melting snow. Its automatic instant reaction to upcoming floods has proven to provide optimal protection against high water levels. This unique Flood Barrier System has been developed to provide optimal protection against extreme high-water levels in rivers and other inland waterways. The SCFB can be built on the top of a dike or quay to protect inhabited as well as industrial or other strategical areas.

Chemtex in the USA manufacture a "Chemtex Grab & Go Flood Control Kit". This kit is designed for quick and easy deployment when timing means everything. The compact container takes up minimal space and is ideal for rapid emergency deployment. Self-activating flood barriers simply expose them to fresh water. They absorb water and grow to full size at 3.5' high in 5 minutes. Swelled barriers contain and divert flood water. Leave in place for ongoing protection. Lasts for up to 8 months of continuous use. Safe, non-hazardous and nontoxic, environmentally friendly and decomposes over time. Store in a closet, cabinet, vehicle or elsewhere. The bucket can be used to pre-activate your H20 Dams/ Flood Barriers — just add water to the bucket and go!

J&S Franklin manufacturers of the DefenCell Flood Protection Barrier has been proven in the US in a flood protection role when the town of Smithland, Kentucky, USA, which is situated at the confluence of the Ohio and Cumberland Rivers had to deal with a record surge in river levels. The Louisville Office of the U.S. Army Corp of Engineers (USACE) requested an emergency installation of a DefenCell Flood Protection Barrier.

DefenCell Flood Protection Barrier

Within 24 hours, 3 miles worth of DefenCell Flood Wall units were delivered.

Within an hour of delivery, small teams were able to start placing, connecting and filling the systems. After just two hours, installation was being achieved at a rate of 20+ units per hour, (Equivalent to 22,196 sand bags in the initial three hours after delivery.)

In 34 hours, more than 10,500 linear feet of DefenCell Flood Walls had been installed, over 700 units were filled with more than 4,700 tons of sand, by a willing and enthusiastic but untrained, local workforce. The barrier was more than one mile in length, adding an extra four foot of flood protection height to the Smithland levee.

Now this isn't the answer to all the floods around the world, but just see what you can do with a little prior warning, pre-preparation and knowledge.

PGI Risk Analysis

This Risk Analysis Report has been brought to you by PGI www.pgitl.com and PVI www.pviltd.com, global leaders in cyber security, maritime security, intelligence, geopolitical risk and training.

Colombia: Authorities seize submarine with 748 kg of cocaine near Gorgona island

The navy intercepted a semi-submersible submarine carrying 748 kg of cocaine near Gorgona island. Authorities arrested four Colombian crew members. Reports did not specify the group affiliation of the arrested suspects. Authorities regularly seize cocaine shipments intended for Central America and the US.

Egypt: Authorities arrest two on smuggling charges at Port Said

Authorities from the Port Said Security Directorate detained two Egyptian nationals on charges of smuggling foreign-manufactured goods through the port. One of those detained was a local import-export businessman while the other was a driver set to collect the goods, which consisted of 1,000 kg of clothes. The two had failed to pay the required customs duties on the shipment.

Gabon: Tbilisi confirms 17 sailors missing after contact with tanker lost off Libreville

The Georgian government confirmed that an investigation is underway after 17 Georgian sailors went missing off the coast of Gabon since 14 August when all contact with their ship was lost as it was sailing off Libreville. The Panama-flagged chemical tanker MT Pantelena was around 18 nm off Libreville when all contact was lost although it is unclear what happened to the vessel and its crew.

PGI Analysis: Although piracy in the Gulf of Guinea is common, incidents off Libreville are rarely reported. Most attacks are concentrated 10-150 nm off the coast of Nigeria, although there is precedent for incidents further south off Sao Tome and Principe.

Israel: Navy intercepts Gaza-bound activist boat

The Israeli navy intercepted a Swedish-flagged activist boat in international waters bound for Gaza. The military released a statement that the boat violated the naval blockade and that any humanitarian aid should be directed through Ashdod port. Activists said the boat was carrying medical supplies. The UN has called for the blockade to be lifted to due to the deteriorating humanitarian situation in Gaza.

Iran: IRGC reports full control over Gulf and the Strait of Hormuz

The head of the Islamic Revolutionary Guard Corps' naval division, General Alireza Tangsiri, said Iran now has full control over the Gulf and the Strait of Hormuz, according to local private news agency Tasnim. Tehran has previously threatened to block the strait, a major oil shipping route, in retaliation for any hostile action against Tehran by the US. The announcement comes ahead of the re-imposition of US sanctions targeting Iran's oil and gas industry on 5 November.

Italy: Authorities disembark 150 migrants, interior minister under investigation

Port authorities allowed 150 migrants to disembark from a ship which had been docked for five days at the Port of Catania over the government's refusal to let the migrants enter Italy. Interior minister Matteo Salvini had refused to let the migrants enter until other EU countries agreed to take some in. Ireland, Albania and the Vatican reportedly accepted to house the migrants. In response to the incident, a prosecutor in Sicily filed kidnapping, abuse of power and illegal arrest charges against Salvini.

Malaysia: Authorities rescue kidnapped fishermen from Thai pirates

Thai authorities announced that they had rescued the last four of a group of 11 Malaysian fishermen kidnapped by a group of armed men off the coast of Pulau Langgun, an island located near the border between Malaysia and Thailand. The fishermen were robbed and captured on 19 August. Malaysia's Marine Operations Force rescued seven of the fishermen later the same day. Four of the kidnappers are in police custody.

PGI Analysis: The incident marks the first report of fishermen being abducted in the region and unconfirmed sources reported that pirates had sought to swap the fishermen for four of their accomplices detained by maritime police. Police have raised concerns criminals could look to target tourist boats and yachts in the area. The Langkawi Tourism Organisation has called for security to be stepped up in the region and said it had received reports of assailants stealing speedboats in the area.

Malaysia: Suspected militants kidnap two fishermen off Sabah state

Police reported that two fishermen were kidnapped by suspected members of Islamist militant group Abu Sayyaf Group (ASG) in the waters off Semporna in Sabah state in the early hours on 11 September. Four crew members were on a fishing vessel docked at the Pulau Gaya jetty when the kidnapping reportedly took place during curfew hours at approximately 0100 hrs local time. Some reports indicated three fishermen had been kidnapped and that an initial probe showed that the masked kidnappers were carrying M16 rifles.

PGI Analysis: If confirmed, the incident would be the first kidnapping by ASG militants in the region in over a year. The kidnapping comes weeks after suspected militants attempted to kidnap crew from a tugboat off Lahad Datu in Sabah state on 10 August and a similar attempt was reported off Basilan province in the Philippines in February, indicating the group have continued operations in the area. Authorities have implemented a series of curfews to combat the kidnappings by the group since July 2014 although ASG has conducted regular kidnappings targeting vessels in the Sulu and Celebes seas in recent years, particularly between March 2016 and March 2017.

Mexico: Authorities seize 2,600 kg of cocaine from semi-submersible

Mexican authorities seized 2,600 kg of cocaine from a semi-submersible vessel in an undisclosed location in the Pacific Ocean. Authorities arrested three drug traffickers, two Colombian nationals and one Ecuadorian. Officials believe the vessel was attempting to smuggle cocaine into the US where the market value of the drug is significantly higher than in Mexico.

Nigeria: Armed robbers steal from vessel at Onne anchorage

Four armed robbers boarded a merchant vessel at Onne Port Anchorage at 0240 hrs local time and stole cans of oil before leaving. Crew were later reported as safe.

PGI Analysis: Crime is rarely reported at Onne port, although this is likely due to a lack of capacity to formally report crime through recognised channels. Onne port is located in the restive Niger Delta region where armed criminal gangs perpetrate a range of violent and opportunistic crimes, making it likely that the actual crime rate at the port is higher than reported. However, Nigerian authorities have lowered the International Ship and Port Security (ISPS) Code level to a level 1 in April 2017, citing significant security improvements at Onne since 2016.

Saudi Arabia: Riyadh resumes oil exports through Bab el-Mandeb

Saudi Arabia announced that oil shipments transiting through the Bab el-Mandeb strait were to resume as of 2 August. Exports had been temporarily suspended after Houthi rebels launched attacks on two Saudi Very Large Crude Carriers in the Red Sea on 25 July, causing light damage to one of the vessels.

PGI Analysis: The announcement comes after the Houthi rebel group said that it would unilaterally halt attacks in the Red Sea for two weeks from 0000 hrs local time on 1 August to support peace efforts. The group said that the halt in naval military operations could be extended to all parts of Yemen if the Saudi-led coalition fighting against the rebel group reciprocates. The group has repeatedly targeted Saudi vessels amid a coalition operation against the group in Hodeidah.

Somalia: Police detain Mogadishu port officials for questioning

According to local media, police detained several officials at Mogadishu port for questioning in connection with corruption allegations. Those arrested included the manager of the seaport customs office. Local media did not confirm details of the allegations.

Togo: Update: Missing tanker docks in Lomé, crew reported safe

Panama-flagged chemical tanker MT Pantelena, which went missing on 19 August off the coast of Libreville, has docked at Lomé port. Reports indicate that all 19 crew on board were safe. The ship's operator, Lotus Shipping, did not provide additional details on the reasons for the disappearance or on the ship's cargo. The crew were reportedly locked in a cabin for nine days, but were given food and water and were not physically harmed.

PGI Analysis: Kidnap-at-sea gangs operate in the Gulf of Guinea and have hijacked tankers and merchant vessels in recent years, predominantly with the aim of obtaining ransom for crew members. It remains unclear whether ransom was paid to secure the crew's release, although it is likely that this was the case.

Yemen: Coalition foils Houthi speedboat attack in Red Sea

The Saudi-led coalition announced it had thwarted a planned Houthi attack involving the use of explosives-laden speedboats against commercial vessels. The target and further details of the attack were not disclosed but the speedboat was reportedly launched from the Houthi-controlled Red Sea port city of Hodeidah.

PGI Analysis: The purported attack comes after Houthi forces used projectiles to attack two Saudi-oil tankers in the Red Sea, one of which suffered minor damage. In May, the Saudi-led coalition reported foiling a similar attack by remote-controlled speedboats loaded with explosives targeting commercial vessels in the Red Sea, including an oil tanker, underscoring the threat to maritime traffic off Yemen.

Playing your part in the protection and resilience of our infrastructure and information

John Donlon
Chairman
International Association of CIP Professionals
(IACIPP)

The first six months of 2018 have been quite significant from both a political and threat perspective. Quarter 2 of this year saw a number of terrorist incidents; 280 attacks across 32 countries and in May the Director General of MI5 in the United Kingdom delivered a clear message on the continued nature of the threats we all face when he stated 'Europe faces an intense, unrelenting and multidimensional international terrorist threat. Daesh continues to pose the most acute threat, but Al-Queada and other Islamist terrorist groups haven't gone away'.

A great deal of good work is going on globally to ensure that threats and vulnerabilities are being addressed. It is more important than ever in this rapidly changing, technologically advanced, world that we inhabit that we continue to try to stay ahead of the game in terms of our approach to security and resilience and none more so than within our critical infrastructure environments

As you are all no doubt aware a nation's critical infrastructure provides the essential services that underpin society and are a significant contributor to the economy, security, and health. Rapid globalization has presented us all with an abundance of economic opportunities but also a growing number of interconnected and diverse threats.

The risk environment affecting critical infrastructure is both complex and uncertain. Threats, vulnerabilities and consequences have all evolved over the past decade and infrastructure that has long been subject to the dangers associated with physical threats and natural disasters are now increasingly exposed to cyber risks which stems from the growing integration of information and communications within their operations.

I believe that our critical infrastructure will continue to be high on the list of targets for terrorist groups who are increasingly using their technical expertise to explore new methods of attacks. Many commentators are of the view that some, if not all, of critical infrastructure presents a relatively soft opportunity to cause harm and disruption and within that the vulnerabilities around the technology employed to deliver our critical services continues to be an area of concern.

If we just examine the most recent breach to make global news headlines, at British Airways, where the motivation for accessing some 380,000 data records may well have been financial gain, can we begin to imagine the consequences if that level of activity was focused and successful on aircraft logistics and or the flight operating systems of the organisation.

Cyber security continues to become more prevalent and rightly so. In my last article I wrote of the significant efforts being driven on cyber matters within infrastructure across the ASEAN region. I am fortunate to be attending two more conferences this year on the protection and resilience of critical infrastructure, CIPRE in The Hague in October and CIPRNA in Tampa, Florida in December. I will watch with interest to see the level of concerns that are articulated on such vulnerabilities and the innovations being developed across these regions in tackling those concerns.

Latest IACIPP Poll Results

Where do you see cybersecurity certification of Operational Technology's (ICS / Scada) components fit best?

Energy	- 17%
Transport	- 9%
Telecomms	- 9%
Defense	- 4%
None of Them	- 4%
Nuclear	- 0%
All of Them	- 57%

The International Association of Critical Infrastructure Protection Professionals (IACIPP) is delighted to announce the appointment of Brian Harrell as Operator Relations Director, North America

Brian Harrell is a Senior Fellow at The George Washington University, Center for Cyber and Homeland Security (CCHS) where he serves as an advisor on infrastructure protection and cybersecurity policy initiatives. Brian is also currently the Managing Director of Enterprise Protective Services (EPS) at the Duke Energy Corporation where he leads enterprise-wide corporate security efforts.

Brian is nationally recognized for his efforts on critical infrastructure protection, continuity of operations, and enterprise risk management. Prior to coming to Duke Energy, Brian was the President and Chief Security Officer at The Cutlass Security Group, where he provided critical infrastructure companies with consultation on risk mitigation, protective measures, and compliance guidance. He has been instrumental in providing strategic counsel and thought leadership for the security and resilience of the power grid and has helped in identifying and understanding emerging threats. Advising corporations throughout North America, Brian has worked to increase physical and cybersecurity mitigation measures designed to deter, detect, and defend critical systems.

Prior to starting his own firm, Brian was the Director of the North American Electric Reliability Corporation's (NERC) Electricity Information Sharing and Analysis Center (E-ISAC) and was charged with leading NERC's efforts to provide timely threat information to over 1900 bulk power system owners, operators, and government stakeholders. During his time at NERC, Brian was also the Director of Critical Infrastructure Protection Programs, where he led the creation of the Grid Security Exercise (GridEx), provided leadership to Critical Infrastructure Protection (CIP) staff, and initiated security training and outreach designed to help utilities "harden" their infrastructure from attack.

John Donlon QPM Chairman of the IACIPP said: I am delighted that Brian has accepted the position as Operator Relations Director, North America with us. Brian has a wealth of experience both as a security practitioner and in an oversight capacity, so he will be a tremendous asset to the organisation and the global CNI community. I'm also pleased to say Brian will be speaking this year's Critical Infrastructure Protection and Resilience, North America to be held in Tampa, Florida in December.

We will continue to welcome new members who share with us the desire to make the world a safer place.

Membership is currently free to government agencies and operators, so if you would like to become a part of our organisation, you can register at: http://www.cipre-expo.com/iacipp-registration

Addressing New Security Challenges at Airports

Security measures at airports have evolved over time to adapt to the new challenges of today's society. Security is no longer aimed at avoiding unintentional intrusion – people who, due to ignorance or scrutiny, invaded the restricted areas of airports –, but at dealing with premeditated intrusion for the purpose of sabotage, smuggling or terrorism.

New security technologies help to avoid these incidents when applied to perimeter protection, outside or inside the terminals, helping security operators to detect threats early enough and react to them.

Intelligent perimeter protection

The implementation of a security policy involves multi-layered protection, the first line of defense being the airport perimeter. Recently, there have been a number of incidents at airports as a result of a security breach in their perimeter, for instance in Atlanta and Las Vegas in the US. Both incidentally and intentionally, such incidents pose an imminent risk to the safety of people and facilities, and they can damage the airport's reputation.

Security guards at the perimeter of an airport are unable to view all cameras that control it, so it is essential to have video analytics systems or other means of detection that alert the security operator in case of intrusion, showing on the screen the associated video image and its location on the plan.

Multi-sensor perimeter detection systems, based on different technologies, such as analytical thermal cameras, radar and motion detectors, are the best tool to protect airport perimeters. Using multiple sensors of different technologies maximizes detection capacity in all environments. However, seamless integration between the different sensors and a unique configuration is necessary to guarantee detection of the intrusion and avoid false alarms.

False alarms can be a major problem if they are not minimized, since the generation of multiple false alarms assiduously ends up causing the security operator not to pay enough attention to them. The only way to minimize them is either using the appropriate video analytics, properly configured and maintained over time, or combining video analytics with other types of sensors so that false alarms can be discriminated.

State-of-the art solutions, such as Siveillance VMS from Siemens, integrate all detection technologies from different manufacturers, either through camera or server-based analytics, radars or other sensors, allowing

their configuration as a whole into a single operating environment and combining the different technologies on the same alarm management system. This helps and guides the operator through automatic rules, live and recorded image and associated drawings.

Use of biometric identification systems

In recent years the demand for biometric identification systems has increased, both to complement security in access control, and to assist with the identification of people in access filters. The new biometric solutions based on video analytics, such as face recognition, are added to existing technologies, such as fingerprint reading. They are now mature tools with a great potential, and they are typically used in the video surveillance infrastructure implemented in airports.

Siveillance VMS is used by major manufacturers of video analytics in the market. It is offered as a platform that integrates the solutions of different manufacturers under the same interface, allowing them to choose the best analytics for each specific case, and combine the alarms and events from all of them in the same application.

It also enables the conversion of the camera on a mobile device or tablet into a CCTV surveillance system camera, sending the video from the mobile as well as its position to the control center, and recording it in the system as one more surveillance camera. This allows security operators to send live videos from their mobile phones, and to receive real time instructions from the control center.

Platform protection

The manoeuvring area and platform, where aircraft are parked, loaded, unloaded and replenished, is always a very sensitive part of the airport security system. To counter potential threats in this area, the latest technologies in video surveillance cameras are required, such as multi-purpose and 360° cameras that offer panoramic views of the area, and advanced video analytics in parking areas allow greater control of the situation and prevent incidents.

Siveillance VMS integrates the most advanced video analytics as well as 360° and multi-purpose cameras, allowing operators to perform the dewarping and stitching processes naturally and improving their field of vision with this type of cameras. Users can also receive the alarms generated by different types of analytics, both in camera and server, from the same interface. On the other hand, its advanced rules engine triggers a series of actions based on any event and alarm, such as showing the operator the camera alarm live while showing the last seconds captured as well as the location map.

Werner Braun, Global Security Portfolio Head, Siemens Building Technologies

Siveillance VMS integrates all detection technologies

Siemens Siveillance VMS is an IP video management (VMS) software designed for large security installations. It integrates more than 7,000 devices from different manufacturers, such as cameras, encoders, or radars, as well as different manufacturers of video analytics on standard hardware. It has Windows, Web and mobile clients, and the mobile device can be used as a security camera. It also includes video wall management, intelligent metadata search, ONVIF gateway for video retransmission, and integration with a large number of video analytics and access and intrusion controls. Siveillance VMS comes in different versions to suit both small security installations as well as large critical infrastructures. It is integrated with anti-intrusion and access control systems. It can also be integrated with BMS solutions, such as Desigo CC from Siemens, providing, in this case, unique management of safety, fire protection and control of facilities.

Wire-Line Well Logging: Regulatory Requirements for the Safe Storage of Nuclear Source Material in the US Oil and Gas Industry

In this article Mark Barbaric, Security Program Manager, Convergint Technologies looks at some of the US regulatory issues around the protection of radioactive materials within the oil and gas industry.

Due to the terrorist attacks in New York City on September 11, 2001, several orders and regulatory measures were put in place by the US Nuclear Regulatory Commission to safeguard nuclear materials from home-grown or international terrorism.

One of those regulations, 10 CFR Part 37, went into effect May 20, 2013 "to provide a reasonable assurance of preventing the theft or diversion of Category 1 and Category 2 quantities of radioactive materials" in use by licensed civilian organizations. The regulation requires that licensees meeting the outlined criteria of certain aggregated nuclear sources must have a physical protection program in place to safeguard these sources.

Oil and gas exploration companies must apply to the Nuclear Regulatory Commission (NRC) for licenses to use nuclear sources for well exploration. Various types of sources can be used for a process called wire-line well logging: the use of radioactive material to determine the geological nature of a well by dropping a radioactive source down the borehole. Common sources for well-logging include a neutron source (which is used to help determine hydrogen-based compounds such as oil, gas, and water) and a gamma source (which is used to measure both density and porosity of the surrounding material). Backscattered gamma emissions or neutrons are then interpreted on

charts and logs to determine the well's ability to produce oil or gas.

Wire-line trucks, used for the specific task of well-logging, travel from various oil and gas field locations to and from vaults located in regional security zone depots, where the source materials are kept when not in active use.

How do the regulations affect the oil and gas Industry?

Regulation requires the licensee of nuclear source material to "establish, implement, and maintain a security program that is designed to monitor and, without delay, detect, assess, and respond to an actual or attempted unauthorized access to Category 1 or Category 2 quantities of radioactive material." While 10 CFR Part 37 covers the requirements of the overall security program, typically security integrators are tasked with providing a turnkey solution to their oil and gas customers to meet requirements for permanent regional source storage depots, referred in sub-section 37.47 as "Security Zones."

As a minimum, security zones are defined in one or a combination of three ways. First, they may be surrounded by physical barriers, either natural (rock or solid earth) or man-made (fencing, walls, and other physical barriers), and allow for unescorted access by only authorized individuals, through an established and controlled access point. Second, they may be under direct control by authorized individuals at all times, a practical solution for temporary security zones more so than permanent security zones. Third is to maintain a combination of physical barriers and direct control.

In permanent security zones, the higher degree of physical control through electronic card access reduces the potential for human error in overseeing the controlled access point. It may also provide for significant cost reduction in manpower since authorized access points can be monitored remotely and electronically.

For these reasons, best practices learned through our years of experience include establishing these controlled access points through fencing and leveraging electronic access control card readers and electromagnetic locks.

While the licensee has the option of direct surveillance and control, meeting this requirement requires a full-time physical presence of an authorized person with constant direct surveillance of the security zone. The introduction of an access-controlled door or a gate integrated with cameras provides the licensee with accountability logs and recorded video to be made available to local law enforcement and NRC compliance inspections.

Adding an access control reader also assists the licensee with the rule requirement to prevent circumvention of the security program background check and documented approval process, reducing the chances of permitting high-risk individuals from becoming authorized personnel.

Licensees of nuclear source materials are required to establish and maintain the capability to monitor and detect any unauthorized individuals entering into the security zone and the unauthorized removal, sabotage, or diversion of source material, even in the event of power failure.

Monitoring and detection can achieved in a number of ways, including intrusion detection systems linked to an offsite 24/7 central monitoring facility, electronic devices that can detect intrusion and alert nearby facility personnel, monitored video surveillance systems, direct visual surveillance by authorized personnel within the security zone, or direct visual surveillance by an individual designated by the licensee from outside of the security zone.

Prudence dictates having a documented process for monitoring and detecting through one or more of these requirements to ensure that there are no gaps in security.

As with control of the security zone, monitoring a permanent security zone with full-time authorized personnel can be cost-prohibitive

and high risk, as it relies on human compliance. Our experienced subject matter experts have found that intrusion detection through a centrally monitored access control system can eliminate the reoccurring monthly cost of a 3rd party alarm monitoring contract as it leverages the equipment already designed to control access.

A well-designed security system also integrates video with both local and remote intrusion, as well as access control alarms, to ensure compliance with the 10 CFR Part 37 requirement. Video surveillance may also be used on occasion to remotely monitor unauthorized personnel in the security zone, provided there is direct surveillance at all times. In addition, for Category 1 materials, the zone must also have immediate detection of any attempted unauthorized removal of source material through electronic sensors, video surveillance, or direct surveillance.

Licensees must also implement a maintenance and testing program for assurance that intrusion alarms, communication systems, and other critical physical components of the permanent security zone remain in operable condition and performing as intended. Annual contracts with the licensee's security integrator can cover the requirement to document periodic inspections and testing, performed as per manufacturer's requirements, or at most every 12 months.

Two years following the implementation of the final rule, a program review team was formed to evaluate the regulation's effectiveness and reported their findings to the US Congress on December 14, 2016. The committee found that the program was indeed effective in achieving its original objective to "provide reasonable assurance of the security of Category 1 or Category 2 quantities of radioactive material by protecting these materials from theft or diversion." It also recommended its indefinite continuance along with outreach efforts to stakeholders to provide additional guidance.

Global security requires regional support, INTERPOL Chief tells EAPCCO meeting

Addressing the 20th Eastern Africa Police Chiefs Cooperation Organization (EAPCCO) General Assembly, INTERPOL Secretary General Jürgen Stock underlined the importance of regional and global connectivity for effective law enforcement.

As part of INTERPOL's commitment to the region, Secretary General Stock said the launch of the I-ONE project earlier this year will see the modernization of 31 National Central Bureaus (NCBs) throughout Africa, more than half of which are in EAPCCO countries.

The project will also see frontline police at border control points given access to INTERPOL's secure global police communications network, I-24/7. This will enable officers to check vital police information in INTERPOL's databases to better detect criminals and criminal activity.

In addition to technological assistance, Secretary General Stock also highlighted the ongoing operational support provided by INTERPOL to member countries, in particular the recent Operation Sawiyan in Sudan.

Nearly 100 victims of human trafficking and migrant smuggling were rescued in the INTERPOL-coordinated operation involving some 200 Sudanese officers.

With biometrics playing an increasingly important role in security, the INTERPOL Chief said the Organization would continue to proactively deploy teams to help national authorities gather data, as well as provide the necessary training, equipment and expertise to boost these efforts.

Germany and Sweden Take Action Against Cyber Fraud Gang

With the support of Europol and Frontex, two suspects were arrested in a series of coordinated raids across Germany and Sweden in an investigation targeting a Syrian organised crime group suspected of cyber fraud. House searches were carried out in Aachen, Dortmund and Essen (Germany), and in Nörrköping, Malmö and Helsingborg (Sweden), where police recovered some EUR 54 000 and USD 55 000. The arrestees are believed to be the key organisers of a cyber fraud gang.

The German Federal Police initiated Operation GOLDRING in October 2017. The intelligence-led operation uncovered the organised crime group, composed of Syrian nationals, which was involved in fraudulently purchasing airline and train tickets. According to information from Germany, more than 493 fraudulent bookings were identified. In most cases the tickets were one way tickets from Beirut to European Member States. The tech-savvy smugglers avoided detection by making the bookings using compromised corporate credit cards and credentials, purchased online from other criminals offering them for sale (see: crime-as-a-service business model).

The fraudulent bookings were brought to the attention of law enforcement by the private sector, highlighting once again how instrumental public-private partnerships are in fighting this type of fraud. This effective working relationship has been established over the course of recent years as a result of Europol's Global Airport Action Day, a recurrent operation bringing together law enforcement, the airline industry and payment card companies to target airline fraud. As part of this operation, Europol and Frontex have jointly identified significant crossovers between payment card fraud and irregular migration and trafficking in human beings, leading to a number of arrests in recent years. The operational successes of today have confirmed this trend.

Europol's European Cybercrime Centre (EC3) actively supported the investigation from the outset, assisting with identifying suspects and exchanging information with other law enforcement authorities through Europol's secure communication channels. A Europol mobile office was deployed to Germany, allowing for the real-time exchange of operational information between all involved parties.

Drone technology: security threats and benefits for police focus of INTERPOL forum

The drone whizzed over the heads of the crowd seated in the auditorium of the INTERPOL Global Complex for Innovation (IGCI) in Singapore, performing aerial manoeuvres displaying its ability to operate in enclosed indoor spaces.

A second demonstration showcased drones designed for use in outdoor spaces, highlighting the benefits and also challenges of deploying such technology in public areas.

Drone technology was front and centre at the IGCI this week during the Drone Expert Forum, a three-day conference which brought together nearly 100 experts from law enforcement, academia and private industry to demonstrate how drones can at the same time be a threat, particularly for critical infrastructure, a tool and source of evidence for police worldwide.

The potential use of drones in a terrorist incident or attack against a critical infrastructure and soft targets is a growing concern for law enforcement as the availability of drone technology becomes more widespread globally. As drones become less expensive and their potential applications continue to expand, it is expected that countries will witness an increase and evolution of this threat.

Recent examples include terrorist groups using drones in surveillance activities

and delivering chemical, biological, radiological, nuclear and explosive materials in conflict zones, and an environmental group which repurposed a hobby drone to enter the secure airspace of a nuclear site and crash into a building highlighted the current reality of the threat posed by the illicit use of drones.

In this respect, experts from the FBI, NATO, the United Nations Security Council Counter-Terrorism Executive Directorate, national police agencies and the private sector underscored the need for a coordinated global law enforcement response which combines the expertise and developments made by various countries, military agencies and private industry to counter the threats posed by the nefarious use of drones.

"The rising threat of terrorist groups using drones to attack critical infrastructure and soft targets has created a pressing need for the global law enforcement community to exchange information and share best practices. INTERPOL is committed to assisting its member countries protect their critical infrastructure by raising awareness, sharing best practices and facilitating information exchange on terrorist incidents involving drones," said INTERPOL's Director of Counter-Terrorism, Patrick Stevens.

A tool for police

While drones can be dangerous in the wrong hands, they are also a valuable tool for law enforcement. Participants heard how drones can be used by police to reconstruct a crime scene by using a drone to take pictures of the site from all angles, then feeding the data into a 3D printer.

Drones can also be used by law enforcement to conduct surveillance, assist with traffic accident investigations, survey natural disaster sites and more.

The conversion of drones and artificial intelligence (AI) technology offers additional benefits to enhance current police capabilities, from increasing officer safety and productivity to live-streaming of incidents.

A source of evidence

Drones can also be a significant source of evidence to support investigations and prosecutions: analysis of digital data such as speed, height, GPS coordinates and flight records can reveal information about the criminals involved, while physical data such as fingerprints and DNA can also be present.

Through further development of these capabilities, INTERPOL seeks to support member countries in increasing information sharing on drone incidents and developing their abilities to conduct effective forensic examinations of seized drones.

"Different countries view drone technology in different ways: some define drones as a weapon, while others categorize them similarly to airplanes. On top of that, police are starting to use drones as a tool in their daily operational work," said Anita Hazenberg, Director of the INTERPOL Innovation Centre.

The EU has approved new measures to combat terrorist financing, by preventing money laundering and tightening cash flow checks

The two laws will make it harder for terrorists and criminals to finance their activities, by closing the loopholes in the current money laundering rules and by making it easier for the authorities to detect and stop suspicious financial flows.

Ignazio Corrao (EFDD, IT) said: "The new rules on criminalisation of money laundering hit criminals where it hurts them most: money. The rules prevent criminals from financing their activities - legal or illegal - with the proceeds of illicit actions. Money laundering is a dangerous crime and its harmful consequences are often underestimated. This directive adds a new important tool to fight against this crime. "

The new rules to prevent money laundering introduce:

EU-wide definitions of money laundering-related crimes,

EU-wide minimum penalties, such as a minimum of four years of imprisonment for money laundering maximum sentences, and new additional sanctions, such as barring those convicted of money laundering from running for public office, holding a position of public servant and excluding them from access to public funding.

Juan Fernando López Aguilar (S&D, ES) said: "To properly fight economic fraud, money laundering and terrorism financing, the EU must reinforce its controls over cash entering or leaving its territory. We have incorporated the best practices at international level to new rules and solved some deficiencies and shortcomings of the current legal framework."

Mady Delvaux (S&D, LU) said: "Cash is difficult to trace and easy to transfer, therefore criminals frequently use it. With this regulation, we are strengthening the tools to combat money laundering and terrorist financing through better and faster exchange of information between authorities, as well as by adopting a more complete definition of cash."

How is Artificial Intelligence is Reshaping Surveillance?

When we spot a CCTV camera in person, it's hard not to get the gut feeling that someone is watching you. In a way, that's historically been one of the benefits of CCTV systems—the feeling that someone is watching can impact how we behave, but the reality is, many CCTV systems are left unmanned. This is because having security personnel to constantly and vigilantly watch a camera system just isn't practical or cost-effective. The good news is: artificial intelligence is reshaping how we view optical security systems and is changing the landscape of the surveillance industry.

Perhaps the largest benefit of systems that utilize artificial intelligence is how quick you can get results out of it. AI can be used to analyse video feeds just about instantly, discerning everything from recognized faces to recognized actions or behaviours. If it sounds like a powerful tool, that's because it is—and it's only growing in its capabilities and applications. We're likely to see even more improvement, such as searchable video that can show you exactly what you want when you want it, in the future.

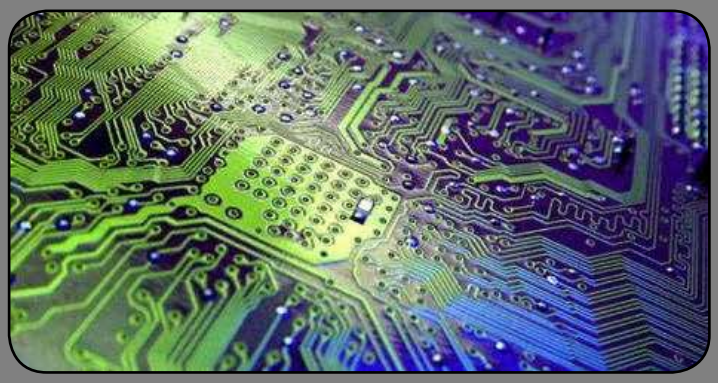
In the past, resolution has been a limiting factor. CCTV cameras were lauded for their laughable grainy quality that often ended up offering few details about what went on at the scene of an incident. Nowadays, optical camera quality has increased tenfold, which allows intelligent optical systems to do their job. With the proper resolution, it makes it much easier for the intelligence behind these surveillance systems to pick out the proper details and work effectively when and where you need it.

As powerful as our current intelligent optical systems may be, there are still limitations. Most of these systems take advantage of machine learning, meaning that they're very good at doing one specific thing: spotting patterns or learning to recognize very specific traits in a video. Still, these systems certainly aren't capable of the same insight as a human operator. They may be able to recognize that someone on camera is running, but they lack the capabilities of knowing why that person is running or understanding context. Only time will tell how and in what ways this may change in the future.

Source: Gatekeeper Intelligent Security

ManTech Wins $668 Million Prime Contract for CDM with Department of Homeland Security

ManTech has announced a $668 million GSA FEDSIM award to support the Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) Dynamic and Evolving Federal Enterprise Network Defense (DEFEND) program. Under the new six-year agreement, ManTech will serve as the prime contractor providing CDM capabilities and support to DHS and the 9 agencies in CDM Group E, strengthening their cybersecurity posture and improving their ability to rapidly respond to today's rising threat of cyberattack.



The objectives of the CDM DEFEND effort are to reduce agency threat surfaces, achieve advantageous cost and price discounts for tools and capabilities, and accelerate the implementation and adoption of the CDM program within participating agencies.

Under this new task order, ManTech will support CDM efforts within the Department of Education (ED), Department of Housing and Urban Development (HUD), the HUD Office of Inspector General (HUD OIG), the Environmental Protection Agency (EPA), the Federal Deposit Insurance Corporation (FDIC), Nuclear Regulatory Commission (NRC), National Science Foundation (NSF), Securities and Exchange Commission (SEC), and Small Business Administration (SBA).

"ManTech has played a strategic role in the CDM program for over three years, supporting more than 65 agencies in both Phases 1 and 2, and we're honored to continue supporting the CDM program's critical role in defending federal networks," said Kevin Phillips, ManTech president and CEO. "This latest award underscores their confidence in us as a long term trusted partner."

"Government agencies are increasingly the target of sophisticated cyber threats. We're excited to support the CDM program to rapidly implement advanced cyber capabilities and secure the critical missions of our customers," said Rick Wagner, president, ManTech's Mission, Cyber & Intelligence Solutions (MCIS) group.

DHS's CDM program provides federal agencies with access to commercial solutions to rapidly identify cybersecurity risks and prioritize risks to mitigate the most significant problems first.

LRAD Corporation Announces $1.0 Million Mass Notification Critical Infrastructure Order

LRAD Corporation a provider in long range voice broadcast systems, and advanced mass notification and distributed recipient solutions, today announced a $1.0 million mass notification systems order for the first phase of a Federal Emergency Management Agency ("FEMA") funded critical infrastructure project. The order consists of fixed LRAD DS-60XL and mobile LRAD 360XT voice broadcast systems.

"Government officials and emergency managers throughout the world are recognizing that broadcasting clear voice warnings and instructions to affected populations in advance of, during, and after disasters saves lives," stated Richard S. Danforth, Chief Executive Officer of LRAD Corporation. "The LRAD systems ordered for this project feature our solar power option and satellite connectivity, ensuring continual operation if the power and communications infrastructure fails."

Danforth added, "This competitively won award is part of a potentially larger program to provide a standard, unified mass notification system for this region's populated areas, and to speed disaster response and recovery."

Powered by LRAD's proprietary XL driver technology, LRAD DS-60XL systems are housed in all-weather enclosures and feature 60° - 360° broadcast area directionality and exceptional vocal clarity.

Fully self-contained and self-powered, the LRAD 360XT mobile mass notification system delivers highly intelligible voice and alert tone broadcasts with uniform 360° coverage from a rapidly deployable, telescoping 30-foot pneumatic mast. The LRAD 360XT is integrated and mounted on a ruggedized trailer featuring securely mounted, lockable electronics and equipment enclosures containing the amplifier modules and pneumatic systems.

Russian Helicopters to supply 150 medical helicopters to the national air ambulance operator

Russian Helicopters, National Service of Medical Aviation and Avia Capital Services LLC have signed a contract to supply 104 Ansat and 46 Mi-8AMT medically equipped helicopters.

The agreements on helicopters delivery will be implemented as part of a large-scale project of Rostec State Corporation on creating a single operator of air ambulance services in the regions of the Russian Federation. In the presence of Minister of Industry and Trade of the Russian Federation Denis Manturov, the document was signed by Andrey Boginskiy, Director General of Russian Helicopters, Ruslan Golik, General Director of National Service of Medical Aviation, and Roman Pakhomov, General Director of Avia Capital Services LLC .

"Development of EMS aviation is one of the priorities of the "Health" national project. Rostec

implements a comprehensive project in this area on establishing a special air ambulance service, providing it with aircraft and building the necessary ground infrastructure. 150 helicopters will be manufactured and delivered specifically for NSMA — this is a record number of helicopters made for EMS aviation. Investments in the project exceed 40 billion rubles. The complex of measures that we implement will allow the new service to effectively carry out life-saving missions," stated Sergey Chemezov, CEO of Rostec State Corporation at the signing of the contract.

Last year, Rostec State Corporation undertook the initiative on creating a united system of air ambulance in Russia, which was supported by the President of Russia. The purpose of the National Service of Medical Aviation is to perform operations providing medical care 24/7 in accordance with a common standard. The project is financed by Avia Capital Services LLC, which procures helicopters and provides them to the National Service of Medical Aviation for 15 years on financial lease terms.

The National Service of Medical Aviation is already transporting patients in need of emergency care in Saint Petersburg, the Moscow Region, the Leningrad Region, the Sverdlovsk Region, the Novgorod Region and Karelia.

Under the contract, at Hydroavaisalon, the first Mi-8AMT EMS helicopter was officially handed over to NSMA. The helicopter is fitted with the necessary medical equipment for resuscitation on board, including an artificial lung ventilation system and a Tele-ECG machine which reads an electrocardiogram in real time.

The Mi-8AMT and Ansat medical helicopters meet all international air ambulance standards and have the necessary equipment to provide medical care during patients' transportation.

360 Vision's Invictus onboard Robot Jack

TBC-France a supplier of advanced security robotics solutions has incorporated 360 Vision Technology's new Invictus high-performance ruggedised all-in-one PTZ camera into its advanced autonomous security robot, Jack.

Developed in Europe, robot Jack has been designed to provide security companies with an effective solution for live roving surveillance of sensitive sites, such as large outdoor or indoor warehouses, ports, industrial complexes, gas and oil facilities, solar power stations, prisons or military bases, etc. An autonomous robot built to exacting standards of component quality and durability, Jack can be deployed to enhance the security surveillance of any critical/sensitive site.

Milestone XProtect gets Smarter and More Secure

Milestone XProtect 2018 R3 video management software brings tighter integration of cameras with built-in analytics starting with Axis cameras, stronger and more secure system documentation and extended audio support to remote users.

With this third release in 2018, Milestone is continuing to respond to the demands from the partner community. We live in an ever-changing world, and the frequent release cycle ensures that the needs of Milestone stakeholders are rapidly met.

Many modern-day surveillance cameras are shipped with advanced analytical functions like motion detection,

temperature detection and perimeter protection. These camera functions generate events. With the versatile Rules Engine in Milestone XProtect VMS, these and other device inputs can be used to trigger actions like starting and stopping recordings, manually or automatically, sending alerts or other responses.

With the 2018 R3 product version and Device Pack 9.9a, users can benefit from an extended event list, allowing them to make use of all the event features the camera has to offer. This improvement starts with support for Axis network cameras, enabling the Axis Camera Application Platform (ACAP) to work even better with XProtect.

An important aspect in keeping a video system secure and best protected against attacks or unwanted behavior is having a clear understanding of what is happening in the system. Here the Log Server plays a vital role storing all log messages for the entire video monitoring system. This provides information about patterns of use, access logging, system performance and administrative activities.

Smiths Detection Inc. Receives $10M Order from DNDO for Handheld RadSeeker Radiation Detectors

Smiths Detection has announced an order of more than $10 million to supply its RadSeeker handheld radioisotope detectors and identifiers for screening at Customs and Border Protection (CBP) ports of entry. The order is part of a five year indefinite delivery/ indefinite quantity (IDIQ) contract with DHS Domestic Nuclear Detection Office (DNDO), which was announced in January of 2016.

RadSeeker is a next-generation, highly accurate radiation detection and identification system. It can locate the source of

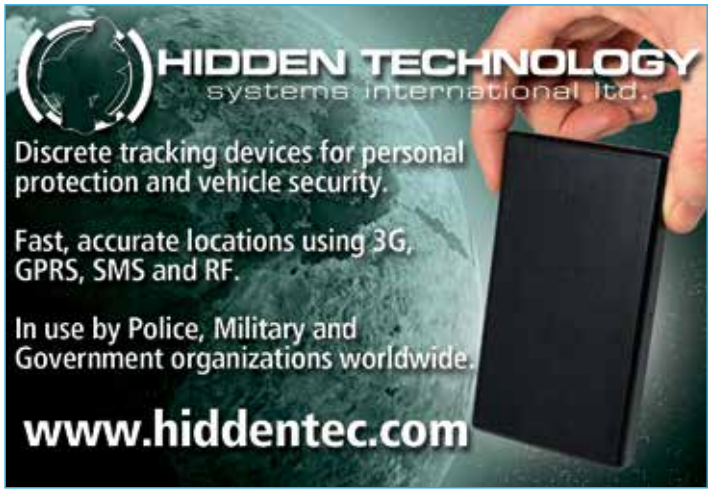
radiological material and identifies if it is harmful or naturally occurring. RadSeeker is the result of several years of collaboration between Smiths Detection and the DNDO to develop a next-generation device suitable for secondary screening, small-area search and rapid mobile identification.

RadSeeker excels in complex real-world environments, providing the operator with quick, simple, specific information for threat assessment.

Shan Hood, President of SDI, said, "RadSeeker is a great example of how Smiths Detection works with customers, such as DHS, to create solutions that meet their needs and prepare them for the future. We look forward to continuing to develop innovative technology solutions, by working with DNDO and other agencies, whose mission is to make the world safer."

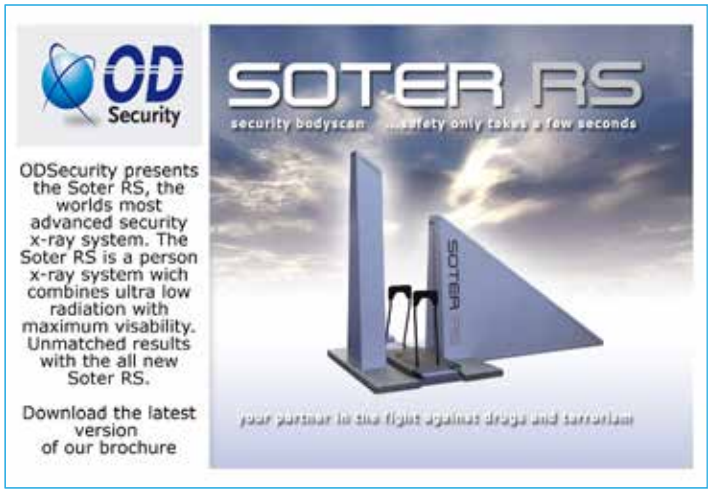
World Security Report

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.



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.



October 2018

2-4
Critical Infrastructure Protection & Resilience Europe
The Hague, Netherlands
www.cipre-expo.com

2-4
Cyber Security Week
The Hague, Netherlands
www.cybersecurityweek.nl

15-18
International Conference on the Internet of Things
Santa Barbara, California, USA
iot-conference.org

25-27
IFSEC Southeast Asia
Bangkok, Thailand
www.ifsec.events/sea/

29-31
Milipol Qatar
Doha, Qatar
en.milipolqatar.com

November 2018

8-10
Secutech Thailand
Bangkok, Thailand
www.secutechthailand.com

15
Cyber Security Summit
London, UK
cybersecuritysummit.co.uk

27-28
ICAO Global Aviation Security Symposium 2018
Montreal, Canada
icao.int/meetings/AVSEC2018/Pages/default.aspx

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

28-29
International Security Expo
London, UK
www.internationalsecurityexpo.com

December 2018

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

March 2019

19-21
World Border Security Congress
Casablanca, Morocco
www.world-border-congress.com

ADVERTISING SALES

Annabel McQueen
(Rest of World)
E: annabel.mcqueen.am@gmail.com
T: +44 20 8249 6152

Jerome Merite
(France)
E: j.callumerite@gmail.com
T: +33 (0) 6 11 27 10 53

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

csm-ace 2018

10th CYBER SECURITY MALAYSIA AWARDS, CONFERENCE & EXHIBITION

24 - 28 September 2018 | Royale Chulan, Kuala Lumpur

Theme:

PARTNERSHIP IN SECURING 4IR TOWARDS NATIONAL SOVEREIGNTY

Cyber Security Malaysia Awards, Conference & Exhibition (CSM-ACE)

is a prestigious cyber security event organised by CyberSecurity Malaysia in collaboration with the National Cyber Security Agency (NACSA), and endorsed by the National Security Council.

The biggest cyber security industry event in Malaysia and the only 3-in-1 cyber security event in the region.

AWARDS, CONFERENCE & EXHIBITIONS

- GLOBAL TALK PROSPECTS
- PARTNERSHIP OPPORTUNITIES
- TECHNOLOGY SHOWCASE

As Sponsor & Strategic Partner:

- Gain inroads into the Malaysian information security market
- Forge strategic partnerships and ink business deals
- Impart your thought-leadership
- Promote collaborative technology research, development and innovation
- Increase brand recognition and visibility

As Exhibitor:

- Showcase and promote innovative information security solutions
- A market place to look for strategic business partners and buyers
- Participate in business matching activities

As Training Provider:

- Increase brand recognition and visibility
- Knowledge sharing on technology research, development and innovation
- Profit sharing opportunity
- Impart your thought-leadership

OPENING & KEYNOTE
- 4 Keynotes Session

CONFERENCE
- Management & Technical Track
- International Speakers
- Talking Slot Opportunities

IT SECURITY EXHIBITION
- More than 40 Exhibitors
- 3 Days Exhibitions
- Business Matching

GLOBAL ACE CERTIFIED TRAINING PROGRAMS
- 9 Certified Professional Training
- HRDF Claimable

MALAYSIA CYBER SECURITY AWARDS 2018 & GALA DINNER
MALAYSIA CYBER SECURITY AWARDS 2018
- Awards Recipients Night

BUSINESS OPPORTUNITIES
- Tech Talk Seminar by Partners
- B2B Session
- Networking Event

CYBER COLLOQUIUM
- Collaboration Program with Universities

SATELITE EVENT
- NICTSED 2018
- YAKSHA
- MTCP
- Various Event by Partners

Organised by: CyberSecurity MALAYSIA

In Collaboration with: NACSA – Agensi Keselamatan Siber Negara / National Cyber Security Agency

Endorsed by: NATIONAL SECURITY COUNCIL

Supported by: MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA

Gold Partner: BAE SYSTEMS

For more information about CSM-ACE 2018, go to www.csm-ace.my