COUNTER TERRORISM POLICING

Inside This Issue

UK PROTECT - Counter Terrorism Protective Security Newsletter—Edition 7 **November 2017**

THREAT LEVELS

INTERNATIONAL to the UK

SEVERE

AN ATTACK IS HIGHLY LIKELY

NORTHERN IRELAND RELATED in Britain

SUBSTANTIAL

A ATTACK IS A STRONG POSSIBILITY

NORTHERN IRELAND RELATED in NORTHERN IRELAND

SEVERE

AN ATTACK IS HIGHLY LIKELY

For more information please see: http://www.mi5.gov.uk

RUN HIDE TELL

ACT ACTION COUNTERS TERRORISM

Safety Campaign for Youth Launched

Counter Terrorism Policing have enlisted the support of celebrities from entertainment and sport to launch their first-ever safety campaign aimed at children and teenagers.

TV star Bear Grylls and England footballer Jamie Vardy are among the leading stars supporting the first phase of a new initiative designed to teach 11-16 year olds how to react in the unlikely event they are caught in a gun or knife terror attack – including advice not to wait around taking pictures on their phones.

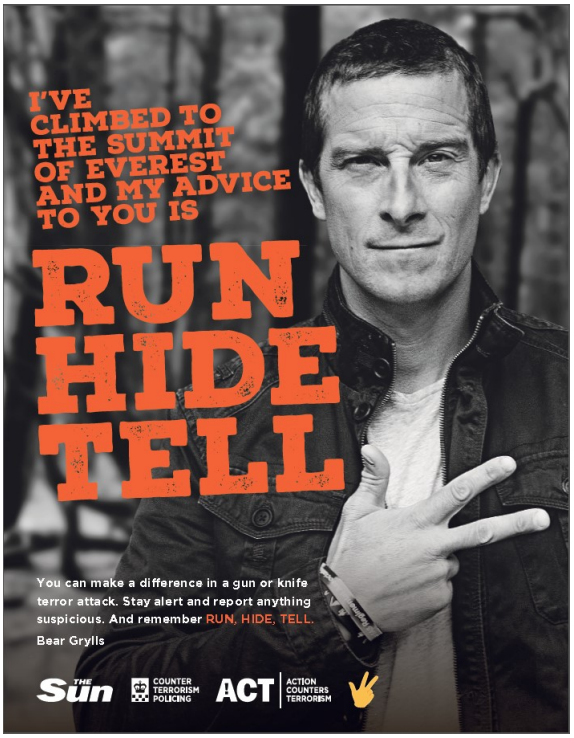
With the UK terror threat level at SEVERE, children will be taught to RUN if they are able to, HIDE if they are not, and TELL police of the threat only when it is safe to do so. They will also be advised to warn others about an on-going threat, and crucially told NOT to stop and use their phones until they are safely away from danger.

Previous messaging – which has formed part of the wider 'Action Counters Terrorism' campaign - has been aimed at adults, but following extensive research with children and young people, security experts from the National Counter Terrorism Security Office (NaCTSO) have created age-appropriate safety advice to engage and empower a younger audience.

NaCTSO have also teamed up with key partners such as the NSPCC, Childline, The Sun and Educate Against Hate, to help and support parents who are understandably anxious about discussing such a topic with their children.

"We appreciate that talking to young people about terrorism can be scary, for parents and children alike," said the National Lead for Protective Security, Deputy Assistant Commissioner Lucy D'Orsi.

"But the atrocities in London and Manchester have sadly resulted in some of the youngest victims of terror this country has ever seen, and if we are able to teach children to act in a way which could potentially save their lives then it is our responsibility to do so. *(continued on page 3)*



(Cont'd) ACT: Action Counters Terrorism for Youth

"We are particularly concerned when we see people – young and old – using their mobiles to film scenes when they should be moving away from the danger. The recent incident in Parsons Green is a good example of this."

"Our research showed that many young people think filming would be a good thing to provide evidence for police. We must get them to understand that the priority must be their safety."

John Cameron, head of NSPCC Helplines, said: "Since April, Childline has already received more than 300 contacts from young people anxious about terrorism, so we know it is a child welfare issue that is impacting on their emotional wellbeing.

"Adults can help a child by listening to their worries, reassuring them these events are rare, and teaching them to Run, Hide, and Tell.

"Although these conversations might be difficult, the spate of devastating events means that they cannot be brushed under the carpet and we all have a duty to help every child stay safe."

CT Policing have very recently, launched a three-phase communications and education plan designed to impart this vital information on young people.

The partnership with The Sun newspaper has seen editorial and creative teams get behind the campaign, as well as enlisting the support of high profile celebrities. They have created a 'Run, Hide, Tell emoji' for phase one, with features promoting the key messages appearing in paper throughout launch week.

This content will run across The Sun's social channels, including the hugely popular Snap channel as part of the wider campaign across social media platforms, television, radio and news outlets giving young people potentially life-saving information.

Tony Gallagher, editor in chief, The Sun, said: "This is a hugely important campaign that will deliver critically important information to a young audience. Through paper, online and our social media platforms we're delighted to do our bit in helping to ensure that the widest possible audience knows to Run, Hide and Tell".

The first of two new Run, Hide, Tell videos features TV personalities Bear Grylls and Ant Middleton, Leicester City footballer Jamie Vardy, England rugby star James Haskell and double Olympic gold medallist Jade Jones, who will tell young people that when caught up in a terror attack: "Real champions run."

Bear Grylls said: I've tackled some of the most dangerous environments on earth, but in the event of a terrorist attack there is only one thing I would advise: "Run, Hide, Tell."

The campaign launch was followed in October by a second, longer, video, designed to explain the 'Run, Hide, Tell' messaging, and also teach children how to spot and report suspicious behaviour or suspicious items.

Later phases of the campaign will then launch this messaging across youth groups such as the Scouts, Guides and Cadets, before finally being made part of the citizenship curriculum of formal education at schools and colleges.

A Conversation With ... Deputy Assistant Commissioner Neil Basu, QPM

'We are still at a Severe threat level from international terrorism and undoubtedly the rhythm of work is very much increased for counter terrorist professionals.'

On 17th October 2016, Neil took up his current role as Senior National Co-ordinator for CT Policing, responsible for delivering the police response to the Pursue and Prevent elements of the Government's CONTEST strategy. In this role he co-ordinates the policing response to threats arising from terrorism and domestic extremism nationally, and also manages the Metropolitan Police Service's Counter Terrorism Command.

What is the role of the Senior National Coordinator?

My role is to provide operational direction to the national counter terrorism network and to oversee the coordination of operational activities across the country. I take responsibility as the national lead during national counter terrorism and domestic extremist incidents, and also major covert operations. Day to day, I direct activity under the Pursue strand of the governments Contest strategy, I work with the Counter Terrorism Coordination Centre to direct activity in relation to the Prevent strand and I ensure Protect and Prepare activity is delivered by the counter terrorism and domestic extremism policing network. A key part of my role is to lead on engagement and communications in order to build public confidence in counter terrorism and domestic extremist policing activity, with the aim of improving safety and security through community intelligence and partnership activity.

We hear lots of stories in the media about the scale of the threat, what's the real situation?

Before March this year, the public could perhaps have been forgiven for thinking that the threat in the UK was somewhat hypothetical or exaggerated. Between June 2013 and March this year, we didn't see any attacks on UK Mainland, however 13 plots were foiled and an increasing number of terrorist arrests were made (340—2015/16) away from the public eye. So whilst the nature of the terrorist threat was clearly changing, with the rise of Daesh, the travel of UK members to Syria and the power of the internet, it probably felt far away and quite remote to many. The pressure on the security service and the police was undoubtedly mounting but despite this, in many ways, we coped. Even after attacks across Europe there was a sense for many of "not in the UK."

However, since March this year the tempo has changed. This is described by experts as a 'Shift' in threat, not a spike. The UK threat level from international terrorism remains at SEVERE and undoubtedly the rhythm of work is very much increased for counter terrorist professionals. Since the Spring, we have suffered multiple ghastly attacks across the nation, 17 weeks of carnage where 36 people were killed, over 200 injured and countless more lives turned upside. Additionally, 6 more attack plots have been thwarted and we can expect that figure to rise. The police and MI5 are currently running just under 600 investigations into 3000 individuals in the UK, who are assessed to pose the biggest threat. There are another 20,000 former subjects, whose risk remains subject to review and I anticipate that these numbers will grow.

What can businesses do to help?

~ Businesses need to make sure they are resilient enough to deal with an attack. Although the attacks feel centred around London, businesses should be mindful that we are thwarting attacks across the nation and as such their resilience should spread just as far.
~ Businesses should be aware of the threats that they can generate or innocently support. Audit the material shared on your internet and intranet websites.
~ Businesses who use hazardous substances, vehicles or dangerous machinery should ensure that none of these can fall into the wrong hands where they could be used for crime or terrorism.
~ Be mindful of who you are employing. Conduct due diligence and look out for signs of radical or extreme behaviours: https://www.gov.uk/government/organisations/national-counter-terrorism-security-office
~ Promote and encourage the reporting of suspicious behaviour amongst all of your work force. They may work in a wide variety of locations and be able to support the wider intelligence picture - the life-blood of our joint fight against terrorism.
~ Ensure that CCTV is working and is the best you can afford. This could deter attackers but also support investigations by providing crucial evidence even if you are sited miles away from an attack
~ Where your commercial interests generate crowded places, businesses have a responsibility to ensure they keep their customers and clientele safe whether its shopping centres, sports grounds, entertainment venues or NTE. That means investing in your own security and public messaging

Learning From Businesses

We have always wanted *Protect* to be a two-way relationship and this is very much starting to happen through initiatives such as the Step Change Summit and the ensuing workshops.

During the recent incident at Parsons Green, it became clear that many businesses had done some great planning and were responding to what had happened through information contained in Protect messaging, and police statements through the media. Importantly, businesses have shared examples of good practice with us in order to bring together more collective experience about security than we have ourselves. It is important that that we tap into this vital learning and share that expertise with others through *Protect*.

Below are some of the great practices we have become aware of across a number of recent events:

Business A
Had a cascade plan to ensure that all their staff were safe and well after the attack

Business B
A producer of a daily product found its premises stuck inside a cordon for a number of days. They had retained facilities at a commercially operated fall-back centre which meant that business was largely uninterrupted.

Business C
Provided a comprehensive briefing note to all their staff explaining what had happened but also what they might expect to see happening both in their own business but also in public spaces
(i.e. soldiers being deployed, more intrusive security at events etc)

Business D
Moved its initial screening of visitors outside the building

Business E
Ensured that its first line of security personnel were outside the building and looking for suspicious behaviour as well as engaging with people approaching their normal security measures

Business F
Rented-in a number of explosive search dogs for screening crowds at a large event

Business G
Increased the number of people delivering its search on entry activity to reduce the build up of crowds

Business H
A hotel, gave every guest a letter explaining that their baggage would be subject to search, could not be stored in the building if they were not present, and would be required to provide proof of identity on checking in

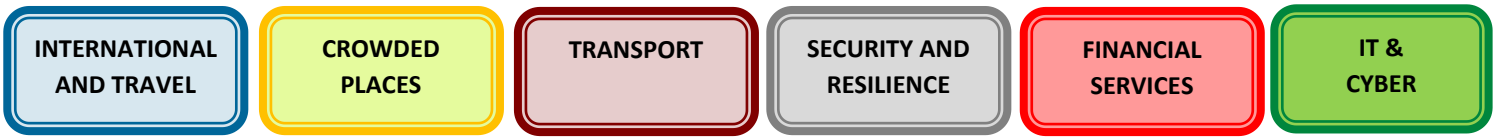
Business I
Increased the searching of vehicles entering its estate

Business J
Tested its security systems including lock-downs, alarms and moveable HVM

Other Businesses
Several businesses increased the number of staff and ensured they were operating in high-visability jackets

Update on Step Change

In July this year National Counter Terrorism held the Step Change Summit which saw people from across all Industry sectors come together following the shift in terrorist activity. Following the event a number of working groups were formed to look at a number of key themes:



These workshops have been meeting and are now collating their findings under the following areas:

A second Step Change Summit is currently being arranged, to be held early in the new year. The summit will provide an update on progress and an overview on each of the themes.

Upcoming Events—Security Expo

A Safer Cities (Closed Door) Roundtable Briefing is taking place on Wednesday 29 November 2017 from 08:30-10:30 in at Olympia in London. This is a high-level meeting on a city-to-city level with Mayoral Offices and leaders on Counter Terrorism & Resilience.

The objective is to consolidate ideas and evolve methodologies to better protect our cities from those intent on causing us harm and ensuring that we are prepared to effectively respond to, and recover from, such attacks. Representatives around the table will include Mayoral Offices and Heads of Counter Terrorism from cities directly affected by terrorist incidents in the last 18 months including London, Barcelona, Melbourne, Brussels, Rotterdam and The Hague.

Places are free-of-charge but strictly by application only for serving members of Government, Authority, Law Enforcement or Emergency Responders.

To attend please apply at www.uksecurityexpo.com/safer-cities-closed-door-briefing

Other presentations by National Counter Terrorism Policing at the event include:

- Detective Chief Superintendent Scott Wilson, Protect and Prepare, National Counter Terrorism Policing HQ, National Police Coordinator on **Enhancing Threat: Step change approach**
- Detective Superintendent David Roney, Deputy National Co-ordinator PROTECT & PREPARE, National Counter Terrorism Policing Headquarters on **Improving Security in Sport**
- James Douglass, IPM, Ports Protective Security Lead, National Counter Terrorism Policing HQ on **Maritime Security Update.**

Cyber Security and the Terrorist Threat 2017

Richard Horne
Partner
PWC

Janet Williams QPM
Chairperson
Torchlight

Terrorists focus on carrying out violent, physical actions. Why? Because such events are most immediate and can be channelled directly into our sitting rooms thereby magnifying their immediate impact, generating publicity for their goals and fear in the population.

However, today, underlying just about every aspect of our physical world, is a set of digital processes and data flows that can be manipulated to affect physical events. Recent events around the world have shown that hospitals can be closed, factories damaged, electrical supplies brought down, TV channels interrupted and control taken of public signage, all via cyber-attacks.

If we cast our minds back to the times of PIRA, their plan was to impact on the U.K.'s electricity supply and cause chaos. So this is nothing new, but now the risks of such attacks succeeding are, arguably, greater. Our digital world is vulnerable and that makes our physical world vulnerable too.

Terrorists use cyber-attacks regularly. Al Qaeda was using cyber-attacks to commit credit card fraud well over a decade ago in order to raise funds. The Syrian Electronic Army was breaching social media feeds years ago and recently we have seen evidence of information gathering from cyber-breaches to help target military personnel. Terrorists use the Internet for online hostile reconnaissance; they use it with great skill to hide their communications and use Internet tools for radicalisation so, we would argue, it is not a great leap to see terrorists using digital techniques within their actual attacks.

Just as we have seen with the physical attacks it is not always possible to predict what they will do and in the digital world the range of possibilities is enormous.

In the near-term there has been speculation about the possibility of the terrorist combining a physical attack on a venue with a cyber breach of some element of the venue management (e.g. the access/exit gates) to maximise impact – i.e. public trapped, emergency responders denied entry.

Such a scenario would require a high degree of sophistication and organisation and *crucially* patiently acquired knowledge of the venues processes.

If we assume that the level of sophistication possessed by terrorists will evolve rather than leap, then we would suggest it likely we will see destructive cyber-attacks aiming to cripple protective security systems infrastructure (e.g. CCTV) and impair emergency services ability to respond to damage/casualties of the physical attack.

The vulnerability of hospitals and global businesses to attacks of this nature has been highlighted in recent months with the Wannacry and Notpetya attacks.

In the longer term the proliferation of connected devices, autonomous vehicles and automated decision-making will rapidly increase our modern society's exposure to destructive cyber-attacks.

So, we would suggest, it is a question of **when** not **if** terrorists deploy cyber-attacks to complement physical attacks. Their motivation to cause maximum harm is a given; the determining factors here are their cyber-capabilities and our cyber-vulnerabilities. Capability can easily be acquired from criminals, supportive nation states or radicalised hackers. Therefore we can be sure that when the opportunity arises, terrorists will exploit it.

We think of our physical world as segregated spaces and entities, public spaces and private spaces. The underpinning digital world doesn't work like that. It is an interconnected world, all space is public space. Thinking back to 9/11 is a helpful physical image of the interrelationship between critical infrastructure, the physical infrastructure and the cyber infrastructure affecting all our space. When the towers came down (part of banking critical infrastructure) the damage destroyed water pipes (physical infrastructure) which then knocked out control systems across parts of New York City (cyber-infrastructure) which in turn affected several key assets (critical infrastructure). Fully understanding these interdependent ecosystems and their multitude of connectivity is important to achieve before an emergency, attack or critical event occurs.

If one understands the true exposure then mitigating negative impact is possible, bringing resilience, enhancing trust and generating a faster return to normality.

Much of counter terrorism has been focussed on protecting against physical attacks only and managing the threat. There now needs to be a greater emphasis on thinking through the potential risk.

Businesses creating new digital technology are forging an incredible new world; and have to think about new risk to their business and customers. This is not identical to the risk to wider society. Individual commercial entities, law enforcement agencies and government bodies can't defend the public in isolation. They may not even understand, on their own, how what they control could be used to cause damage. All three communities need to work together much more closely to anticipate the possible, understand the real exposure and determine the responsibilities for addressing it.

A 'quick win' first piece of work for such an alliance could be to look at hostile reconnaissance online. We know that terrorists have to conduct hostile reconnaissance before an attack, in order to maximise damage & casualties. We also know that this is a vulnerable time for them and they are sensitive to any intervention hence the development of pulse police patrols and behavioural analysis training. Increasingly such hostile reconnaissance is partly conducted online where the terrorist feels safest. By working together to identify patterns for such reconnaissance (what the constituent parts look like, better understanding of what preparatory activity online looks like) and alerting the target base to this knowledge - we can diminish the terrorists scope and effectiveness. We must educate and encourage partners to develop challenges to potential hostile reconnaissance online, e.g. patrolling police avatars or pop-up 'personal assistants' suddenly appearing with a "can I help you?" may unnerve and deter the adversary. Is this *"can I help you?" pop-up* evidence of counter-surveillance defences, or a trip-wire? They cannot be sure.

What is important is that all three communities of interest, work together to identify problems and help each other to solve them.

Summary of Incidents at Home and Abroad

La Rambla, Barcelona, Spain – 17th August 2017

Younes Abouyaaqoub drove a van along La Rambla in Barcelona, hitting pedestrians. 13 people were killed and at least 130 injured. Abouyaaquob fled the scene. Nine hours later five men thought to be members of the same terrorist group, drove into pedestrians in Cambril, killing one woman and injuring six. All five attackers were shot dead by police. On 21st August Abouyaaquob was also shot and killed by police.

Near Buckingham Palace, London, UK – Tuesday 29th August 2017.

Mohiussunnath Chowdhury drove at a police vehicle outside Buckingham Palace. When officers stopped to question him, he attacked them with a 4ft sword and shouted "Allahu Akbar". After a struggle during which the officers sustained minor injuries, the male was arrested.

Outside Commonwealth Stadium, Edmonton, Canada – Saturday 30th September 2017

A hired U-Haul van was used by a lone male to drive into a police checkpoint outside the Commonwealth Stadium during a Canadian National Football League game, hitting one officer. The male then got out of the van and stabbed the officer before driving off. The van was later stopped after hitting several pedestrians. The incident is being investigated as a terror attack, some reports claim and ISIL flag was found in the van.

Parsons Green Tube Station, London, UK – Friday 15th September 2017

At 0820 on 15th September, an improvised explosive device (IED) failed to properly detonate on an eastbound District Line tube train, instead combusting and causing burn injuries to approximately 30 people in the crowded carriage. The main charge which failed to detonate contained TATP the same chemical used in the Manchester Arena bomb.

St Charles Train Station, Marseille, France – Sunday 1st October 2017

Two female cousins were attacked with a knife outside a train station in Marseille by a man shouting "Allahu Akbar". Mauranne Harel, 20, and Laura Paumier, 21, died from their wounds after being stabbed as they waited for a train at Saint Charles station. The assailant was shot dead immediately after the attack, by Operation Sentinelle soldiers, patrolling the station.