



# COUNTER TERROR EXPO

25 - 26 April 2012

Olympia London

[www.counterterrorexpocom](http://www.counterterrorexpocom)

Register by  
24 February  
and save  
£100.00



## CONFERENCE PROGRAMME

- Global Counter Terrorism
- Protecting Crowded Places
- Critical National Infrastructure – Protection, Security & Resilience
- Cyber Security and Electronic Terrorism
- The Cost of Terrorism to Business – Best Practice Risk Assessment



**PRE-REGISTRATION ONLY – ON-SITE REGISTRATION NOT PERMITTED**

Conference Partner



Conference Sponsors



International Protect and Prepare Security Office

Networking Reception Sponsor



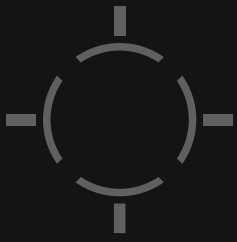
Supported by



Co-located



Register today at [www.counterterrorexpocom/confbrc](http://www.counterterrorexpocom/confbrc)



## Counter Terror Expo's operationally critical and highly respected centrepiece conference has a well deserved reputation for its delivery of insight, analysis, and perspective on the range of threats faced.

This conference gathers together over 100 internationally recognised experts in the field of counter terrorism annually to debate the issues we face, define operational strategies, and to help shape future policy within the secure conclave of a conference.

Counter Terror Expo's centrepiece conference is a multi-stream event bringing clarity to the most critical and topical issues of concern to the international counter terrorism community.

The conference features a mix of one and two day programmes and will cover five main areas, details of the themes and an explanation of each programme is shown overleaf, the detailed programmes and speaker details can be found throughout the brochure.

### GLOBAL COUNTER TERRORISM Two Day Conference 25<sup>th</sup> – 26<sup>th</sup> April

In the twelve months since this Global Counter Terrorism conference last convened here in London, dramatic events have occurred which have reshaped the threat horizon.

Al Qa'ida leader Osama bin Laden is dead; its remaining leadership is being successfully targeted and the much-weakened terrorist organisation has further fragmented. Meanwhile, hard-line leaderships across large swathes of the Arab-speaking world have been toppled in popular uprisings, bringing about a shift to democratic principles in governance and freedom of expression.

These dramatic events force us to reassess and realign counter terrorism strategies in line with the shifting threat horizon, but against a backdrop of considerable fiscal upheaval that threatens our ability to maintain secure borders, civil order and safe societies.

This two-day conference brings clarity and focus to the important task at hand.

### CRITICAL NATIONAL INFRASTRUCTURE PROTECTION, SECURITY & RESILIENCE Two Day Conference 25<sup>th</sup> – 26<sup>th</sup> April



The loss or compromise of any of the critical elements of the national infrastructure could have a major and detrimental impact on the national wellbeing and possibly lead to severe economic and social impact.

This is the potentially stark consequence of failure to properly protect the physical assets, services and supplies a modern society requires to function.

This highly important two-day conference examines the threat to the key areas of energy, water, food, finance, communications, transport, health, emergency services and governance, delivering insight into best practice answers to the threats each faces.

Securing and protecting the national infrastructure is a vital prerequisite in maintaining resilient services in the event of a major terrorist attack or environmental event.

## PROTECTING CROWDED PLACES Two Day Conference 25<sup>th</sup> – 26<sup>th</sup> April

Crowded places remain amongst the most vulnerable to possible terrorist attack and continue to be the most difficult of spaces to secure.

Thousands of people pass through our transport hubs, visit major shopping centres, go to the theatre or catch a movie every day and all are at risk from some form of attack.

This conference examines the increasingly utilisation of a combination of innovative building design, blast mitigation techniques and effective surveillance and policing methodologies to effectively secure our most crowded places and protect the people who use them.

With the more traditional of terrorist targets having been significantly hardened against attack, the imperative is to devise solutions that work for the remaining soft targets in these fiscally challenging times.

## CYBER SECURITY & ELECTRONIC TERRORISM One day Conference – 26<sup>th</sup> April

Increasing global interconnectivity brings huge benefits to the way we live and work, but conversely delivers with it many challenges that we must still overcome.

In the few relatively short years since the internet became a reality, this digital phenomenon has become a playground for state actors, terrorists, criminals and hacktivists, bent on infiltrating computer networks and individual computer systems to steal information and disrupt operations.

The cyber security and electronic terrorism conference examines the magnitude of the threat and outlines how government agencies and corporate entities are putting in place effective counter-measures to appropriately protect restricted information, intellectual property and customer data.

The digital world is the new frontier in our constant battle against those who wish to inflict harm for ideological, commercial or monetary gain and requires robust defences.

## THE COST OF TERRORISM TO BUSINESS BEST PRACTICE RISK MANAGEMENT One Day Conference – 25<sup>th</sup> April



The threat from terrorism continues to evolve, with the number of incidents and plots growing each year. With no peace dividend yet in sight the risk to business remains acute.

An attack directed at business could result in major property damage, operational disruption, human casualties and long-term damage to both brand and reputation. In today's increasingly litigious society, businesses must ensure corporate governance and duty of care responsibilities are a central tenant of their crisis management strategy.

AON's one-day conference will look at developments in the global terrorism landscape, and the human and economic impact on business. The conference will examine the full range of risk management options and what companies need to consider around their duty of care obligations.

### Key speaking organisations include:

- Cabinet Office • E.ON • BT • Highways Agency
- Police Service of Northern Ireland (PSNI)
- Centre for the Protection of National Infrastructure (CPNI)
- International Cyber Security Protection Alliance
- Association of Chief Police Officers (ACPO)
- Cisco • Symantec • Metropolitan Police Service
- Kings College London • British Transport Police
- Department of Health • Home Office
- Office for Security and Counter Terrorism
- National Counter Terrorism Security Office (NaCTSO)
- European Policy Centre • NATO • United Nations

**Each conference pass can be purchased on the basis of a 1 or 2 day pass for a particular stream, for those requiring access to multiple streams it is possible to buy multiple passes. Register today at [www.counterterrorexp.com/confbrc](http://www.counterterrorexp.com/confbrc)**

# Global Counter Terrorism

## DAY ONE: WEDNESDAY 25 APRIL

**08.00 – 08.45** Coffee/Registration

**08.45 – 09.00** **Chairman's Opening Remarks**  
**Niki Tompkinson, Security Consultant and former Director**  
**TRANSEC, DfT**

### ADDRESSING NEW AND EVOLVING SECURITY THREATS

**09.00 – 09.30** **Securing the State – National Security for a Modern World**

- Assessing the current national security and counter-terrorism strategies – big picture messages
- Medium and long term implications for the UK from the Strategic Defence and Security Review (SDSR)
- New approaches for new threats – the changing nature of threats and the risks to the UK

**Professor Paul Cornish, Professor of International Security, University of Bath**

**09.30 – 10.00** **The New Counter-terrorism Strategy**

- Key updates to CONTEST and the implications for counter terrorism strategy, planning and operations
- Assessing the impact across Government and likely areas for development
- Importance of maintaining and developing dialogue and co-operation with overseas counterparts to achieve effective counter terrorism for the UK

**Charles Farr, Director General, Office for Security and Counter Terrorism, Home Office**

**10.00 – 10.30** **Strategic Choices for Europe's Security**

- The role of transatlantic cooperation in achieving security in Europe – aligning military and political dimensions
- Influence of US domestic politics on European security and structures
- Assessing the implications for security and counter terrorism from the Euro crisis

**Josef Janning, Director of Studies, European Policy Centre**

**10.30 – 11.00** Coffee/Tea/Exhibition Visit

### COUNTERING GLOBAL TERRORISM

**11.00 – 11.30** **Tackling Emerging Threats**

- The role of the trans-Atlantic relationship in tackling emerging threats
- A strategic analysis of the key threats – terrorism, cyber, energy security and weapons of mass destruction
- Strategies for non-traditional threats

**Jamie Shea, Deputy ASG, Emerging Security Challenges Division, NATO**

**11.30 – 12.00** **Preventing and Combating Terrorism**

- Actions for national governments in tackling the conditions conducive to the spread of terrorism;
- The importance of building States' capacity to prevent and combat terrorism
- Ensuring respect for human rights for all and the rule of law as the fundamental basis for the fight against terrorism

**Kasper Ege, Counter Terrorism Implementation Task Force (CTITF) and CTITF Office, United Nations**

**12.00 – 12.30** **Supporting the Global Campaign against Terror**

- Planning and taking action against global terrorist networks
- Implications of key threats emanating from the Middle East
- Collaboration with international partners – the role of non state actors, multilateral organisations and foreign jurisdictions
- Implications of the evolving nature of Al Qa'ida

**Dr. Michael Rubin, The American Enterprise Institute**

**12.30 – 14.00** Lunch/Exhibition Visit

### NEW SECURITY CHALLENGES

**14.00 – 14.30** **The Fight against Terrorism – The EU Counter Terrorism Strategy**

- Assessing the importance of collective EU level action against terrorism – PREVENT and PROTECT
- Enhancing information sharing and practical cooperation between member states
- Interlinking European counter terrorism capabilities and tools
- New challenges for Europe from the Arab Spring

**Senior Representative, Council of the European Union**

**14.30 – 15.00** **New Security Challenges**

- Assessing the extent of the linkage between terrorism, political violence and warfare
- Comparing developments in Iraq and the enduring terrorism threat in Northern Ireland
- Emerging trends in international terrorism and what this means for national security

**Dr. Dave Sloggett, Author and Independent Academic**

**15.00 – 15.30** **Islamism and Political Violence – The Effects on Europe's Security**

- Influence of political violence on European security and structures
- Implications for security of current trends in jihadism in Europe

**Lorenzo Vidino, Fellow – Center for Security Studies, Zurich**

**15.30 – 16.00** Coffee/Tea/Exhibition Visit

### CYBER SECURITY – TACKLING THE DIGITAL ARMS RACE

**16.00 – 16.30** **Dealing with Cyber Security – The Role of the UK Defence Cyber Operations Group**

- Defending the UK's digital infrastructure from cyber attacks
- The role of cyber weapons as an integral part of the country's armoury to tackle conflicts without borders
- The UK Defence Cyber Operations Group – detecting cyber attacks against UK defence systems

**UK Defence Cyber Operations Group, MoD**

**16.30 – 17.00** **Building a Safe, Secure and Resilient Cyberspace**

- Implications for cyber from the CONTEST counter-terrorism strategy
- Ensuring the resilience and security of government ICT infrastructures
- Engaging with international partners in improving the security of cyberspace and information security

**Mike St John Green, Deputy Director, Office of Cyber Security and Information Assurance (OCSIA), Cabinet Office**

**17.00 – 17.30** **Security and the Cyber Threat**

- Assessing the unprecedented growth in cyber criminality and the associated threats and challenges
- Who is the main enemy? State-sponsored actors, organised criminal groups, hactivist networks or terrorist groups?
- The role of international partnerships and alliances in building sufficient capacity and capability to handle increasing volumes of cyber crime
- Countering cyber criminality by promoting expertise, information-sharing, best practice and technical assistance to domestic and international law enforcement cyber crime units

**John Lyons, Chief Executive, International Cyber Security Protection Alliance**

**1730** **Close of Day One and Evening Drinks Reception**

Networking Reception Sponsor

Industry Sponsor



\* subject to final confirmation

# Global Counter Terrorism

## DAY TWO: THURSDAY 26 APRIL

**08.00 – 08.45 Coffee/Registration**

**08.45 – 09.00 Chairman's Opening Remarks**  
**Dr. Dave Sloggett, Author and Independent Academic**

### THE EVOLVING TERROR LANDSCAPE

**09.00 – 09.30 Counter Terrorism Beyond 2012**

- Implications of budgetary prioritisation on the current focus of security efforts
- Impact on counter-radicalisation of Islamic violent extremism and the political and ideological messages of Al Qa'ida
- Assessing the success of military operations
- The need to exploit technology as a key part of a broad counter-terrorism strategy
- Addressing organised crime and cyber security

**Benoît Gomis, International Security Programme, Chatham House**

**09.30 – 10.00 Applying the UK's Counter Terrorism Legislation**

- A prosecutor's viewpoint on the challenges involved in terrorism prosecutions
- Working together with the police and the intelligence services to build a coherent picture of the plot
- Maintaining respect for human rights while protecting national security
- Importance of sharing information and providing transparency and accountability

**Sue Hemming, Head of the Special Crime and Counter Terrorism Division, Crown Prosecution Service (CPS)**

**10.00 – 10.30 The 2011 Arab Spring – Opportunity or Threat for Terrorism**

- Assessing the Arab revolutions and the implications for international terrorism
- Likelihood of Al Qa'ida and global jihadists exploiting the outcomes
- Implications of extended revolution in Yemen and Syria
- Identifying the potential for and risks from a rise in religious extremism

**Anna Boyd, Senior Global Risk Forecaster, Exclusive Analysis**

**10.30 – 11.00 Coffee/Tea/Exhibition Visit**

### TACTICAL COUNTER TERRORISM

**11.00 – 11.25 Tactical Operations for Terrorism Response**

- Basic concepts and tactics
- Proven tactics, techniques and procedures for SWAT operations
- Tactical considerations when dealing with a terrorist threat such as improvised explosive devices, and weapons of mass destruction

**Chadd Harbaugh, President, Government Training Institute**

**11.25 – 11.50 Countering Terrorism and Managing Operational Risk through Intelligence**

- The role of intelligence in counter terrorism and risk assessment and management
- Obtaining and using intelligence to track terrorist, guerrilla and insurgent activities
- Assessing and managing categories of risk from terrorism, insurgency or other local factors

**Mark Fitt, Managing Director, N49 Intelligence (N49i)**

### THE FIGHT AGAINST TERROR FINANCING

**11.50 – 12.15 Do Terrorist Groups Have Charitable Arms?**

- Assessing the extent to which charities and the not-for-profit sector are vulnerable to abuse for terrorist purposes
- Implications for governments of terrorist groups exploiting charity in conflict zones – reviewing the UK government's view and the approach of other countries
- The challenges for governments of fighting terrorism internationally without stopping legitimate aid
- The role of charities and voluntary organisations in ensuring that their funds are not diverted for terrorist purposes

**Michelle Russell, Head of Investigations and Enforcement, Charity Commission for England and Wales**

**12.15 – 12.40 Combating Terrorist Financing**

- An assessment of global efforts to tackle money laundering and the financing of terrorism

- The terror financing spectrum – and asymmetric approaches to terror financing
- Advanced intelligence solutions for tracking and targeting illicit finance

**Andrew Lewis, President, Ulysses Group**

**12.40 – 14.00 Lunch/Exhibition Visit**

### DEFEATING RADICALISATION AND HOMEGROWN TERROR

**14.00 – 14.25 Challenging Radical Ideology – Defeating Homegrown Terror**

- How big is the threat from home grown terror – and is Islamist radicalisation still a major concern?
- Challenging westophobic ideological influences and social insularity from within Muslim communities
- Why do transnational extremist organisations succeed where democratic movements fail?

**Maajid Nawaz, Director and Co-founder, Quilliam**

**14.25 – 14.45 Guidance for Identifying People Vulnerable to Recruitment into Violent Extremism**

- Using radicalisation research to develop guidance for identifying individuals who are vulnerable to being recruited into or involved in violent extremism
- How the guidance supports the UK Government's CONTEST counter-terrorism strategy
- Helping public agencies identify those who may be vulnerable to being targeted by extremists.
- Positive strategies for engaging with families, peers, communities and religious organisations to prevent extremist recruitment

**Dr. Jon Cole, School of Psychology, University of Liverpool**

**14.45 – 15.10 Lessons from the Toronto 18 – An Insider's Review of Islamist Radicalisation and Terrorism**

- How radical thought can move to terrorist action – theories of radicalisation
- How online radicalisation culminated in a plot to attack law enforcement, intelligence personnel and government sites
- Indicators of radicalisation and prevention tools for law enforcement and intelligence agencies

**Mubin Shaikh, National Security Consultant and former Canadian Security Intelligence Service Agent**

**15.10 – 15.30 Social Networking Terrorism: The IVP guidance in Practice**

- Assessing the extent to which terrorist organisations have embraced the influence of the internet in distributing their message and recruiting individuals
- Using the internet as a source for intelligence and a means for learning how terrorist entities influence individuals
- Identifying Vulnerable Persons guidance in practice – how to identify persons vulnerable to extremism
- Examining the IVP's effectiveness in classifying terrorist social networks and internet sites

**Jeff Weyers, M.Sc., University of Liverpool**

### UNDERSTANDING EMERGING THREATS

**15.30 – 16.00 Ripples of Consequence – Global Change**

- Understanding the fundamental changes taking place that will cause a rise in extremist behaviour and terrorist activity
- Impact of changing political and economic maps, the divisions between societies and the role of new digital technology
- Assessing the opportunity for extremism of all shapes and forms
- Future consequences and implications

**James Stuart, Director, Alt3**

**16.00 – 16.30 Panel Discussion**

- Which groups will be the key actors in global counter terrorism in the future and why?
- Where is the greatest threat likely to emerge from?
- What will be the long term impact of a leaderless Al Qa'ida?

**16.30 Close of Global Counter Terrorism Conference**

# Critical National Infrastructure – Protection, Security & Resilience

DAY ONE: WEDNESDAY 25 APRIL



**08.00 – 08.45 Coffee/Registration**  
**08.45 – 09.00 Chairman's Welcome and Opening Remarks**  
**Neil J Hall AFNI, Assistant Commissioner (Retired)**

## PROTECTION AND SECURITY FOR CRITICAL INFRASTRUCTURE

**09.00 – 09.20 Protecting Offshore Installations and Structures**

- The role of non-governmental security forces in protecting offshore installations and structures like oil and gas rigs or wind farms
- Monitoring the Safety Zone – enforcement of Safety Zones and prosecution of infringements
- Views on the use of force in repelling infringements and potential acts of terrorism against oil rigs and high sea mining facilities
- The defence against clear and present danger by non-governmental security forces

**Ingo Klaus Wamser, Rechtsanwalt, Member of the International Criminal Bar**

**09.20 – 09.40 Challenges and Opportunities in Critical National Infrastructure Protection**

- Asia risk landscape in 2012 and challenges for critical infrastructure protection in India
- Growing relevance of critical infrastructure security in the maritime sector
- Case Study – Design and implementation of an integrated security system for a major Oil & Gas company

**Cdr. Jasbir Singh, Head-Critical Infrastructure Group, Mahindra Special Services Group (MSSG)**

**09.40 – 10.00 Resilience of Critical National Infrastructure and its Interdependencies – Building Resilient Futures**

- Maintaining critical assets and industries – what is critical and what is not
- Assessing the interdependencies between critical infrastructures
- The importance of non-critical infrastructure in ensuring resilience
- The role of government and private industry in critical infrastructure resilience

**Centre for the Protection of National Infrastructure (CPNI)\***

**10.00 – 10.30 Round Table**

- What are the main threats for critical infrastructure and what are the consequences of failure?
- What are the contingencies and will they work?

**10.30 – 11.00 Coffee/Tea/Exhibition Visit**

## PREVENTING AND RESPONDING TO DISASTER

**11.00 – 11.20 The UK Response – Building a Resilience Community**

- How the UK structures emergency planning and response
- The role of horizon-scanning and risk assessment in mitigating disruptive challenges to the UK
- Ensuring effective and proportionate central Government response to major emergencies
- The importance of the human component of resilience – inspiring responders at all levels including civil society, communities and the public

**John Tesh, Deputy Director, Civil Contingencies Secretariat, Cabinet Office**

**11.20 – 11.40 The Role of Business Continuity in Critical National Infrastructure Protection**

- Assessing national and international standards – differences, common ground and contradictions
- Making the transition from the British Standard to the ISO
- Business continuity vs. crisis management in ensuring organisational resilience
- Is the Organisational Resilience ISO really the future of Business Continuity for Critical National Infrastructure protection?

**Tim McGarr, Risk & Business Continuity, BSI**

**11.40 – 12.00 Crisis Management in the Digital Media Age**

- Assessing the impact of social and digital media from recent events
- Emerging and evolving challenges of digital crises
- Key components of a crisis media strategy

**Anna Averkiou, International Media & Communications Consultant, Trainer & Journalist**

**12.00 – 12.30 Round Table**

- Are generic business continuity plans any good?
- How important is it to have response plans which are appropriate to the threat and proportionate to the risk?
- What are the key steps to enhancing emergency preparedness?

**12.30 – 14.00 Lunch/Exhibition Visit**

## SECURING INDUSTRIAL NETWORKS AND ESSENTIAL UTILITIES

**14.00 – 14.20 A Holistic Security Approach to Securing Remote Industrial Facilities**

- Assessing the complexities of designing and implementing physically and logically secure solutions for remote industrial facilities for CNI
- Cyber security threats to industrial control networks
- Impact of changes in technology and in the political environment that put unmanned CNI facilities at risk
- The importance of a blended approach to physical hardening, electronic surveillance and cyber security
- Unique challenges of securing remote industrial facilities

**David Ratcliffe, Security Consultant, United Utilities**

**14.20 – 14.40 Securing Power Networks in the Critical National Infrastructure (CNI)**

- The importance of power networks in the UK's critical infrastructure
- Challenges and responsibilities in delivering a safe, secure and sustainable power via electricity distribution networks
- Preventing and responding to the impact of crime on power networks
- Practical steps to securing vital electricity distribution networks

**David Shepherd, Head of Security, UK Power Networks**

**14.40 – 15.00 Maintaining the Supply – the Role of an Essential Utility Provider**

- Assessing the threats and risks – securing the control and monitoring of critical functions
- Preventing interruption of supply during a crisis – responsibilities and actions for an essential utility provider
- The role of effective crisis management planning incorporating emergency response, disaster recovery, contingency communications and business continuity

**Barrie Millett, Head of Business Resilience, E.ON**

**15.00 – 15.30 Round Table**

- How should the UK go about architecting resilient control networks?
- What can utilities owners and operators do to strengthen emergency preparedness?

**15.30 – 16.00 Coffee/Tea/Exhibition Visit**

## THE ROLE OF INNOVATION AND TECHNOLOGY

**16.00 – 16.20 The Role of Resilient Communication Technology**

- Assessing the extent to which increasing reliance on technology and communications increases vulnerabilities
- Ensuring communications network resilience in response to crime, natural disasters or terrorist attacks
- Solutions to increasing technology resilience

**Bernie Auguste, Head of Security, BT Openreach**

**16.20 – 16.40 Innovation and Technology Exploitation for Aviation Transport Security**

- The Office for Security & Counter-Terrorism (OSCT) and Thales Technology Demonstrator investigation into Aviation Security
- Innovation & technology exploitation with the goals of improved security, increased revenue, and enhanced passenger experience
- A new philosophy and systems approach to delivering aviation security in the 21st century
- System-level integration of cutting-edge security technologies and processes across three domains

**Professor Adam Ogilvie-Smith, UKTI Security Adviser**

**16.40 – 17.00 Harnessing Augmented Reality for CNI Protection**

- How augmented reality can help us understand risk in the real world
- How scenario planning can be visualised and trained for using multiple scenarios and multiple threats – its role in protecting critical infrastructure
- Making counter-terrorism more accessible – using AR to enhance design and asset protection

**Julian Cracknell, Director – National Security and Public Safety, Logica**

\* subject to final confirmation

# Critical National Infrastructure – Protection, Security & Resilience

## 17.00 – 17.30 Round Table

- Who should guard the digital realm, local authorities or the protection services?
- What opportunities do new technologies bring and how can they best be exploited?
- What difference should innovation and technology make in how businesses plan for crisis?

## 17.30 Close of Day One and Evening Drinks Reception

Networking Reception Sponsor

Industry Sponsor



## DAY TWO: THURSDAY 26 APRIL



### 08.00 – 08.45 Coffee/Registration

### 08.45 – 09.00 Chairman's Welcome and Opening Remarks

Neil J Hall AFNI, Assistant Commissioner (Retired)

## EMERGING THREATS

### 09.00 – 09.20 Smartphone Security Risks and Exploits

- An update on new and emerging threats – implications for owners and operators of critical national infrastructure
- An insight into current hacker techniques – practical steps to protect organisations
- The terrorist and the smartphone

Nigel Stanley, Practice Leader – Security, Bloor Research

### 09.20 – 09.40 Cyber Attack! Recovering from Computer Compromises: Case Study

- Preparing for common network attacks and security incidents
- Why lack of preparation and planning results in longer than necessary outages
- Why a lack of computer forensic evidence means criminal investigations are highly improbable
- How simple plans can greatly enhance an organisation's ability to resist and respond to an attack
- Concepts, planning stages and countermeasures

Steve Armstrong, Senior Incident Responder, Logically Secure

### 09.40 – 10.00 Protecting Site Security from Social Engineering

- Breaches of site security – a review of example techniques including social engineering
- Importance of maintaining rules processes
- Countering the dangerous assumption that null events indicate that risk has reduced

Julian Lea-Jones C.Eng, FRAeS, Assessor for European Commission Advanced Technology Projects

### 10.00 – 10.30 Round Table

- What is the extent of the threat from disruptive technologies?
- How can CNI be protected from threats delivered by evolving digital technologies?

### 10.30 – 11.00 Coffee/Tea/Exhibition Visit

## MAINTAINING CRITICAL NETWORKS

### 11.00 – 11.20 Managing Disruptions to the Road Network

- Using intelligence led risk assessment to manage the threat
- Extent of threat to the road infrastructure from natural hazards, acts of terrorism and crime
- Ensuring resilience in weather emergencies and other extreme events
- Importance of good working relationships between local authorities and the Highways Agency

Martin Hobbs, NDDC Network Management Group Leader, Highways Agency

### 11.20 – 11.40 Security Assurance and Resilience for London's Transport Networks

- Extent of the threat to the transport network from breaches of physical, personnel and electronic security
- Ensuring appropriate security measures are in place and are commensurate with the identified risk
- Importance of key relationships between TfL, intelligence and law enforcement agencies in delivering security and resilience
- Impact of the 2012 Olympics on the threat landscape

Richard Bell MSyI, Security Audit Manager, Transport for London (TfL)

### 11.40 – 12.00 Aggro Terrorism and Disruption of Food Supply in Non Conventional Attacks

- What is the nature of the threat from aggro-terrorism and what are the prospects of a large scale act of bioterrorism?

- Assessing the potential impact on food supply and other critical networks?
- Possible roles of animals in perpetuating a biological agent in a non conventional attack

David Bailey BVSc MRCVS, Veterinary Advisor – Police Service of Northern Ireland (PSNI)

### 12.00 – 12.30 Round Table

- Is there too much focus on low probability threats? Where should the focus lie?
- What are the greatest threats – are they 'human' or 'natural'?

### 12.30 – 14.00 Lunch/Exhibition Visit

## HUMAN FACTORS AND SECURITY CULTURES

### 14.00 – 14.20 Resilience War-Gaming for Counter Terrorism Preparedness and Crisis Management – "Developing Preparedness and Exercising Resilience"

- Understanding the threat of terrorism and the potential impact on organisations
- Using resilience-war gaming for CT preparedness and crisis management
- The need for preparedness and resilience
- Types of exercises
- Strengths and weaknesses of traditional exercise regimes

Malcolm Baker, Director, Resilience

### 14.20 – 14.40 Resilience War-Gaming for Counter Terrorism Preparedness and Crisis Management – "How to Design and Run a War-game"

- Benefits of using hypothetical scenarios to test resilience plans and schemes
- Introducing real counter terrorism scenarios – simulating crisis situations and testing crisis management
- Designing a war-game
- Running and facilitating a war-game
- Learning from a war-game

Philip Hannah, Director, SevenQuestions

### 14.40 – 15.00 The Human Element

- The role of human factors in security and counter-terrorism
- The applicability and relevance of human factors in the protection of critical national infrastructure
- Key factors in the identification and interpretation of any form of possible suspect behaviour
- The 'human element' and its application in the security realm

Dr Martin Langham, Director, User Perspective

### 15.00 – 15.20 Protecting Human Resources – Security Screening Best Practice

- Assessing the need for pre-employment screening across all sectors of commerce, industry and the public services
- The extent to which screening must be carried out by any companies employing personnel with access to sensitive and confidential information, or in positions of responsibility
- The nature of ISO 9001:2000 compliance and the requirement to incorporate screening
- A review of the major update of BS 7858 – Security screening of individuals employed in a security environment

Justin P. Bentley, Chief Executive Officer, International Professional Security Association

### 15.20 – 16.00 Round Table

- What are the best strategies for ensuring workforce security & resilience?
- What are the key pointers for when current or former employees represent a security risk? What action to take?

### 16.00 Close of CNI Conference

# Protecting Crowded Places

DAY ONE: WEDNESDAY 25 APRIL

08.00 – 08.45 **Coffee/Registration**

08.45 – 09.00 **Chairman's Welcome & Opening Remarks**  
**Professor Chris Kemp, Executive Dean, The International Centre for Crowd Management and Security Studies, Bucks New University**

## DESIGNING-OUT TERRORISM

09.00 – 09.25 **Securing and Protecting Crowded Places through Innovative Venue Design**

- Key principles in the design and planning stages
- Relevance of counter terrorism concerns to large venue design
- Designing in anti terrorism measures that are aesthetically and operationally unobtrusive

**Nick Goldby GCGI LCGI, Senior Consultant, Resilience, Security and Risk, Arup**

09.25 – 09.50 **Counter Terrorism and Crime Prevention through Design**

- The role of design in creating products, places and systems resistant to crime, disorder and terrorism
- Assessing why some designed environments are successful while others are unsuccessful and prone to crime
- Key design methodologies and principles for securing people, places and buildings

**Professor Paul Ekblom, Professor and Co-Director of the University of the Arts London Research Centre on Design Against Crime and Associate UCL Jill Dando Institute Of Security And Crime Science**

09.50 – 10.40 **Mitigating Vehicle Borne Terrorism**

- Types of vehicle-borne threat and the essentials of hostile vehicle mitigation
- Latest measures to protect assets from terrorism and vehicle borne devices
- Striking a balance between effective and visible security

**Centre for the Protection of National Infrastructure (CPNI)**

10.40 – 11.00 **Coffee/Tea/Exhibition Visit**

## PROTECTING THE ULTIMATE SPORTING EVENT

11.00 – 11.30 **Delivering Safe Events**

- The role of police counter terrorism security coordinators at large events
- The police security philosophy – basic principles and lessons from other major events
- The importance of police/public partnerships in delivering secure events

**Chief Inspector Phil Maddock, Counter Terrorism Security Coordinator, SO20 Protective Security Command, Metropolitan Police Service**

11.30 – 12.00 **Protecting Crowded Places in the Olympic Year – UK Strategies**

- Assessing the terrorist threat to crowded places – the Olympic angle
- Impact of large events on the protection strategies for public places, buildings and transport environments
- Assessing the public's acceptance and support of crowded places counter terrorism measures
- Using Project ARGUS to design counter terrorism measures into structures and space for safer crowded places

**National Counter Terrorism Security Office (NaCTSO)**

12.00 – 12.40 **Radios, Riots and Responses – Emerging Lessons for 2012**

- The emergency service response during the riots in London and across the United Kingdom – the evolving role of communications
- The criticality of force mobilisation and integrated response to terrorism threats and incidents
- Addressing the security burden associated with the Olympics – communications enhancements and developments
- Implications of fiscal austerity for future communications infrastructure and systems beyond 2012

**Dr. Dave Sloggett, Author and Independent Academic**

12.40 – 14.00 **Lunch/Exhibition Visit**

## PROTECTIVE SECURITY IN CROWDED PLACES

14.00 – 14.30 **Crowded Places Security – Policing Britain's Railway**

- Assessing the terrorist threat to major transport hubs and the impact of large events, such as the Olympics
- Security and policing options for crowded places – protecting mass transit rail
- Responding proportionately to ambiguous incidents and communicating risk effectively

**Adrian Dwyer OBE, Force Counter Terrorism Risk Advisor, British Transport Police**

14.30 – 15.00 **Ensuring the Safety and Security of Visitors, Retailers and Staff in Shopping Centres**

- The role of integrated communications solutions in the management of security in shopping environments
- Promoting a co-ordinated effort in tackling criminal activity and providing tightened security
- Views on the design of security environments for shopping centres – what works and what doesn't

**Dawn Osborne DipSCM, Head of Operations, Meadowhall Centre**

15.00 – 15.30 **Protective Security for Public Transport Systems**

- Securing open and accessible transportation systems while delivering protective security
- Assessing where and when to take action – getting the balance between high and low probability threats
- A view of the future of transport security – innovations and technologies for countering the threat of terrorist attacks

**Chris Lynch, Transport Security Lead, Deloitte**

15.30 – 16.00 **Coffee/Tea/Exhibition Visit**

16.00 – 16.30 **Major Incident Response**

- How Category One responders deal with mass casualty and crowded places incidents
- Special arrangements to be implemented by hospitals, ambulance trusts and primary care organisations
- Building successful responses to incidents by consistent command structures and good liaison between responding agencies

**Sheena McCabe, Sector Emergency Planning Officer, NHS East London and the City**

16.30 – 17.00 **Enhanced Ambulance Response – Hazardous Area Response Team (HART)**

- Update on HART progress and linkages with emergency preparedness structures in the NHS
- Preparations for the Olympic and Paralympic games
- Examples of work to date and future developments

**Russ Mansford, Strategic Ambulance Advisor, Department of Health**

17.00 – 17.30 **Crisis Communication following CBRN Terrorism**

- A review of protective actions following disasters or acts of terrorism involving a CBRN agent
- Lessons learned from the PIRATE and Chemical Incident Emergencies Toolkit (CIE) research projects
- Key factors influencing public compliance – the importance of perceived incident severity

**Dr Julia Pearce, Department of War Studies, Kings College London**

17.30 **Close of Day One and Evening Drinks Reception**

Networking Reception Sponsor

Industry Sponsor



# Protecting Crowded Places

DAY TWO: THURSDAY 26 APRIL

**8.00 – 08.45 Coffee/Registration**

**08.45 – 09.00 Chairman's Welcome & Opening Remarks**

**Professor Chris Kemp, Executive Dean, The International Centre for Crowd Management and Security Studies, Bucks New University**

## BIG PICTURE INFLUENCES ON SECURITY IN 2012

**09.00 – 09.40 Crowded Places Protective Security – Specific Issues for London 2012**

- Strategies for crowded places to prepare for, respond to, and recover from terrorist attack
- Design, implementation & management issues when protecting 'soft' targets
- Securing sports grounds, shopping centres and entertainment facilities

**Chris Phillips GCGI Fsysl, International Protect and Prepare Security Office**

**09.40 – 10.20 The Evolving Terrorism Landscape – Influences and Threats**

- Is Al Qa'ida exploiting the 2011 Arab revolutions?
- Will the increased volatility in the region encourage jihadists?
- Implications for the UK of the evolving footprint of Al Qa'ida
- How can businesses stay ahead of the game and understand the changes?

**Hugh Macleod, COO, Stirling Assynt**

**10.20 – 10.40 Panel Discussion**

- What are the implications of Olympic security and preparedness for owners and operators of crowded places?
- How can businesses get ready for 2012? Key actions, tactics and strategies

**10.40 – 11.00 Coffee/Tea/Exhibition Visit**

## PRACTICAL RESPONSES TO TERRORISM

**11.00 – 11.30 Bombs, Buildings and Crowded Places**

- Brief introduction to explosive threats and their effects
- Building design attributes – good and bad.
- Recent glazing trials research – large façade trial.
- Blast effects on building elements – conclusions

**Darius Aibara, Director, Aibara Associates & Mike Crossley, Michael Crossley Consult**

**11.30 – 12.00 Reducing Vulnerability to Attack – the Role of Vulnerability Assessments**

- Understanding vulnerabilities to attack – delivering best practice advice
- Responsibilities and obligations of business to protect staff and customers and to have plans in place to manage terrorism situations
- Identifying and promoting key actions to reduce vulnerability to a terrorist attack
- Update on the Vulnerability Self Assessment Tool

**National Counter Terrorism Security Office (NaCTS0)**

**12.00 – 12.30 Enhanced Terminal Security**

- Deploying high tech security measures and technologies to enhance terminal security
- The role of the Aviation Security Operation Centre in Israel
- Addressing terrorism opportunities at airports through the use of technology
- Lessons from the implementation of security measures

**Dvir Rubinstein, Aviation Security Operation Centre Manager, Ministry of Transport, State of Israel**

**12.30 – 14.00 Lunch/Exhibition Visit**

**14.00 – 14.30 Tactical Responses to Crowded Places Terrorism**

- Identification of critical need factors in responding to crowded places incidents
  - Tactics for law enforcement and other agencies
  - Strategies for collaboration between all levels of law enforcement
- Chadd Harbaugh, President, Government Training Institute, USA**

**14.30 – 15.00 Urban CBRNE Preparedness**

- Mapping out what is expected to happen during a terrorist CBRNE attack in a megapolis
- Assessing the preparedness of major megapolis hospitals for a CBRNE incident
- Operational experiences and lessons for 2012

**BG(ret'd) Ioannis Galatas, MD, MA(Terr), MC(Army) former Head Department of Asymmetric Threats, Hellenic National Defence General Staff, Greece**

**15.00 – 15.30 Preventing Exploitation of Fireworks and Amateur Bombs**

- Mechanisms employed by the Fire and Rescue Service, Police Force and other agencies in tackling the threat
- Implications for crowded places safety from the importation and use of illegal fireworks
- Legislative and regulatory difficulties – distinguishing between 'fireworks' and 'IEDs'

**Chris Case, Group Manager, Merseyside Fire & Rescue and Vice President, Institute of Explosive Engineers**

**15.30 – 16.00 Combating the Evolving Threat of Body-worn and Packaged Explosive Devices**

- Emerging technologies for explosive residue detection
  - Using stand off imaging for real-time observation of residue on people, clothing, luggage and cargo
  - Method of operation, results obtained and security applications
- Professor John Tyrer, Professor of Optical Instrumentation, Loughborough University**

**16.00 – 16.30 Panel Discussion**

- Is an all hazards all agencies approach to emergencies in crowded places in place and effective?
- What is best practice and how can it be best shared to enhance protective security against traditional and non-traditional threats?

**16.30 Close of Protecting Crowded Places Conference**



# The Cost of Terrorism to Business – Best Practice Risk Management

DAY ONE: WEDNESDAY 25 APRIL



## 09.00 – 09.15 Introduction

**Chris Holt MBE, Consulting Director, Aon**

## 09.15 – 10.15 International Terrorism Today

- The current situation: perception versus fact
- Looking to the future, what lies ahead?

**Frank Gardner OBE, Security Correspondent, BBC**

## 10.15 – 11.00 Quantifying Terrorism Risk

- Rhetoric and reality – what terrorists say and do
- Data versus intelligence
- Potentiality, probability and risk
- Where does terrorism fit on the corporate risk register?

**Dr David Claridge, Managing Director, The Risk Advisory Group**

## 11.00 – 11.30 Coffee/Tea/Exhibition

## 11.30 – 12.15 The Psychology of Terrorism and Martyrdom

- Propaganda of the Deed
- Terrorist Target Selection
- Building Resilience by Communicating the Threat
- Variations in perception and behavioural responses to the risk of CBRN terrorism

**Dr Brooke Rogers, senior lecturer on Terrorism, King's College, London**

## 12.15 – 13.00 Effective Terrorism Risk Management for Business Today

- Implications of terrorism for the private sector
- Mitigating the threat by reducing vulnerabilities
- Using insurance as a means to improve security
- Introducing PML (Probable Maximum Loss)

**Chris Phillips, former head of the National Counter Terrorism Security Office (NACTSO)**

## 13.00 – 14.00 Lunch/Exhibition

## 14.00 – 15.00 Blast Modelling and Hostile Vehicle Mitigation

- Blast modelling: benefits to business
  - Hostile vehicle mitigation – a pragmatic approach
  - Design concepts for reducing business interruption
- Gary Heward, Managing Director, MFD International**

## 15.00 – 15.30 Coffee/Tea/Exhibition

## 15.30 – 16.15 Responding to the Crisis – a Legal Perspective

- Terrorism and the law
- Duty of Care and other liabilities
- Association to terrorism – reputation management
- Extortion – lessons in response

**James Libson, Partner, Mishcon de Reya Solicitors**

## 16.15 – 17.00 Kidnap: the Human Cost

- Where, why, how and when?
- Incident management: what organisations need to know
- Tactical negotiation strategy
- Reducing the risk and incident recovery

**Graham Ashcroft MBE, Operations Director, NYA International**

## 17.00 Close of Day One and Evening Drinks Reception

Networking Reception Sponsor

Industry Sponsor



## 09.15 – 10.15 Frank Gardner OBE, Security Correspondent, BBC



Frank Gardner is the BBC's first fulltime Security Correspondent, reporting for TV, radio and online on issues of both UK and international security. In 2004 he was shot six times at close range by Al-Qaeda gunmen while filming in Riyadh, Saudi Arabia but survived with major injuries. He is an Arabist with a degree in Arabic & Islamic Studies from Exeter University and he worked all over the Gulf before becoming the BBC's Middle East Correspondent in Cairo. He has reported firsthand on terrorism and security from around the Middle East, notably Saudi Arabia and Yemen, as well as Afghanistan, Pakistan, the US, Guantanamo Bay and the Horn of Africa. He has given evidence to various UK Parliamentary Select Committees on the conduct of the War on Terrorism. He was awarded the OBE by HM The Queen in 2005 for services to journalism, awarded Honorary Doctorates of Laws by Nottingham, Staffordshire and Exeter Universities, the McWhirter Award for Bravery, Spain's El Mundo Prize for International Journalism, the Zayed Medal for Journalism and voted Person of the Year by the UK Press Gazette. He is a Fellow of the Royal Geographical Society and his Sunday Times bestseller 'Blood and Sand', describing his 25 years of Middle Eastern experiences, was published by Transworld in 2006. His most recent book, Far Horizons, about unusual journeys to unusual places, was published in paperback in July 2010.



# Cyber Security & Electronic Terrorism

## DAY TWO: THURSDAY 26 APRIL

**08.00 – 08.45** Coffee/Registration

**08.45 – 09.00** Chairman's Opening Remarks  
Gordon Morrison, Defence & Security Director, Intellect

### NATIONAL SECURITY IN THE CYBER AGE

**09.00 – 09.30** Securing Cyberspace – Challenges and Consequences

- Assessing evolving digital infrastructures and the capacity for warfare in cyberspace
- How organisations are threatened by computer malwares and organised cyber criminal gangs
- The significance of digital and social media in combating or advancing cyber terrorism

Azeem Aleem, Principal Lecturer Internet Security and Course Leader for Risk and Security Management Programme, University of Portsmouth

**09.30 – 10.00** Security and the Cyber Threat

- Assessing the unprecedented growth in cyber criminality and the associated threats and challenges
- Who is the main enemy? State-sponsored actors, organised criminal groups, hactivist networks or terrorist groups?
- The role of international partnerships and alliances in building sufficient capacity and capability to handle increasing volumes of cyber crime
- Countering cyber criminality by promoting expertise, information-sharing, best practice and technical assistance to domestic and international law enforcement cyber crime units

John Lyons, Chief Executive, International Cyber Security Protection Alliance

**10.00 – 10.30** Cyber Attack Analysis

- What are the real threats posed by modern cyber attacks, how has it evolved from Cybercrime to warfare, espionage, hacktivism and terrorism
- What are the implications of attacks targeted at critical infrastructure providers and industrial control systems?
- How have attacks such as Stuxnet, Duke and Nitro changed the anatomy of an attack
- What is being or should be done to promote and coordinate protection of critical industry cyber networks and guard against complex threats

Greg Day, EMEA Security CTO and Director of Security Strategy, Symantec

**10.30 – 11.00** Coffee/Tea/ Exhibition Visit

### COUNTERING CYBER TERRORISM AND CRIMINALITY

**11.00 – 11.30** Policing Criminality in Cyberspace

- Implications for cybercrime prevention and response from the upsurge in digital technologies and social media
- Building capacity to fight cyber crime – best practice in cybercrime investigation, prosecution and training
- Countering the threat of cybercrime through collaboration, education and outreach

Deputy Chief Constable Stuart Hyde, Lead on e-Crime Prevention, Association of Chief Police Officers (ACPO) and President of the Society for the Policing of Cyberspace

**11.30 – 11.55** Social Media – Friend, Foe or Terrorist Threat?

- Assessing the extent of the exploitation of social media by terrorist groups – what is the threat?
- Using social media to curb terrorism
- How should the UK Counter-Terrorism Strategy adapt to deal with social media terror

David Lacey, UK Director of Research, ISSA

**11.55 – 12.20** Corporate Espionage and Cyber Security

- An assessment of how organisations are at risk from corporate espionage in the digital age
- Countering sophisticated targeted attacks – how organisations might be attacked and how to reduce the risk
- Why robust cyber security solutions are vital to prevent corporate espionage

Paul King, Senior Security Adviser, Cisco

**12.20 – 12.45** Cyber Security and the Threat to Information

- Assessing the reason for the increasing volumes of the number and type of cyber security incidents and the prevalent threats to information
- What are the main threats and challenges for agencies and businesses from increasing volumes of cyber attack?
- Strategies and practical advice on methods and techniques for countering cyber threats
- Identifying technical and non-technical methods for attaining acceptable levels of security

Gareth Niblett – Chair BCS Information Security Specialist Group

**12.45 – 14.00** Lunch/Exhibition Visit

### EVOLVING AND EMERGING THREATS

**14.00 – 14.25** Addressing Evolving Cyber Challenges

- Assessing the consequences of a well-planned, well-executed attack against our digital infrastructure
- How do countries, agencies and businesses tackle the issue of a cyberspace without geographic barriers when addressing cyber security and terrorism?
- The evolving capabilities of cyber challenges and use of technology to plan and disguise attacks

Craig Goodwin, Chief Security Officer, Benefex

**14.25 – 14.50** Multidimensional Threats in the Mainstream

- Assessing the importance of the upsurge in targeted attacks
- Identifying the sources – nation-states, industrial competitors or organised crime
- Countering threats to steal valuable proprietary information, compromise individual identities or gain access to their employers network
- Key lessons when deploying mobility together with some practical mitigation techniques

Nader Henein, Security Advisory, BlackBerry Security Group, Research In Motion (RIM)

**14.50 – 15.15** Smartphone Security Risks and Exploits

- An update on new and emerging threats
- Apps from hell – understand the use of downloaded applications to attack your smartphones
- An insight into current hacker techniques – practical steps you can take to protect you and your organisation
- The terrorist and the smartphone

Nigel Stanley, Practice Leader – Security, Bloor Research

**15.15 – 15.40** Countering Evolving and Emerging Cyber Security Threats – Best Practice

- Importance of ensuring good governance and compliance with legislation
- Balancing risk, threat and cost in addressing emerging and evolving security threats
- Building a security culture in which people and processes are perpetually aware of latest threats
- Case Study Example

Richard Nethercott, Global Managing Director of Security, Logica

**15.40 – 16.05** Cyber Security Preparedness in the UK

- To what extent is training and awareness reflected in the next update to the UK cyber strategy?
- Highlighting the clear distinctions between training and awareness
- Assessing the effectiveness of initiatives such as the UK cyber challenge

Steve Southern, Director, Amethyst Risk Management

**16.05 – 16.30** Panel Discussion

- What effect will financial austerity measures have on cyber security? Will investigations into cyber crime, network security investigations and digital forensics be affected?
- Where does the biggest threat lie? With state-sponsored actors, organised criminal groups, hactivist networks or terrorist groups?

**16.30** Close of Cyber Security & Electronic Terrorism Conference

