World Security Report

For the latest news, features, essential analysis and comment on security, counter-terrorism, international affairs, warfare and defence

January 2015

Subscribe Here

www.worldsecurity-index.com

Editorial:
Tony Kingham
E: tony.kingham@worldsecurity-index.com

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

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

Advertising Sales:
Tony Kingham
T: +44 (0) 208 144 5934
M: +44 (0)7827 297465
E: tony.kingham@worldsecurity-index.com

Paul Gloc (UK & Europe)
T: +44 (0) 7786 270820
E: paulg@torchmarketing.co.uk

Denne Johnson (Americas)
T: +1 918 863 9792
E: dennej@torchmarketing.co.uk

Subscriptions:
Tony Kingham
E: tony.kingham@worldsecurity-index.com

World Security Report is a bi-monthly electronic, fully accessible e-news service distributed to 38,000 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.

Je suis Charlie

The recent tragic events in France make depressing reading, but are unfortunately no surprise. The reality is that events like these were always likely to happen and will happen again.

Why, because it is impossible to be secure everywhere in a free society and it is the determination of the terrorist to seek the element of surprise. They have a plethora of soft-targets to choose from and you simply cannot be secure everywhere all the time!

The Charlie Hebdo attack also highlights the fact that even if you have identified a high priority target, how secure is secure?

The Charlie Hebdo office was guarded by an armed police officer, who was tragically killed doing his duty, as well as a police officer patrolling the area. They were killed because they were outgunned, taken by surprise and not mentally prepared for a gunfight. When the officers left for work that morning they were expecting a routine shift in the centre of a highly civilized city. The terrorists left that morning heavily armed, pumped with adrenalin and fanatical religious zeal, ready to ruthlessly kill or be killed. The outcome was never really in doubt.

Now the questions have started about how this could have happened when the perpetrators were known to the security services, and one of the attackers Cherif Kouachi had already been convicted of terrorism offences and served 18 months in prison.

The fact is that the security services in democratic nations have limited resources and have to make difficult decisions about who should and who shouldn't be kept under surveillance. Clearly, in this case, it was a fatal error of judgement but that is also inevitable.

So what lessons can be learnt from this tragedy?

There has been a lot of talk amongst politicians about increased resources and sharing of information amongst European nations.

Well, more money and resources are obviously necessary and welcome but in these cash strapped times will they be enough? We are facing a growing radicalisation of young Muslims citizens in Europe and a huge increase in numbers of those who have been to Syria and Iraq, that have returned home trained, experienced and motivated.

EUROPOL Director, Rob Wainright, told a UK Home Affairs Select Committee that: "We're talking about 3,000-5,000 EU nationals."

"Clearly, we're dealing with a large body of mainly young men who have the potential to come back and have the potential or the intent and capability to carry out attacks we have seen in Paris in the last week." He went on to say: "The reality is the security authorities today don't have the necessary capability to fully protect society from these kinds of threats."

Sharing information on people movement among EU member states, again is a welcome start but definitely not enough. Identifying individuals that are making their way back to Europe from Syria or Iraq, starts by knowing they have gone there in the first place. And how can that be achieved with only part of a picture.

Exit checks at border crossings and information sharing would need to be truly international; otherwise it is all too easy for our travelling jihadist to simply bypass our notice by travelling to a friendly third nation outside of Europe, before making their way to or from one of the usual entry points, such as Turkey or Lebanon.

At BORDERPOL we have been lobbying for these global measures to be taken for more than 10 years, but to date not even within EU do we effectively share information, and exit checks simply do not exist. So in the light of experience, it is difficult to see this happening any time soon.

It must also be said that information sharing about people movement and exit controls does nothing to address the threat of the lone wolf or home grown terrorists that has never trained and fought in Syria or anywhere else.

So, in the short term what can be done?

Well, as usual good intelligence that stops the event before it happens is our best defence, and the security services have performed admirably in preventing attacks that we know about and others that we don't know about, year in year out. More personnel and resources can only help.

But they also need greater powers, especially in regard to monitoring the internet and social media. It is understandable that civil liberties groups and the public have concerns about privacy, but the reality is that the internet is the chosen command, control and communications system for international terrorist groups, as well as a training manual offering all the information you need to commit atrocities.

In reality, the security services will never have enough time or resources to monitor all the potential threats, let alone checking personal emails of the members of the public, so civil liberties groups should be reassured, although they won't.

Also, more has to be done about the flood of refugees coming into Europe through the Mediterranean. This is not only a humanitarian crisis but if terrorists can't get in via legal means, they will take advantage of the human trafficking channels that already exist, if they are not already. This should be regarded as a European issue and all nations take their fair share of the burden, not leave it to Italy and Greece.

Another issue is the availability of weapons, such as assault rifles and semi-automatic pistols. Cutting off the sources of weapons and monitoring weapons dealers, legal and illegal has to be a priority. After all, not all would be attackers are jihadists. The worst shooting attack in European history was Anders Breivik, a right wing fanatic, who killed 77 people with a home-made bomb and a variety of weapons, including an assault rifle and a carbine in Norway in 2011.

Whilst curbing weapon supply won't stop fanatics from committing atrocities (like the murder of the off duty soldier Drummer Rigby in the UK, committed with cleavers and a car), it will reduce their lethal efficiency.

Lastly, the democratic powers need to hugely increase their military efforts in Syria and Iraq.

Better that the jihadists die fighting there than bring their holy war home.

Tony Kingham
Editor
World Security Report

critical infrastructure PROTECTION AND RESILIENCE EUROPE

incorporating Critical Information Infrastructure Protection

Hosted by:

National Coordinator for Security and Counterterrorism
Ministry of Security and Justice

4th-5th March 2015

The Hague, Netherlands

www.cipre-expo.com

Convene; Converse; Collaborate

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.

The European Union is developing its policy on critical infrastructures in relation to the European Programme for Critical Infrastructure Protection ("EPCIP") which considers measures that will enhance, where necessary, the level of protection of certain infrastructures against external threats.

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

REGISTER TODAY AND SAVE WITH EARLY BIRD

Save up to 20% on delegate fees when you register online and save with the Early Bird discount rate.
(Early bird discount deadline - 4th February 2015)

ADDITIONAL 10% DISCOUNT FOR READERS OF WORLD SECURITY REPORT

As a reader of Crisis Response Journal, you can save a further 10% on your delegate fee by quoting 'WSR10' at the Online Registration at www.cipre-expo.com - Offer ends 31st January 2015.

For further details and to register visit **www.cipre-expo.com**

Opening Keynote Presenters:
- Mr Opstelten, Minister of Security & Justice, The Netherlands
- Mr Fernando Sánchez, Director General, National Centre for Critical Infrastructure Protection (CNPIC), Spain

Speakers include:
- Hans de Vries, Head of National Cyber Security Centre, NCTV, Ministry of Security & Justice, Netherlands
- Benny Jansson, Deputy Head Strategic Analysis Section, Swedish Civil Contingencies
- Evangelos Ouzounis, Head of Unit – Secure Infrastructure and Services, European Union Agency for Network and Information Security – ENISA
- Jakub Boratyński, Head of Unit, Trust & Security, DG CONNECT, European Commission
- Mauro Facchini, Head of Copernicus Services Unit, DG Enterprise and Industry, European Commission
- Andrew Wright, Head of Industrial Resources and Communications Services Group (IRCSG), NATO Operations Division
- Mr. Leif Villadsen, Senior Programme Officer and Deputy Director, United Nations Interregional Crime & Justice Research Institute (UNICRI)
- Christian Sommade, Executive Director, Haut Comité Français pour la Défense Civile (HCFDC), France

Leading the debate for securing Europe's critical infrastructure

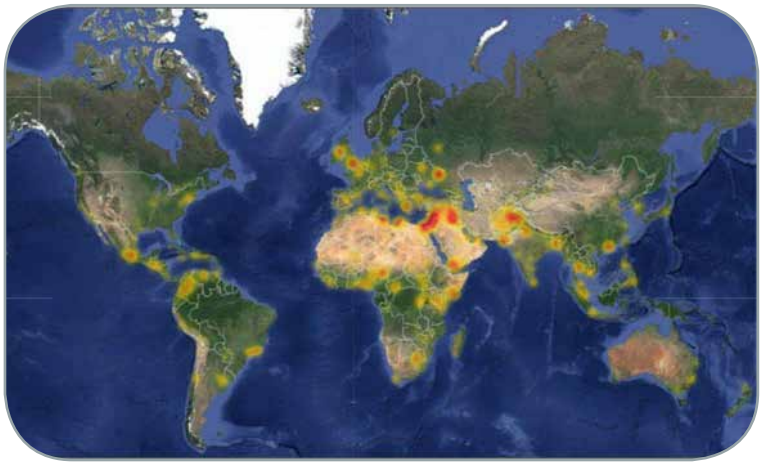
Owned & Organised by: TORCH, KNM Media

Hosted by: National Coordinator for Security and Counterterrorism, Ministry of Security and Justice; the hague

Supporting Organisations: International Association of CIP Professionals, HSD The Hague Security Delta, ISIO, NS&RC, Association of Risk and Crisis Communication, ECIPS

Media Partners: World Security-index.com, World Security Report

G4S Risk Consulting Global Forecast 2015



The Global Forecast 2015 is brought to you by G4S Risk Consulting's team of analysts based around the world. Leveraging five-years' of data and regional expertise, the forecast discusses the most pertinent threats to operating environments in the coming months.

Multiple sources of conflict and unrest have shaken the international community in 2014. From the seizure of territory in Iraq and Syria by militant Islamist group Islamic State (IS), to a proxy war between Ukraine and Russia in the eastern Donbass region, and the largest Ebola outbreak in history spreading through West Africa, it has been a turbulent year. Looking ahead, 2015 is set to see the continuation of these trends, with terrorism, civil unrest and public health among central concerns for risk managers.

Increased Global Terror Threat

Blowback from US-led coalition airstrikes in Iraq and Syria, targeting the Islamic State (IS) and other jihadist groups, will result in an increased terror threat in all coalition partner countries, further exacerbated by the return of foreign fighters and a heightened risk of lone-wolf attacks. Several countries, including the UK, Australia and Canada, have already increased their terror threat ratings over concerns of an increased domestic threat posed by returning fighters. The US issued a warning in September 2014 for security agencies to be on alert for lone-wolf attacks in the country as returnees and self-radicalised individuals increasingly seek to act alone in order to lessen the threat of interception by authorities.

The heightened threat will be driven by increased militant recruitment. Reports of terror-related arrests have increased since September 2014, including in the UK, France, Morocco, Malaysia, India and the US, indicating the growing global draw of IS to alienated individuals. Glorification of the jihad via social media strategies allows IS to reach a wider audience, gaining further prominence.

Global Spread of Ebola

Although the Ebola outbreak has largely been confined to three nations in West Africa, isolated cases may still emerge in countries across the world. Transport hubs are most vulnerable to infections, including the UAE, Istanbul, London and Frankfurt. Unlikely to pose a major threat of outbreak in developed countries, cases in densely populated areas with limited public health infrastructure may result in localised outbreaks, particularly in countries such as India or Brazil. The outbreak will continue to impact upon supply chains and international travel as countries implement heightened border controls to prevent the spread of the virus, potentially requiring adjustments to business continuity planning.

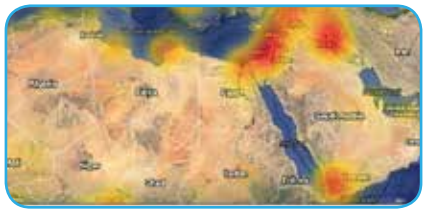
Regional Summaries

Africa

Africa offers a mixture of promising frontier markets and rapidly developing economies, but political risk, localised conflicts, poor socio-economic conditions and inadequate infrastructure mean the continent

will remain a diverse and often challenging region in which to invest and operate. Key concerns persisting into 2015 include the ongoing Ebola epidemic in West Africa, terrorism and insurgency as Boko Haram, al-Shabaab and al-Qaeda continue to pose a threat in specific regions, as do civil conflicts in the Central African Republic, South Sudan and the DR Congo. Political risk is anticipated to increase as a series of long-term presidents face questions of succession or the distortion of constitutional limits, raising the risk of civil unrest from increasingly assertive civil societies and creating volatile investment and policy environments.

Middle East and North Africa



The rise of the Islamic State jihadist insurgency will continue to dominate the security outlook for the Middle East in 2015. However, facing increasing unity among its diverse enemies, the rapid gains made by IS in 2014 are likely to be gradually rolled back in the year ahead, most of all in Iraq. In neighbouring Syria, there are few indications to suggest the conflict will end in 2015. In ungoverned spaces elsewhere in the region, the IS model will attract some adherents, but the overwhelming theme of political struggle will continue to be the confrontation between secular authoritarians and Islamists, as typified by Egypt. Meanwhile, the reluctant rapprochement between Iran and the US will offer a rare opportunity for a regional de-escalation of hostility, but one that will draw enmity from both the region's Sunnis, led by Saudi Arabia, and from Israel.

South Asia

The Subcontinent continues to be dominated by two major issues; the India-Pakistan bilateral relationship and the impact of the withdrawal of NATO troops from Afghanistan. Elsewhere, national capitals will continue to harbour concerns over militancy that has been galvanised by the success of Islamic State (IS) in Iraq and Syria. A business-friendly government in India will help account for much of the region's economic growth, but underlying political fragility, potential for civil unrest and ongoing problems of corruption should be among investor concerns through 2015.

Asia Pacific

Regional relations will be framed within the context of China and the country's dominant role in a range of significant regional issues. These will include China's territorial interests, energy policy and diplomacy, which will unnerve its neighbours. However, the regional security situation will remain stable as leaders concentrate on ambitious domestic reform

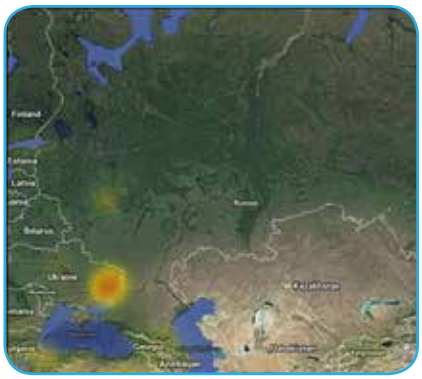
programmes. Governments will continue anti-corruption efforts that will target officials, but also foreign companies, as authorities change and enforce regulations. There remain latent fears over the gradual spread of militant Islam, with national security services set to increase cooperation in order to track suspected militants. Despite the incidence of civil unrest throughout the region during 2014 as a result of political and labour issues, little risk is posed to the internal stability of the countries concerned.

The Americas

Latin America and the Caribbean remains a promising developing market for foreign investors, with declining inequality, a growing middle class and vast natural resources. However, key concerns surrounding security, the economy and political stability will persist

into 2015, centred in particular on organised crime, civil unrest and political interference in national economies. In North America, concerns are growing over the domestic impact of fighters returning from Iraq and Syria and conducting attacks, as well as the growing threat from self-radicalised "lone-wolf" attackers.

Russia / CIS



The consequences of Russia's deteriorating economic outlook and anxiety about the Kremlin's adventurism, most of all in Ukraine, will dominate both the security environment and the investment climate over the coming year. The fall in oil prices will drive political instability and entrenched authoritarian regimes will face growing challenges to their dominance from opposition driven by socio-economic discontent.

Europe

Europe will remain a stable environment for business operations and foreign investment in 2015. However, key issues persisting into 2015 include rising Islamist extremism and radicalism within EU countries, particularly the response to the domestic terrorist threat posed by "lone-wolf" extremists; ongoing austerity measures, which are likely to trigger strikes and protest action; and the potential impact of Russia's perceived belligerence in Eastern Europe.

For a copy of the detailed report click here to download.

For further information and to sign up for a seven-day complimentary trial, please visit:
http://gis.g4s.com

Security management for critical infrastructures

By Ralph Müller, Market Manager Utilities, Siemens Building Technologies

Critical infrastructures ensure the survival of a functioning community. At the same time, they are exposed to any number of hazards. Experts around the globe are working on organizational as well as technical responses to these challenges. At the core is the implementation of systematic security management for critical infrastructures.

ThInCritical infrastructures are institutions and facilities that are vital to the functioning of a public community. If they fail partially or even completely, major supply bottlenecks and serious disruptions to public safety and security can result. Because critical infrastructures are increasingly interwoven and interdependent, serious incidents can set in motion cascade or avalanche effects. Last but not least, terrorist threat scenarios are bringing the security of critical infrastructures to the fore in national and private-sector security policy. Institutions and facilities that need safeguarding include energy supply, information technology, telecommunications as well as transportation and traffic, e.g. airports.

The mutual interdependence of critical infrastructures is not limited to individual sectors but, because of globalization, is increasingly transnational in nature. For example, countries purchase energy from neighboring nations to ensure a continuous supply. If the energy supply in one country is compromised, bottlenecks arise in neighboring countries. Because protecting critical infrastructures is not just a national issue, higher-level organizations such as the European Union have started to focus on it as well.

Safeguards are growing in importance

A recent incident highlights how dire the need for action is when it comes to critical infrastructures. In the spring of 2013, a transmission substation near California's third largest city of San Jose was the target of a night-time attack. Unknown gunmen opened fire on the facility and destroyed 17 out of 21 major Silicon Valley transformers valued at several million dollars each. With a minimum of effort, the culprits took down the entire facility. The attack immediately raised fears in the U.S. that the national power grid could become a terrorist target. These fears were not unfounded, considering it took 27 days to restore operations. Similar cases of intentional sabotage of substations have also occurred in Europe, such as in Great Britain.

Even less dramatic incidents can have serious consequences for critical infrastructures. Remote substations, railway tracks and power transmission lines are not only vulnerable to vandalism and sabotage, but also at risk of theft of valuable metal cables. Rising metal prices worldwide have substantially driven up the number of thefts in recent years. The methods used by thieves, who primarily target copper and nickel, are becoming more professional and aggressive; even armed attacks are no longer rare. The damage total amounts to several hundred million euros annually. Even more serious, however, are the associated disruptions in businesses and public rail traffic.

The introduction of smart grids, intended to optimize the balance between energy supply and demand, will make the

overall energy supply network even more complex. Electronic security solutions can minimize the potential threats in this network infrastructure, thanks to technology such as access control and video surveillance systems.

Research programs on critical infrastructures

Because of this growing risk, government agencies worldwide have begun to define minimum security standards for critical infrastructures. The North American Electric Reliability Corporation (NERC), for instance, is currently working on a security standard for substations. Large-scale security exercises, such as GridEx II in November 2013, produced valuable insights. This effort simulated cyber and physical attacks on U.S. energy supply facilities and tested emergency measures.

In the European Union, numerous research programs are focusing on the protection of critical infrastructures, with cross-border infrastructures of particular interest. The European Reference Network for Critical Infrastructure Protection (ERN-CIP) established by the European Commission aims to strengthen relations between public institutions responsible for protecting critical infrastructures and the private sector. The ERN-CIP project launched in 2011 uses models and simulations to map cross-linked dependencies so sensitivity analyses can be performed. The design and processes of European energy, information and transportation infrastructures are being reviewed to determine if they are adequate for protecting critical infrastructures. The goal of these efforts is to ensure the uninterrupted availability of critical infrastructures.

Siemens study defines security management requirements

From a strategic point of view, it is absolutely essential that risk analysis, planning, communications and coordination of security measures for critical infrastructures be performed centrally. Siemens has been intensely engaged in security management issues for some time. In a recent study, the Building Technologies Division investigated how operators of critical infrastructures manage risk and what they expect from software solutions for security management designed to support them in their tasks. Four areas particularly at risk were studied: energy production and transmission facilities, airports, chemical and pharmaceutical plants, and campus-like environments such as universities.

The vast majority of those surveyed want security management software that first and foremost ensures the safety of individuals. In addition to protecting people, energy suppliers want to ensure a continuous supply of energy to the public as well as to fulfill official compliance regulations. Airport operators, on the other hand, see maintaining air traffic in accordance with official regulations and guidelines as especially important.

What special requirements do the study respondents have for security management software? Modular design that can be customized as needed is at the top of the list.

The software also needs to accommodate the growing need for technical consolidation of command and control stations. This is particularly true for air traffic as well as energy supply.

Siveillance Vantage as a central security solution for critical infrastructures Over many years Siemens has gained a wealth of experience managing the security of critical infrastructures. This knowledge of precise customer needs was built into the Siveillance Vantage command and control solution. This software is specifically designed to support security management in critical infrastructures such as energy supply, airports, seaports, transportation, industrial complexes and campus environments. Whether for daily routine processes or in crises and emergencies, the solution provides real-time, targeted support for a reliable, scalable

and efficient response to security incidents. The software solution is designed for installation in existing IT infrastructures. Open interfaces and integration technologies support the integration of a wide range of security systems. By consolidating these subsystems on one platform and combining all the data in one control point, security officers can quickly assess the current situation, make informed decisions and coordinate the necessary measures. This integrated communication approach saves critical minutes and seconds, thereby ensuring very quick response times to keep the situation under control.

A Geographical Information System (GIS) shows the incident location and the current position of security and safety resources onoverview maps. Security and safety personnel and vital equipment can be pinpointed within a building using floor plans. In addition to displaying the status, availability and current position of resources, the system suggests the best available intervention forces for the task at hand.

Siveillance Vantage offers integrated phone and emergency call handling on a failsafe and networked platform. The software not only sets up connections to the police and fire departments, but also supports radio communication with internal company security personnel. It also offers individual interfaces to internal telephone, communication, alarm, access control, video surveillance and fire detection systems.

In addition, Siveillance Vantage can display messages from the various alarm systems with defined priorities to ensure that the most critical incidents are addressed first. Each alarm and incident can be associated with defined actions, which are then suggested to the operator as the situation warrants or carried out automatically. The software can be adapted to internal security policies, and appropriate measures for daily routines, time-critical procedures, and emergency and crisis situations can be defined.

Conclusion

More than ever before, critical infrastructures are tied to a multitude of security-related challenges. Intelligent software-based command and control solutions like Siveillance Vantage help infrastructure operators face these challenges.

Obama and Cameron: Arm-in-Arm on Cybersecurity

During their bilateral meetings in Washington, D.C. this week, President Obama and UK Prime Minister David Cameron have agreed to further strengthen and deepen the cybersecurity cooperation between their two countries, with a range of collaborative cyber-initiatives that include staging "war games" to test bank readiness.

The news comes in the wake of Obama unveiling a sweeping proposal on data breaches, hacking and information sharing; and after Cameron caused a stir by advocating a prohibition on encrypted communications.

Both world leaders addressed the surveillance piece during a joint press conference from the White House's Oval Office on Friday, with Cameron reiterating the need to be able to intercept suspected terrorist communications.

As far as the war games, the initial joint exercise will focus on the financial sector, with a program running over the coming year.

The first war game of the set will target the City of London and Wall Street, and involve the Bank of England and commercial banks, which will be followed by "further exercises to test critical national infrastructure," according to Downing Street.

The UK's GCHQ and MI5 meanwhile will work with the US National Security Agency and the FBI to create "a joint cyber cell," with an operating presence in each country. The cell will have colocated staff from each agency.

ECIPS warns that terror threat is more likely to increase

The European Centre for Information Policy and Security (ECIPS) said on Friday after successful closure of operation Charlie Hebdo, that terrorists are more like to strike again. According to counter intelligence analyst, there are several countries that stands out and should be on high alert.

Germany, Holland and Belgium seems to be on the top of the list at present with England to follow. The ECIPS said all indicators are

there that this is far from over. It called upon border force to be extra vigilant, especially with new terror trends such as cyber terror and media targets.

New indicators indicates that terrorists are using social media more and more as their messaging and marketing tools. Google also came under the fire for its Google maps. The ECIPS intelligence analytical department stressed and said that it provides a geospatial platform that terrorist could use to recognize their targets and thus such attacks could be planned from outside the EU.

Apparently the Paris headquarters of satirical newspaper Charlie Hebdo attack proofs just that, when the terrorists were looking for the right building but did not recognize it. Probably due to the fact that they have only seen it on Google maps. ECIPS says that these tools are free tools provided whilst governments spends billions in strategic warfare.

More coordinated training is necessary according to several specialist. It seems a coordinated terror risk management programs is necessary that conforms with updated risk management standards, however it is absent at the same time whilst governments implement ISO 31000 risk management standardization.

ECIPS said that this attack could have been avoided and that the officers who knew that these terrorists were on the wanted list and international "No Fly Zone" list should be brought in for questioning by the French government, since, this could be a problem across the EU that needs legal attention and investigation.

It is unclear as to why these terrorist were not monitored but it is very clear that they knew they were not monitored according available intelligence in open source. The ECIPS published a alert month ago warning governments of provocative media and speeches. Have they paid attention 3 officers and 17 civilians would still be alive today.

critical infrastructure PROTECTION & RESILIENCE ASIA

including Critical Information Infrastructure Protection

24th-25th June 2015

Bangkok, Thailand

www.cip-asia.com

Co-Hosted By:

Department of Disaster Prevention & Mitigation

Ministry Of Information and Communication Technology

Electronic Transactions Development Agency

Invitation to Participate

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.

On a country level, there are strategies to deal with infrastructure protection issues. On a regional level, there is the Association of Southeast Asian Nations (ASEAN) Agreement on Disaster Management and Emergency Response (AADMER), under which several teams have been set up to deal with disaster management in general, but none is geared towards the protection of critical infrastructure.

Cyber security is also becoming more prevalent, and as more critical infrastructure becomes connected to the internet and exposed to the dangers of cyber security attacks, new strategies and systems need to be developed to mitigate these threats.

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

- **Learn about the latest issues, threats and risk management challenges.**
- **Share information, case studies and ideas with international colleagues and peers that you need to work with and may rely on in an unforeseen emergency.**
- **Discover the latest in technologies and techniques for better securing your infrastructure and how to incorporate these into continuity plans.**

For further details and to keep up to date with developments visit **www.cip-asia.com**

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

How to Exhibit

Gain access to a key and influential audience with your participation in the limited exhibiting and sponsorship opportunities available at the conference exhibition.

To discuss exhibiting and sponsorship opportunities and your involvement with Critical Infrastructure Protection & Resilience Asia please contact:

Suthi Chatterjee
Exhibit Sales Manager - Asia
Tel: +66 2 247-6533
E: suthi@prmcthailand.com

Paul Gloc
Exhibit Sales Manager – UK & Europe
T: +44 (0) 7786 270820
E: paulg@torchmarketing.co.uk

Denne Johnson
Exhibit Sales Manager – The Americas
T: +1 918 863 9792
E: dennej@torchmarketing.co.uk

Owned & Organised by:

Supporting Organisations:

Media Partners:

The Western and Arab Alliance together across the Levant Region in the fight against extremism

John Baker Head of Global Operations for the National Security and Resilience Consortium www.nsandrc.co.uk and Michael Fuller MBE Chief Executive of the NS&RC Resilience Directorate examine the current issues surrounding the Syrian conflict the ISIS threat and its increasing impact upon the political economic stability and infrastructure of the neighbouring countries.

The Arab spring continues to have a profound effect across a wide geographical region long after its start on the 18th December 2010.

Political stability across North Africa and the Middle East has become increasing complex due to factional, tribal and religious differences and internal conflict .

With Syria at the core of the problem the economic political and social collapse in these regions has created a vacuum now filled by extremist groups.

The failure in Iraq to deliver a stable, politically balanced, well funded, well managed infrastructure has allowed rapid territorial advances by the Islamic State forces ISIS. This advance has been accompanied by a brutal regime of lawlessness causing fear and bloodshed.

The Western and Arab alliance now face ISIS which is well funded and coordinated. It is increasingly difficult to see a short term resolution. to this challenge to peace and democracy.

The war is drawing radicalised and disaffected individuals from across Europe and the rest of the world to fight in Syria and Iraq and the additional challenge now facing governments and the security services is how to deal with those individuals if and when they return.

The attack in Paris highlights the level of threat faced by a free and open society from just a few radicalised extremists . The security services have stated openly that another attack is inevitable and as such all western democracies remain on high alert.

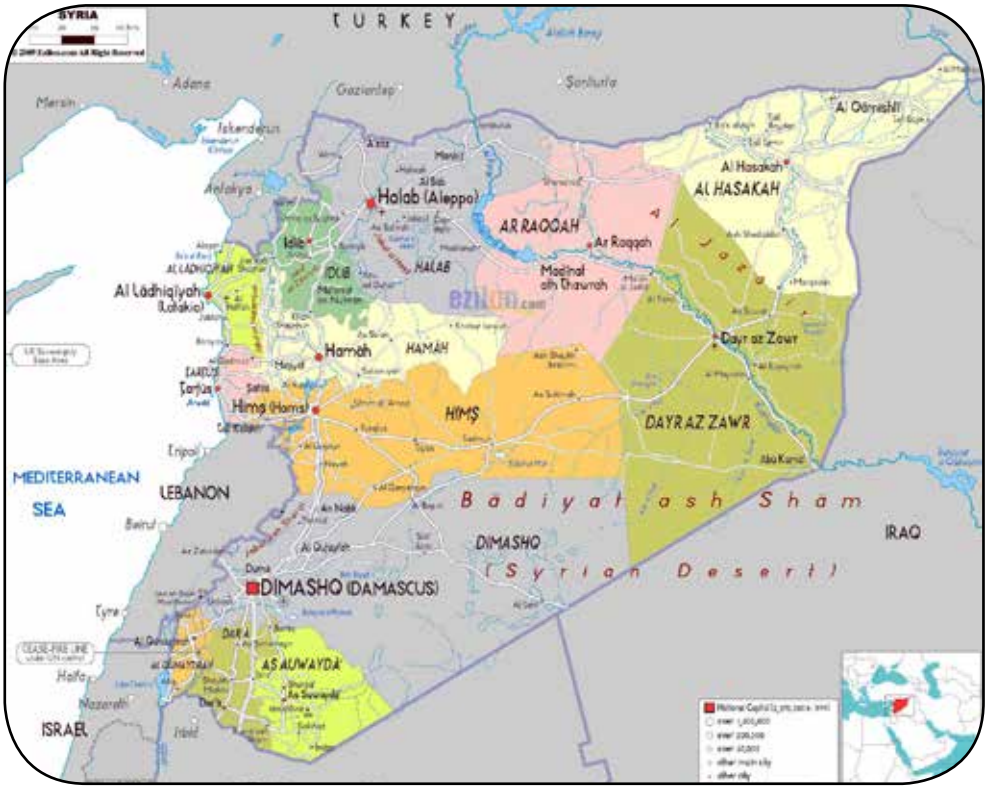
In France the complete protection of national and local infrastructure in the wake of such an attack becomes an impossible task despite the deployment of tens of thousands of security personnel.

The Syrian war and the subsequent emergence and spread of ISIL captured the world's attention and transformed the Levant region in ways one could not have imagined prior to 2011.

As the numbers of dead and of refugees and internally displaced kept climbing, and as families were torn apart and neighbourhoods were turned into war zones, economies slumped and regional economic ties broke down..

The greater Levant area is comprised of : Turkey, Syria, Lebanon, Jordan, Iraq, and Egypt. The direct effect to this region comes from the decline in the size and skills of Syria's labour force due to loss of life and refugee outflows, infrastructure destruction, the trade embargo on Syria, cost-of-doing-business increases, and a decline in productivity. The indirect effect captures the opportunity cost of foregone trade integration initiatives aimed at improving trade logistics and liberalising trade in services

"absorbing the influx of refugees has been an enormous challenge for Syria's neighbours, with strong implications for the stability of the entire region."



Billions in losses

The indirect effect is important to consider because the war disrupted the intra-Levant trade, which grew seven-fold between the early and late parts of the 2000s. It put an end to plans for deepening intra-regional trade ties further following the signing of the "Levant Quartet" agreement in 2010. The benefits of deep trade integration reforms were expected to be sizable.

Areas affected An estimated 9 million Syrians have fled their homes since the outbreak of civil war in March 2011, taking refuge in neighbouring countries or within Syria itself. According to the United Nations High Commissioner for Refugees (UNHCR), over 3 million have fled to Syria's immediate neighbours Turkey, Lebanon, Jordan and Iraq. 6.5 million are internally displaced within Syria. Meanwhile, under 150,000 Syrians have declared asylum in the European Union, while member states have pledged to resettle a further 33,000 Syrians. The vast majority of these resettlement spots – 28,500 or 85% – are pledged by Germany.

While it is true that the EU is a leading contributor of humanitarian aid to the region, the amount donated by each of its 28 member states has varied greatly. Furthermore, while the EU has accepted the vast majority of Syrians who have applied for asylum, it has to date received relatively few requests. Its response to a UNHCR call for more than 130,000 resettlement spots for Syrian refugees between 2013-2016 has also been tepid.

In contrast, absorbing the influx of refugees has been an enormous challenge for Syria's neighbours, with strong implications for the stability of the entire region.

The effect on Lebanon provides a good example of the infrastructure challenges faced by other nations.

Geography of Lebanon

Lebanon is located in Western Asia between latitudes 33° and 35° N and longitudes 35° and 37° E.

The country's surface area is 10,452 square kilometres (4,036 sq mi) of which 10,230 square kilometres (3,950 sq mi) is land. Lebanon has a coastline and border of 225 kilometres (140 mi) on the Mediterranean sea to the west, a 375 kilometres (233 mi) border shared with Syria to the north and east and a 79 kilometres (49 mi) long border with Israel to the south. The border with the Israeli-occupied Golan Heights is disputed by Lebanon in a small area called Shebaa Farms]

Lebanon is divided into four distinct physiographic regions: the coastal plain, the Lebanon mountain range, the Beqaa valley and the Anti-Lebanon mountains.

Lebanon

Lebanon is currently on the front line of the fight againt ISIS.

Lebanon is the second largest recipient of US military aid in the middle East outside of Israel and is also partnering with the UK

Government in order to fund its border security needs through the provision of training, weapons and kit to the military border guards.

The current and long term threat from extremism to Middle Eastern security and global security has found a focus in Lebanon which now represents a 'line in the sand' for western and middle eastern forces currently engaged in the war against ISIS and the spread of its violent and brutal ideology.

Political parties

March 14 *- Pro-western Sunni-based alliance named after mass demonstrations that followed killing of ex-premier Rafik Hariri*

Hezbollah *- Pro-Syrian Shia military/political movement that fought Israel in the 2006 war. Leads alliance of Shia Amal militia and Christian Free Patriotic Movement*

On 27 December 2013, former Minister of Finance Mohamad Chatah, a senior aide to former Prime Minister of Lebanon Saad Hariri, was killed along with seven others in a car bomb explosion in downtown Beirut, a security source said The 62-year-old was on his way to a March 14 coalition meeting at Hariri's residence.

A year after neighbouring Syria began its descent into civil war in 2011, deadly clashes between Sunni Muslims and Alawites in Tripoli and Beirut raised fears that the conflict was beginning to spill over the border and that Lebanon's already fragile political truce could once more collapse into sectarian strife.

In 2012, the Syrian civil war threatened to spill over in Lebanon, causing more incidents of sectarian violence and armed clashes between Sunnis and Alawites in Tripoli. As of 6 August 2013, more than 677,702 Syrian refugees were in Lebanon.. As the number of Syrian refugees increases, the Lebanese Forces Party, the Kataeb Party, and the Free Patriotic Movement fear the country's sectarian based political system is being undermined.

The massive influx of people fleeing the Syrian conflict - by April 2014, Syrian refugees were estimated to make up around a quarter of the population - has placed a severe strain on the country's resources. In March 2014, the Lebanese foreign minister warned that the refugee crisis was threatening his country's very existence.

Critical infrastructure

Hospitals and medical facilities are struggling to cope with a 25% increase in population. The threat from terrorism or large scale local protests which can quickly descend into violence is affecting travel, tourism. logistics and the ability to trade effectively.

The security services are over stretched and are working hard to protect major infrastructure including the airport, power stations the port areas and primary trading centres.

Refugees, particularly nearer the border with Syria, are taking jobs from local Lebanese families creating considerable unrest..

The border with Syria was recently closed in an effort to stem the influx, however without increased aid and even with additional aid further destabilisation of the country is in the short term inevitable.

Before the Syrian civil war erupted, there were signs that the revival of Lebanon's tourism industry might lead the way to economic recovery. In 2010, shortly before the conflict began, tourism accounted for a fifth of Lebanon's economic output. However, the fighting in Syria and the associated resurgence of sectarian tensions in Lebanon have severely jolted the country's tourism industry and dented hopes of a return to the cosmopolitan prosperity of the 1950s and 1960s.

The National Security and Resilience combines national security needs with an in-depth understanding of the design and implementation of resilience solutions for major events, cities, critical infrastructure and corporate entities. The NS&RC capability platforms provide expertise, proven credibility and bespoke solutions to resilience and security challenges.

Is Europe's Critical Infrastructure prepared for an attack?

Following the recent attacks in Paris, we have seen the changing nature of threat and terrorism in Europe. Are we surprised by these attacks? Well the security services are believed to have been aware of the potential of these groups of extremists, but the direction their plots have been focussed has caught many unprepared.

How long could it be before these types of attacks become focussed on essential parts of our infrastructure that would cause longer term paralysis of our economies?

The Arab spring continues to havOrganisations, such as IS, are also becoming more skilled at using the dark web and social media, not just to spread their message, but also attack our communities, businesses and government.

Nearly 70 Percent of Critical Infrastructure Providers Have Been Breached in the Past Year

Utility, oil and gas, energy and manufacturing organizations are unprepared for both internal and external threats, according to survey from Unisys and Ponemon Institute.

New research from Unisys Corporation finds alarming gaps in the security of the world's critical infrastructure. Nearly 70 percent of companies surveyed that are responsible for the world's power, water and other critical functions have reported at least one security breach that led to the loss of confidential information or disruption of operations in the past 12 months, according to a survey released recently in partnership with the Ponemon Institute.

In a survey of 599 security executives at utility, oil and gas, energy and manufacturing companies, 64 percent of respondents anticipated one or more serious attacks in the coming year. Despite this risk, only 28 percent ranked security as one of the top five strategic priorities for their organization, while a majority named their top business priority as minimizing downtime.

The survey also highlighted the concerns many of these executives feel regarding the security of industrial control systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems, which monitor and control the processes and operations for power generation

and other critical infrastructure functions. When asked about the likelihood of an attack on their organizations' ICS or SCADA systems, 78 percent of the senior security officials responded that a successful attack is at least somewhat likely within the next 24 months. Just 21 percent of respondents thought that the risk level to ICS and SCADA has substantially decreased because of regulations and industry-based security standards, which means that tighter controls and better adoption of standards are needed.

This research report comes at the same time that an international organised cybercrime network, composed mostly of Romanian citizens, was successfully taken down in Romania and France with the support of the European Cybercrime Centre (EC3) at Europol.

The cybercrime network is suspected of sophisticated electronic payment crimes including intrusions into international non-cash payment systems (through malware attacks), illegal worldwide financial transactions and money transfers, card data compromising (via skimming attacks), money laundering and drug trafficking. Members of this criminal network were using malware – RAT (Remote Access Tool) with key logger functionality - to take over and gain access to computers used by money transfer services all over Europe (Austria, Belgium, Germany, Norway, UK).

Critical Infrastructure Protection & Resilience Europe, incorporating Critical Information Infrastructure Protection (cybersecurity), will take place in The Hague on 4th-5th March 2015 and brings together leading stakeholders from industry, operators, agencies and governments to debate and collaborate on securing Europe's critical infrastructure.

Focussing on Convergence

Convergence is one of the key issues at this year's conference so the event will start with a combined plenary session 'Bridging the communications gap and enhancing the integration, cooperation and security between CIP and CIIP operations' before splitting into separate CIP and CIIP tracks.

This session examines how as more and more of vital CNI data is being held in cyberspace, opening it up to the threat of an attack that could delivery overwhelmingly disastrous consequences to CNI operations and the wider economy. The link of SCADA networks with IT networks allow better and faster communications, yet increase the threats and risks on SCADA communications. Discussed will be how communication and cooperation, good practice and guidelines can improve cyber security detection and response systems for CIP and CIIP?

Once the conference splits into tracks key discussions will revolve around transport, power and telecommunications which are crucial to the economic lifeblood of any modern industrial economy. The fragility of Europe's exposed transport network across a borderless continent provides unique challenges, including freight and passenger travel through our ports, harbours and airports. Communications infrastructure becomes key during any threat scenario in which many fail when severely damaged,

limiting coordinated efforts and potentially causing damage to the economy far in excess of any physical damage they may incur. The problem for the authorities, operators and agencies is to ensure the right balance of security, safety and resilience in facilities that are widely dispersed and subject to diverse ranges of threats.

Another modern phenomenon is the increasing use of smart phones as the preferred option to move or information/data and communicate among businesses and CNI sites. A session will discuss how secure are smart phone for your critical information and data exchange and what can be done to enhance security? With more sophisticated apps and more sophisticated cyber criminals, what's all the hype around electronic security?

Johan Willemen President of the FIEC will be amongst those who discuss how can we design and build in better security and resilience into critical infrastructure. How can standards be raised and what techniques can be employed to ensure structural analysis and monitoring of a building before, during or after an extreme event?

The final session will again combine CIP and CIIP delegates to discuss where and how agencies and CNI operators better work together for common purpose, resource sharing and intelligence gathering to deliver better value for the tax payer or shareholder and greater success in delivering security and resilience to our CNI, and improving disaster risk reduction.

The full conference programme, CIP and CIIP tracks and sessions can be found at www.cipre-expo.com, along with the speaker line up and event details, such as the IET Round Table being held on 3rd March.

IET Round Table

Open to all professionals working in the field of critical protection and resilience of national network systems and infrastructure, the IET Round Table will explore the inter-operability of systems for greater resilience across transport, the built environment and communications. Key conclusions from the round table will form part of the plenary session on Day 1 of the conference.

Ministerial Opening Keynote

The opening keynote presentations will be delivered

by Mr Ivo Opstelten, Minister of Security & Justice, Minister for Security & Justice, Netherlands and Mr. Fernando Sánchez, Director General, National Centre for Critical Infrastructure Protection (CNPIC), Spain.

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.

With the increasing threat from cyber attacks on critical infrastructure, the information and data stored and used by CNI systems and operators can be more crucial than the system itself. CIIP is becoming ever more important as part of the cyber security strategy of an organisation or CNI operator.

You can join the discussion at Critical Infrastructure Protection & Resilience Europe on 4th-5th March in The Hague, Netherlands. Further details can be found at www.cipre-expo.com.

FBI are "very concerned" about industrial espionage

A recent interview on San Antonio Channel 4 News with Christopher Combs of the San Antonio FBI s highlights that the FBI are "very concerned" about theft of trade secrets from US companies.

His interview was primarily talking about those US companies engaged in the multi-billion dollar "fracking" business in the Eagle Ford Shale in Texas but he also spoke about the threat to US organisations nationally.

"It's corporate espionage, there's no question about it," said Combs. "Foreign governments or foreign companies are looking for any competitive advantage. Whether it's the widget that you use to drill, or it's a process that you use to track inventory better. They're really looking at the company as a whole to find out every little thing that you do that makes you a better company on the world market."

Whist not mentioning specific incidents he outlined some of the scenarios being played out such as employees being targeted when they travel outside the country as well as so called "insiders" i.e. individuals being placed inside target companies with the specific purpose of engaging in espionage. Sometimes this process can take many years and would

indicate the involvement of national intelligence agencies. Another threat mentioned is the disgruntled employee who can 'go rogue,' and begin collecting and selling trade secrets to strike back at their employer. Then of course there is simple greed, the employee who sees the opportunity for a fast buck.

"It's not just the threats coming in from the outside, but what information is going from the inside out," Combs said.

He said Chinese companies are "aggressively" engaged in industrial espionage. However, the problem isn't limited to China. Companies with ties to governments that are U.S. allies are believed to be conducting espionage against innovative US firms as well.

But this is not just a US problem, it is global. According to the UK Centre for the Protection of National Infrastructure web site says: "The threat from espionage (spying) did not end with the collapse of Soviet communism in the early 1990s. The UK has been and remains a high-priority target for a number of countries looking to obtain information and technologies to help advance their own military, technological, political and economic interests."

According to Gerry Hall Managing Director Managing Director of International Procurement Services "The proliferation of GSM technology and devices means that insiders now have the technology available to them to listen-in on conversations in any part of any building that they have access to, even if only for a few minutes. Via GSM they can then listen to private conversations from anywhere in the world. This sort of technology is easily and cheaply available via the internet and can make a spy out of anyone."

He went on to say "Unless you have the right security policies, staff, procedures, training and equipment available to protect your business. There are a number of approaches available to safeguard your organisation from illicit eavesdropping. One approach is a "safe room". This is a selected room such as the board room, with the appropriate detection equipment permanently installed."

"Another route is to buy your own equipment and train your own staff in the use of the equipment. This gives you the flexibility to hold your meetings anywhere, from the board room to an office, meeting or hotel room, to a private residence. The last option is to employ an outside specialist sweep team to perform a thorough sweep of key meeting rooms, offices and phones as and when required."

"We have twenty-five years' experience supplying countermeasures equipment to government and corporate offices all over the world and have been performed operational sweeps over the same period. There is no substitute for the right equipment and the right expertise when it comes to protecting your intellectual property."

BORDERPOL Announces Establishment of a Common Council

Establishment of an external advisory group of border security and migration management officials was approved by BORDERPOL's Management Board at its annual general meeting in Budapest December 10, 2014. This decision was reached during the 3rd World BORDERPOL Congress which is the annual assembly of senior leaders from border safety, security, traveller and migration management organisations from around the world.

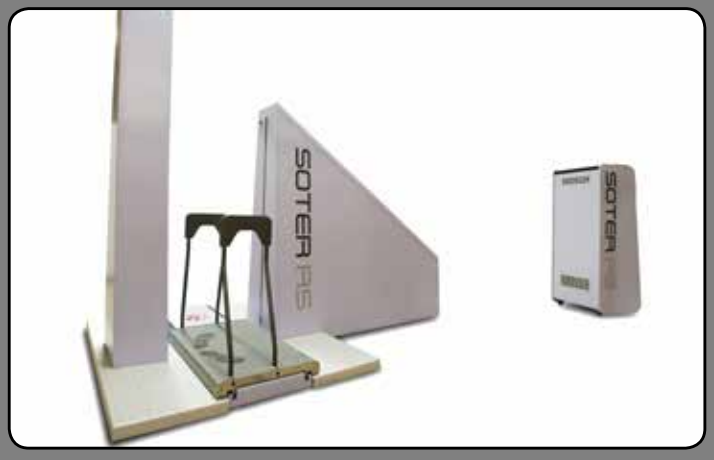
In May 2014 a strategic independent review was commissioned by the General Secretariat to examine the mission, membership and structure of the organization. Among the conclusions of the report delivered to the Management Board in October 2014 was a recommendation to establish an external advisory group of senior border service officials that would sustainably mentor and support the mission of BORDERPOL. Follow up consultations with key border service leaders led the General Secretariat to concur with the report's October recommendations. The General Secretariat therefor announces the establishment of a Common Council consisting of senior representatives from national border security, traveller and migration management services whose role will be to guide and mentor BORDERPOL as it expands its mission and programs over the next five years.

The Common Council will be composed of representatives appointed by the border services of invited member countries. The members of the Council will choose a President to represent the views of Council at BORDERPOL's annual general meetings. Common Council will counsel the General Secretariat on matters affecting the organizations general policy, resources needed to meet its goals, working methods, finances, and programmes.

SOTER RS Through-Body Scanners deployed in seven South African correctional facilities

An one of their largest orders ever, ODSecurity of the Netherlands has sold 14 SOTER RS Through-Body Scanners to the Department of Correctional Services in South Africa.

Two units each will be deployed in each of seven correctional facilities across the country.



The SOTER RS is a low dosage full body scanner which combines ultra low radiation with maximum visibility and is in use in airports for drug interdiction and correctional facilities worldwide. The SOTER RS takes just a few seconds to reveal hidden items both on the body, in body cavities and even ingested items such as weapons, mobile phones, drugs and other contraband. It will clearly show a difference between human tissue and any other materials, not just metal but organic materials and man-made materials.

The scanners will be offered for both inmates and visitors, which avoids the use of intrusive strip searches.

Smuggling into prisons is a worldwide problem which is on the increase. A recent report in Canada determined that between 2007 and 2011, the amounts of drugs, intoxicants, weapons and other unauthorized items confiscated by staff at Canadian prisons has steadily risen, in some cases by more than 170 per cent.

SOTER RS is successfully deployed in prisons, in airports, detention centres, police and customs facilities worldwide including; Australia, Denmark, Ghana, Hong Kong, Kuwait, Malaysia, Mexico, Nigeria, Netherlands, UAE, USA, UK, Chile, Sri Lanka and Vietnam and now South Africa.

Swedish CBRN Academy, Swedish Rescue Training Centre and Lutra Associates Ltd Team Win First Contract

Consortium demonstrates capabilities and benefits of SMEs by delivering training package at short notice to security teams from NATO nation

Skövde Sweden, Stalbridge, Dorset, UK; 8th January 2015. The recently announced CBRN training and consultancy team formed by Swedish CBRN Academy (SCA), Swedish Rescue Training Centre (SRTC) and Lutra Associates Limited (LAL) has won its first contract.

Working together the team was selected to provide CBRN close protection and decontamination training to the national security forces of an unnamed NATO country through a prime contractor who was delivering a wider package of equipment and services.

For obvious reasons the country does not wish to be named but the training involved national police and defence resources.

This initial training was run in- country and consisted of practical work to ensure that the selected protection officers involved are capable of reducing the risk to their VIPs prior to an attack. This is achieved by carrying out threat assessments and risk reduction drills, and then dealing with an attack should one occur with rapid protective and remedial actions. The aim of the training was to give a basic introduction to the concepts, skills and responses required to allow a further assessment to be made as to what follow up training will also take place.

Dan Kaszeta of Strongpoint leads a class discussion during the CBRN close protection and decontamination training to the national security forces of an unnamed NATO country provided by the joint team of Lutra, Swedish CBRN Academy (SCA), and the Swedish Rescue Training Centre (SRTC).

Speaking from Skövde Johan Carlqvist Chief Executive of SCA said, "By delivering this contract at short notice, we demonstrated the speed and rapid reaction that groups of small companies can provide when dealing with a request for urgent action. The training delivered by Strongpoint was thorough, effective and very much appreciated by the students who recognised the obvious expertise of the training team."

The training was facilitated by SCA and SRTC and carried out by Lutra through Strongpoint Security. Commenting on the contract from Stalbridge Tim Otter, Chief Executive of Lutra said "I am delighted for the team that we have won this first contract as it demonstrated the wide depth of experience and skills that reside within the team. This country, like many others has suddenly realised, that they had not addressed the CBRN threat with sufficient money or vigour over the past few years. They have now started to take positive steps to rectify the problem. We are delighted to provide low cost, high quality advice across the CBRN spectrum to enable them to do so."

Commenting on the training course Dan Kaszeta the Managing Director of Strongpoint commented, "The students were excellent, keen and motivated, extremely interested and professional. This allowed us to build on the excellent facilitation SCA and SRTC managed so that the course went smoothly and the students gained the absolute maximum from the training time available.".

Bruker DE-tector™ Explosives Trace Detector Meets New European Civil Aviation Conference (ECAC) Standard for Airport Passenger and Baggage Screening

SGThe Bruker Detection division announced late last year that the DE-tector™ has successfully met the new European Civil Aviation Conference's (ECAC) Common Evaluation Process of Security Equipment (CEP) for airport checkpoint screening of passengers and baggage. The DE-tector is the first European-built explosives trace detection (ETD) instrument to pass the demanding ECAC testing protocol which was established to set standards for the performance of security equipment across the forty four member nations of ECAC.

Dr. Norbert Kloepper, Head of the Bruker ETD business, commented: "The 44 ECAC nations represent a significant business opportunity for Bruker Detection. Many of our potential clients from EU countries have delayed their ETD acquisitions until the new ECAC CEP standard had been established and applied to systems submitted for testing. As a key ETD supplier, we believe we are well positioned to satisfy customer requirements for certified equipment with strong local training and service support."

The DE-tector system is a bench-top explosives trace detector using Ion Mobility Spectrometry. Using the patented, non-radioactive HEPITM-source, the DE-tector lowers the administrative and compliance burden on our customer significantly. The system provides exceptional trace detection capabilities whilst maintaining an exceptionally low false alarm rate. An intuitive 'traffic light' user interface and minimized user interaction resulting from the incorporation of automatic calibration, along with a 12-month maintenance cycle, reduces the total cost of training, maintenance and operation.

New HT2-Matador Surface Mount Sliding Bollard facilities

Heald have introduced the new HT2-Matador offers surface mounted automated security bollard.

It has recently been tested with a 7.2 tonne vehicle travelling at 64 kph, with the impact resulting in zero penetration past the bollards and what's more, remained fully operational following the test. This means uninterrupted site protection and no expensive repairs.

The new Matador can be specified to work in a variety of ways; using either electro-hydraulic, electro-mechanical or even manual operation. It can also be supplied with an EFO (Emergency Fast Operation) feature, which enables the moving bollard to close in around 1.5 seconds in emergency situations. It also features a special mechanism to secure the central bollard in the locked position, ensuring that it cannot be moved or pushed open.

As with previous models, the new Matador can either be surface mounted or it can be installed flush with the road with a depth of only 115 mm. This makes it ideal for short term or temporary installations as well as permanent ones. To ensure integration with any architecture, the Matador is available with a range of stainless steel covers.

Like other Heald automated products the HT2-Matador is available with Hydra control and monitoring system. This allows for far more detailed and user friendly interaction with the unit.

Zaun secures critical infrastructure in the Oman

AA British high security fencing systems manufacturer has completed the first of two pilot projects, worth almost £1.5 million, with Oman's premier oil company.

Zaun Limited is supplying the perimeter security for two prestigious booster stations in Oman for Petroleum Development Oman (PDO), the foremost exploration and production company in the Sultanate. It accounts for more than 70% of the country's crude oil production and nearly all of its natural gas supply.

Zaun has completed work at the Nahada site in the north of Oman, about 400km from Muscat towards the Saudi border,

having overcome on-site challenges, such as the formation of wadis when rivers spring up in flash floods in the desert and violent sand storms that can shred the coatings on the fence panels.

Zaun has supplied almost 9km of HiSec 358 premier British-made fencing and a large number of PAS 68 crash rated entry and exit gates.

The fencing and gates are integrated with razor wire, PIDs and CCTV to form inner and outer cordons around the oil booster stations. Now Nahada is complete, they have now begun to mobilise for its sister Hubara station in the south.

The purpose of the oil booster stations is to pressurise the crude oil in pipes buried under the Omani desert as it is fed from the fields into the main oil line for export.

Jeremy Knight, head of Middle East operations for Zaun, said: 'The pilot has given us real credibility across the Middle East and constitutes a sizable contract for our business in the region. As they are well known for setting the benchmark for their industry, we hope to build on the back of that.'

In the United Arab Emirates, Zaun has won work to supply an Abu Dhabi military base and has also bid to upgrade perimeter security solutions for the American school in Dubai.

Avoid Costly Losses by Increasing Visibility in the Supply and Distribution Chain

Tony Pelli, Senior Intelligence Analyst with BSI, Supply Chain Solutions writes globalization has proven to be a boon for most companies, as it has allowed firms to sell their goods or services across the globe. However, this has also increased the complexity of supply and distribution chains, which often span dozens of far-flung countries, making it more difficult to monitor security conditions. Companies are unable to guarantee that transportation providers, warehouse facilities, or

third-party factories abide by the same security standards as they do. This lack of visibility can lead to costly losses due to cargo theft or decertification from government security programs such as the E.U. Authorized Economic Operator Programme or the U.S.C-TPAT programme. Major incidents can also be a black mark against a company's image, tarnishing their hard-earned reputation.

Companies can overcome these difficulties by assessing security risks to their business partners and company sites. Objectively evaluating country risk factors comes first; for example, the risk of cargo truck hijacking is much higher in Italy than in Germany. Continuous reporting of incidents can build a "live" view of risk as it shifts. Companies should then conduct assessments of the sites themselves, beginning with initial self-assessments before moving to site visits for high-risk business partners. Assessment results can be displayed to view risk across the supply and distribution chain so security managers can identify areas for improvement. Regularizing this process will allow companies to see quickly see gains to their bottom line through increased security both upstream and downstream.

Kratos Receives $26 Million in Critical Infrastructure Security Awards

Kratos Defense & Security Solutions has announced that its Public Safety & Security Solutions (KPSS) Division has recently received approximately $26 million in new critical infrastructure security awards, including the deployment of a specialized comprehensive security system for a major mass transit authority in the United States.

Under these recent contracts awards, Kratos will design, engineer, deploy and integrate into command and control infrastructure specialized security systems and assets, including video surveillance, access control, physical asset protection and other security elements. KPSS is a leading public safety, security and critical infrastructure protection system integrator in the United States. Due to customer specific and other considerations, no additional information will be provided.

Ben Goodwin, President of KPSS, said, "Our entire organization is proud to have received these recent contract awards for the protection of our country's most important critical infrastructure and mass transportation networks."

Illicit Tobacco has no hiding place when Wagtail Dogs are on the job

Although the smuggling of tobacco and its products has been happening the world over since its initial appearance in 1492, now more than ever Governments are keen to stamp out this illegal trade which is depriving the EU of over 10 billion Euros of lost revenue every year in unpaid taxes and duties, encourages a high youth uptake, and increasing health risks for consumers.

With a high profit rate, and high demand, illicit tobacco is often seen by organised criminal groups operating across borders as an easy way to make large sums of untraceable cash without the high sentences associated with drug trafficking. It is estimated that the illegal tobacco market is now one of Europe's fastest growing type of organised crime, and has been responsible for funding larger operations such as drug smuggling or people trafficking.

Across the UK there is a war being waged against counterfeit and illicit tobacco.

Working in conjunction with various Council Trading Standards Departments HMRC Officers and Police across the country, Wagtail UK Limited's Tobacco Detection Dog Team have been thwarting the criminals by detecting vast quantities of illegal and illicit tobacco products.

Previously searching shops, lock-ups, storage facilities were carried out manually by HMRC officers, now with the use of Sniffer Dogs, and their amazing scenting abilities, tobacco can be found in places that you and I would find it very difficult to locate. Past finds have been inside, vacuum cleaners, in false cupboards, in toilet cisterns, hidden inside food packets, even in hydraulically operated lifts hidden under the floor!

In a recent operation in Chester, with what would appear upon first glance as a normal empty shelving unit, upon further inspection, following a insistent indication by one of Wagtail's Tobacco Detection Dogs, revealed a hiding hole concealing a large haul of illegal tobacco products.

In this particular search Wagtail UK worked alongside officers from Cheshire West and Chester Regulatory Services and the North West Illicit Tobacco Team.

Councillor Lynn Riley, executive member for localities, said: "Tobacco detection dogs have become valued members of the team – but they are not so popular with those who sell contraband or counterfeit tobacco."

"Those involved in dealing in illegal tobacco may be encouraging people, including children to smoke by providing a cheap source.

"Dogs like Ozzie and Alfie can find tobacco and cigarettes even if they are hidden in the most unlikely places. In one of the premises, the stash of illicit tobacco was concealed behind an innocent-looking shelving unit on a wall. Luckily, super sniffer dog Alfie was on the case and pointed officers directly to it.

Collin Singer, MD of Wagtail UK said, "We work with Trading Standards Teams up and down the Country, and it is amazingly satisfying knowing that it is our dogs that are helping take these dangerous products off the streets."

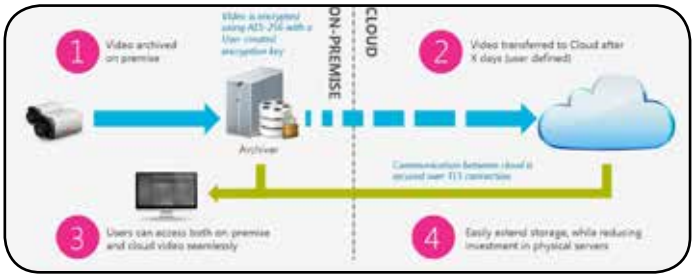
Select 2015 Security Industry Predictions from Genetec

Unification

We see a continuing trend towards unification of security systems, as well as unification between security, communications and other business systems. A good example is end users looking at comprehensive security strategies that take into account VoIP-based communications such as SIP-enabled intercom servers and devices. Another is the extension of security beyond an organization's buildings and facilities into parking and other areas.

Cloud

As the latent appetite for the Cloud grows and the affordability of cloud-based resources becomes apparent, we expect larger organisations to begin



adopting a Hybrid-Cloud model to take advance of these savings. As such, we see a growing demand for hybrid services that allow end users to extend their on premise security systems (eg. video surveillance) with cloud-based services geared to security system users, such as cloud-based storage for longer-term retention or redundant archiving. To support this move Genetec has recently announced its Cloud Archiving Service with Microsoft Azure.

Open vs Proprietary 'Closed' Security Systems

2014 saw a continued divergence between open platform IP security manufacturers and proprietary 'end-to-end' vendors, so IT and security managers will continue to review the pros and cons of these two industry models. It isn't possible for a single company to anticipate all the future technological developments that will be needed. We predict adopters of closed systems will regret making short-term gains at the expense of long-term pain.

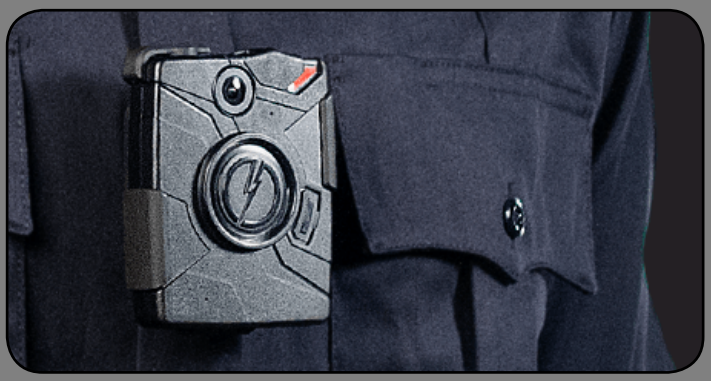
Wearable Tech for Security

With US presidential backing and trials already underway in the US and UK, we expect this to gain momentum in 2015. Equipping security and law enforcement professionals with body-worn cameras provides an opportunity to capture and record events where fixed security cameras are not in place. It can also help to restore trust in a community that law officials have acted appropriately in emotive situations.

15 New US Police Agencies Deploy More Than 1,200 TASER AXON body-worn camera systems

TASER International announced multiple large orders of its AXON body-worn video cameras and EVIDENCE.com solution, a back-end digital evidence management system.

A year-long Cambridge University study conducted at the Rialto, CA Police Department investigated whether officers' use of video cameras could bring measurable benefits to relations between police and civilians. The results showed an 88% reduction in citizen complaints and a 60% reduction in uses of force after implementation of TASER's AXON flex cameras. In a study by Arizona State



University, the Mesa Police Department's use of AXON cameras revealed a 48% reduction in citizen complaints against camera officers for misconduct during the study period, and a 75% decline in use of force complaints.

TASER's AXON cameras are small, yet highly visible, and can be attached securely to sunglasses, a cap, a shirt collar, or a head mount. They are powered by a pocketsize battery pack, which ensures recording capability during an entire shift. When recording, the cameras capture a wide-angle, full-color view of what an officer is facing. The video automatically uploads via a docking station to EVIDENCE.com, a cloud-based storage and management system, where it can be easily accessed for review.

EVIDENCE.com helps police capture, manage, and share their digital evidence without the complexity or cost of installing in-house servers. It enables greater transparency through seamless integration with the industry-leading AXON body-worn video cameras. EVIDENCE.com is the most secure, scalable, and cost-effective solution for managing all types of digital evidence. EVIDENCE.com automates the upload process to ensure security and integrity while keeping officers in the field rather than sitting at computers.

Fortinet launches rugged devices to connect, secure critical infrastructure

Fortinet has announced four new "Rugged" products –networking, security and wireless devices purpose-built to meet the demanding standards of public utilities, oil and gas, mining, manufacturing and the transportation industries that operate in harsh physical environments. The release of the FortiGate Rugged 60D, FortiGate Rugged 90D, FortiAP 222C and FortiSwitch 112D-PoE, marks another important step in the company's already strong and growing critical infrastructure presence, which has expanded to include securing seven of the top 10 global petroleum refiners and six of the top 10 global utilities.

"The dangers to our critical infrastructure from foreign and domestic cyber-attacks have increased dramatically in recent years. No sector is without exposure. Electric power generation and distribution, transportation, water, oil and gas just to name a few," said Steve Keefe, president of Patriot Technologies. "Fortinet's 'Rugged' line makes it possible to apply enhanced levels of security in some of the most demanding environments, enabling better visibility, manageability and control to our countries critical assets and security."

The Critical Infrastructure Challenge

Critical infrastructure and other businesses that rely on industrial control systems face unique and growing security issues. Threats have evolved into highly sophisticated and targeted assaults leveraging multiple attack vectors to penetrate networks and steal valuable information. These include disruption of critical services, environmental damage and prospective widespread harm.

In addition, distributed critical infrastructure is often located in places that are physically inaccessible, lack connectivity, subject to intemperate climate or otherwise constrained by limited space. As a result, traditional security solutions intended for indoor environments are often ill-equipped to operate under duress or in harsh conditions.

"Fortinet allows customers to protect themselves from attack at the very point where they are most vulnerable. If cyber criminals want to break into an environment, they're generally not going to break into a datacenter, they're breaking into a remote location a thousand miles away. Pushing those controls out allows you to create a defense perimeter at the far regions of the network – but those far regions are often subject to extreme conditions," said Andrew Plato, CEO of Anitian, a security intelligence and risk management firm. "It's not feasible to be putting SOHO type equipment in these locations, you need a purpose-built device. A failure of that equipment isn't just an annoyance -- it's critical downtime and a plane ride. A very long plane ride for some of them."

And finally critical infrastructure, which leverages Operational Technology applications, hardware and networks, relies on different communication protocols, older operating systems and more industry-specific applications than Information Technology systems. All of these factors -- sophisticated threats, harsh conditions and proprietary systems -- make it more difficult to increase security for industrial control systems.

"Vital systems such as utilities and manufacturing face harsh conditions and a proliferation of new attacks that pose numerous threats to public well-being and safety," said John Maddison, vice president of marketing products for Fortinet. "Addressing these unique problems, Fortinet's new Rugged products enable customers to reduce the risk of catastrophic security incidents to critical infrastructure that could put public health and safety in jeopardy."

Partnership With Leading Manufacturer's Rep Enhances Data Center Safety for New York, New Jersey, and Connecticut

Anord Critical Power, Inc., a leading independent provider of critical-power infrastructure to the global data center industry, today announced the company is expanding its presence throughout the Northeast via a newly established partnership with Wavetech Associates, Inc. The new partnership will enable Anord to distribute its award-winning Form 4b Type 7 design AMS switchgear to power mission-critical facilities across New York, New Jersey and Connecticut.

Wavetech Associates is the tri-state area's leading manufacturer's representative, focusing on mission-critical infrastructure support systems with data center power quality products for both industrial and commercial applications. Offering solutions across the total power spectrum, the company's technicians are focused on providing customers with maximum data center uptime.

"Our region is consistently ranked one of the most robust data center markets in the U.S., as such industries as financial services rely on a strong power infrastructure to keep systems running." said Jose Alvarez, President of Wavetech Associates, Inc.

World Security Report

World Security Report is a quarterly electronic, fully accessible e-news service distributed to over 40,000 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 Matters

Border Security Matters is the quarterly newsletter of BORDERPOL, the World Border Organisation, delivering agency and industry news and developments, as well as more in-depth features and analysis to over 10,000 border agencies, agencies at the borders and industry professionals, policymakers and practitioners, worldwide.

World Security Report

Advertising Booking Form

Complete this form and fax to +44 (0) 872 111 3210 or email to sales@torchmarketing.co.uk

☐ I/we hereby apply for advertising space in World Security Report.

Please indicate issue:

- ☐ January 2015 (booking and copy deadline - 10th January 2015)
- ☐ April 2015 (booking and copy deadline - 10th April 2015)
- ☐ July 2015 (booking and copy deadline - 10th July 2015)
- ☐ October 2015 (booking and copy deadline - 10th October 2015)

Contact name: _____

Company name: _____

Address: _____

Street: _____

Town/City: _____ County/State: _____

Post/Zip Code: _____ Country: _____

Tel: _____ Fax: _____

E-mail: _____

Signature: _____ Date: _____

Advertising requirements
(Please check appropriate boxes)

Full page	- £500 per issue	☐
Half page	- landscape - £350 per issue	☐
	- portrait - £350 per issue	☐
Quarter page	- landscape - £225 per issue	☐
	- portrait - £225 per issue	☐
Product Focus	- quarter £225 per issue	☐
	- eighth £150 per issue	☐

Buyers Guide / Company Listings

- Basic Listing - £100 per issue ☐
- Enhanced Company Listing - £195 per issue ☐

Contact

If you have any queries please contact:

Paul Gloc - UK & Europe
paulg@torchmarketing.co.uk

Denne Johnson - The Americas
dennej@torchmarketing.co.uk

PAYMENT DETAILS
(METHOD OF PAYMENT - Advertising fees are subject to VAT at 20%.)

☐ Wire Transfer (Wire information will be provided on invoice)

☐ Credit Card
Invoice will be supplied for your records on receipt of the order/payment.

Please fill in your credit card details below:
☐ Visa ☐ MasterCard

All credit card payments will be subject to standard credit card charges.

Card No: _____

Valid From ____ / ____ Expiry Date ____ / ____

CVV Number _____ (3 digit security on reverse of card)

Cardholder's Name: _____

Signature: _____ Date: _____

For use by Torch Marketing only:

Date received: Amount Due: £

Amount Received: £ Agent:

January 2015

18-20
Intersec Middle East, Dubai
www.intersecexpo.com

February 2015

5
Public Security Exhibition, Bucharest, Romania
www.adsgroup.org.uk/articles/44239

22-26
IDEX, Abu Dhabi, UAE
www.idexuae.ae

March 2015

4-5
Critical Infrastructure Protection & Resilience Europe, The Hague, Netherlands
www.cipre-expo.com

10-12
HomeSec, Madrid, Spain
www.homsec.es

10-12
Security & Policing, Farnborough, UK
www.securityandpolicing.co.uk

23-25
ConnectID, Washington, USA
www.connectidexpo.com

April 2015

14-16
INTERPOL World, Singapore
www.interpol-world.com

14-16
IPOMEX, Munster, Germany
www.ipomex.de/en

14-17
LAAD Defence & Security, Rio de Janeiro, Brazil
www.laadexpo.com.br/2015

21-22
Counter Terror Expo, London, UK
www.counterterrorexpo.com

22-24
Security Printers, Copenhagen, Denmark
www.securityprinters.org

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

28-30
Secutech Taiwan, Taipei, Taiwan
www.secutech.com/15/en

May 2015

5-8
IDEF, Istanbul, Turkey
www.idef15.com/en

19-21
IMDEX Asia, Singapore
www.imdexasia.com

19-21
IDET, Brno, Czech Republic
www.bvv.cz/en/idet

June 2015

24-25
Critical Infrastructure Protection & Resilience Asia, Bangkok, Thailand
www.cip-asia.com

December 2015

8-10
4th World BORDERPOL Congress, The Hague, Netherlands
www.world-borderpol-congress.com

4th World BORDERPOL Congress

8th-10th December 2015

The Hague, Netherlands

Enhancing collaboration in global border protection and management challenges.

Save The Dates

The World BORDERPOL Congress is the only multi-jurisdictional transnational platform where the border protection, management and security industry policy-makers and practitioners convene annually to discuss the international challenges faced in protecting not only one's own country's borders, but those of neighbours and friends.

Join us for developing co-operation and collaboration through high level discussions and presentations on the future for border protection and management.

We look forward to welcoming you to The Hague, Netherlands on 8th-10th December 2015 for the next gathering of border and migration management professionals.

www.world-borderpol-congress.com

Owned & Organised by:

Supported by:

Media Partners: