National Police Chiefs' Council

National Counter Terrorism Policing Headquarters

NaCTSO National Counter Terrorism Security Office

National Stakeholder Menu of Tactical Options

Background

This document outlines a set of options which can be used by the private sector and security industry to enhance their security posture at times of raised terrorism threat levels or in response to a terrorist incident.

They can be employed independently or in support of the police service's 'National Menu of Counter Terrorism Tactical Options'.

The tactical options included in this document are not exclusive or exhaustive and it is anticipated that this document will be reviewed periodically to ensure it is fit for purpose in meeting the ongoing and ever changing threat from international terrorism and extremist other extremist activity to the UK.

This document has been developed with the assistance and guidance of a number of security experts within the private sector and we thank them for their assistance.

Introduction

The UK threat levels were first made publicly available by the British Government on 1st August 2006, to warn of the likelihood of terrorist activity (prior to this they were available on a restricted basis). Aligned to the threat levels were alert states. To ensure a consistent approach, the response levels replaced all other forms of alert states and indicate how government departments and agencies and their staff should react to each threat. This system serves to inform and prompt businesses to consider their own security arrangements in light of any changes to the threat level.

The MI5 reports on three different categories of terrorist threat.
https://www.mi5.gov.uk/threat-levels

- Threat from international terrorism
- Terrorism threat related to Northern Ireland in Northern Ireland itself
- Terrorism threat related to Northern Ireland in Great Britain

<table>
<tr><th colspan="2">THREAT LEVEL</th><th>ALERT STATES</th><th>RESPONSE</th></tr>
<tr><td>CRITICAL</td><td>An attack is expected imminently</td><td>EXCEPTIONAL</td><td>Maximum protective security measures to meet specific threats and to minimise vulnerability and risk</td></tr>
<tr><td>SEVERE</td><td>An attack is highly likely</td><td rowspan="2">HEIGHTENED</td><td rowspan="2">Additional and substantial protective security measures reflecting the broad nature of the threat combined with specific business and geographical vulnerabilities and judgements on acceptable risk.</td></tr>
<tr><td>SUBSTANTIAL</td><td>An attack is a strong possibility</td></tr>
<tr><td>MODERATE</td><td>An attack is possible, but not likely</td><td>NORMAL</td><td>Routine protective security measures appropriate to the business concerned.</td></tr>
</table>

MI5 maintain a history of threat levels: -

DATE	THREAT FROM INTERNATIONAL TERRORISM	THREAT FROM NORTHERN IRELAND-RELATED TERRORISM	
		IN NORTHERN IRELAND	IN GREAT BRITAIN
11 May 2016	SEVERE	SEVERE	SUBSTANTIAL
29 August 2014	SEVERE	SEVERE	MODERATE
24 October 2012	SUBSTANTIAL	SEVERE	MODERATE
11 July 2011	SUBSTANTIAL	SEVERE	SUBSTANTIAL
24 September 2010	SEVERE	SEVERE (first published)	SUBSTANTIAL (first published)
22 January 2010	SEVERE		
20 July 2009	SUBSTANTIAL		
4 July 2007	SEVERE		
30 June 2007	CRITICAL		
13 August 2006	SEVERE		
10 August 2006	CRITICAL		
1 August 2006	SEVERE (first published)		

In general, the UK threat level has been raised due to a specific terrorist related event that has had an impact to the United Kingdom. However in August 2014 the threat level was raised due to a combination of factors, both International & Domestic, which together compelled an increase to 'Severe'.

It should be noted that an increase to 'Critical' is likely to have a significant impact on the economy of the United Kingdom and resourcing across all agencies, as such it is unlikely to remain in place for an extended period.

Against this background the tactical options included in this document could be used to provide assurance against a range of threats and threat levels.

Attack Methodology

Under the Protective Security Improvement Activity (PSIA) introduced by NaCTSO in 2014, there are six methods that have been identified by which a terrorist attack is assessed as most likely to take place: -

- Non penetrative vehicle attack
  - A vehicle borne explosive that is delivered by parking a vehicle
- Penetrative vehicle attack
  - A vehicle borne explosive that is delivered by force, such as 'ramming'
- Person Borne Improvised Explosive Device (PBIED)
  - An explosive delivered by a person in a suicide attack
- Marauding Terrorist Firearms/Weapons attack (MTFA/MTWA)
  - An attack on individuals with firearms or other weapons (including vehicles) by a single or group of terrorist(s)
- Postal device attack including courier and hand deliveries
  - An explosive, contaminant or hoax delivered by post
- Placed Improvised Explosive Device (IED)
  - An explosive placed within an area (a suspicious package etc.)

The options outlined in this document reflect potential responses to these types of threat.

Overall Strategy

The overall business strategy in dealing with a change in threat level, and in particular with an increase to 'Critical' or in response to an attack should be: -

To understand the type of threat posed (why did the threat level increase? What was the attack methodology?) and to consider the appropriate level of response and tactical options that are best suited to allow them to continue 'business as usual', within the parameters of this heightened state of alert.

As a general guide, the following principles should be central to any decisions:

- It may not be possible to protect everything so prioritise the areas to protect
- Measures employed should be proportionate to the threat
- Do not let the cost exceed the value of the asset being protected
- Security is more cost effective when incorporated into longer-term planning
- Agree a strategy and document all decisions including rationale for change or preserving the status quo

Considerations

Areas that organisations may wish to consider when **planning** for an increase in threat level to 'Critical' are: -

- To agree a menu of site specific tactical options that are suitable for your organisation that can be considered if the threat level increases
- Regularly exercise the plan for 'Critical' to ensure that key stakeholders and staff are aware of the impact on their area of work should a change be necessary
- Ensure that staff have been consulted and agreements are in place if options impact on their working practices (terms and conditions etc.)

Areas that organisations may wish to consider when **reacting** to an increase in threat level, particularly to 'Critical' are: -

- To escalate and engage quickly with key stakeholders
- To consider the range of options relevant to mitigate the threat posed
- To continually review the tactical options to ensure they remain 'fit for purpose'
- Ensure that any change to tactical options serve to provide reassurance to staff rather than cause alarm
- Implement communication strategy to provide advice to staff around changes to planned events, deliveries or changes to access points etc.
- Only react to information from official sources such as the Government, Security Services and the Police
- To have an immediate holding plan available to allow a more permanent solution to be found
- Consider implementing a command and control strategy using the Gold, Silver and Bronze system
  - **GOLD** is in overall control of the organization's resources at the incident and will formulate the strategy for dealing with the incident
  - **SILVER** manages tactical implementation following the strategic direction given by Gold and makes it into sets of actions that are completed by Bronze
  - **BRONZE** directly controls an organization's resources at the incident and will be found with their staff working at the scene
- Minimise disruption to business

Menu of Tactical Options

The following list of tactical options should be considered to support an increase in the threat level, particularly to 'Critical' or following an incident or attack. It is not an exhaustive list and there may be other site specific options which would be relevant to your premises.

A. Lock down procedure
- Have the ability to restrict the number of access points to your premises and if necessary to prevent any access or egress to protect staff

For further Information:
https://www.gov.uk/government/publications/developing-dynamic-lockdown-procedures

B. Increase security presence
- Implement temporary changes to shift patterns to increase staff numbers , (consult with staff in advance and agree on how this can be achieved)
- Consider reciprocal agreements with neighbouring businesses to widen footprint, search areas and consolidate staff
- Implement overt and unpredictable patrolling
- Consider the use of high visibility clothing to increase impact
- Challenge all staff/visitors including those in livered vehicles (Police, utility companies)

For further Information:
https://www.cpni.gov.uk/optimising-people-security

C. Staff Vigilance
- Direct all staff and visitors to wear identification (if this is not usual practice)
- Encourage staff to challenge those not wearing identification and that they do not recognise
- Ensure staff know how to report suspicious behaviour
- Brief staff on response and threat levels

For further Information:
https://www.cpni.gov.uk/embedding-security-behaviour-change

D. Partnership working
- Work in partnership with surrounding businesses to share information on suspicious behaviour, security posture etc.

E. CCTV
- Ensure all parts of the system are fully functioning
- Check vulnerable areas to ensure adequate coverage

For further Information:
https://www.cpni.gov.uk/intruder-detection-tracking-monitoring-and-lighting

F. Parking
- Restrict parking close to buildings and vulnerable areas
- Check parked vehicles for staff or visitor passes

G. Visitors
- Restrict visitors to pre-booked appointments only
- Check photographic identification
- All Visitors to be escorted at all times

For further Information:
https://www.cpni.gov.uk/robust-visitor-entry-processes

H. Implement search regimes
   - Vehicles, hand baggage, people, goods
   - Consider unpredictable times and locations if a full screening regime cannot be maintained to maximise impact/effect

For further Information:
https://www.cpni.gov.uk/building-and-area-search

I. Consider cancelling or postponing events that may place your staff, customers or suppliers at risk

J. Review staff abstractions and consider cancelling non-essential training to maintain resources

K. Deliveries
   - Restrict deliveries to essential and expected items only
   - Where possible scan all mail items
   - Train staff to recognise suspicious items

For further Information:
https://www.cpni.gov.uk/screening-mail-and-courier-deliveries-0

Remember robust and vigilant 'communities' provide a hostile environment for terrorists/criminals to operate in.

Useful Links

The following links provide additional useful information that may assist when deploying the tactical options;

https://www.cpni.gov.uk
https://www.gov.uk/government/publications/stay-safe-film
https://www.gov.uk/nactso
https://www.mi5.gov.uk