National Stakeholder Menu of Tactical Options

COUNTER
TERRORISM
POLICING

NaCTSO
National Counter Terrorism Security Office

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

They can work independently or in support of the police service National Menu of Counter Terrorism Tactical Options. They can be implemented independently by an organisation or can be deployed at the request of police following an extraordinary Security Review Committee (SRC (E)).

The tactical options included in this document are not exclusive 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 to the UK.

This document has been developed with the assistance and guidance of number of security experts within the private sector and the authors would like to thank all of 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 forms of terrorist activity. Prior to this they were available on a restricted basis.

Aligned to the threat levels were alert states, including what was known as the "Bikini state" a colour coded system that was used predominantly by the Military, Police etc. To ensure a consistent approach, the Response Levels replaced all other forms of escalation, 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 Home Office reports on three different categories of terrorist threat.

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

THREAT LEVEL		RESPONSE	
Critical	An attack is expected imminently	EXCEPTIONAL	Maximum protective security measures to meet specific threats and to minimise vulnerability and risk.
Severe	An attack is highly likely	HEIGHTENED	Additional and sustainable protective security measures reflecting the broad nature of the threat combined with specific business and geographical vulnerabilities and judgements on acceptable risk.
Substantial	An attack is a strong possibility		
Moderate	An attack is possible, but not likely	NORMAL	Routine protective security measures appropriate to the business concerned.

MI5 maintain a history of threat levels:

Date	Threat from international terrorism	Threat from Northern Ireland related terrorism	
		In Northern Ireland	In Great Britain
1 Mar 2018	SEVERE	SEVERE	MODERATE
17 Sep 2017	SEVERE	SEVERE	SUBSTANTIAL
15 Sep 2017	CRITICAL	SEVERE	SUBSTANTIAL
27 May 2017	SEVERE	SEVERE	SUBSTANTIAL
23 May 2017	CRITICAL	SEVERE	SUBSTANTIAL
11 May 2016	SEVERE	SEVERE	SUBSTANTIAL
29 Aug 2014	SEVERE	SEVERE	MODERATE
24 Oct 2012	SUBSTANTIAL	SEVERE	MODERATE
11 July 2011	SUBSTANTIAL	SEVERE	SUBSTANTIAL
24 Sept 2010	SEVERE	SEVERE (first published)	SUBSTANTIAL (first published)
22 Jan 2010	SEVERE		
20 July 2009	SUBSTANTIAL		
4 July 2007	SEVERE		
30 Jun 2007	CRITICAL		
13 Aug 2006	SEVERE		
10 Aug 2006	CRITICAL		
1 Aug 2006	SEVERE (first published)		

In general the threat level has been raised post incident because of something happening which has impacted on mainland UK. However, in August 2014, the threat level was raised because of a combination of factors (both Internationally & UK based) which together compelled a raise in threat level to Severe.

It should be noted that an increase to 'Critical' has a huge impact on UK PLC and resourcing across all agencies and it is therefore unlikely to remain in place for long periods of time.

It should also be noted that the tactical options included in this document do not just become employable post a rise to Critical.

Attack Methodology

Under the Protective Security Improvement Activity (PSIA) introduced by NaCTSO in 2014, six methods of attack have been identified:

- Non penetrative vehicle attack
- Penetrative vehicle attack
- PBIED - Person borne Improvised Explosive device (suicide) attack
- Firearms/Weapons attack – (Marauding Terrorist Attack)
- Postal device attack including courier and hand deliveries
- Placed IED.

The tactics outlined in this document reflect the options for response to these types of threat.

Overall Strategy

The overall business strategy in dealing with an increase in threat level to 'Critical' or in response to an attack is:

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 range of tactical options that are best suited to (insert name of contract here) to allow them to continue 'business as usual', within the parameters of this heightened state of alert.

Operational Requirement

The operational requirement to consider when planning for an increase in threat level to 'Critical' is:

- To agree a menu of site specific tactical options that are suitable for your organisation that can be considered if the threat level increases to 'Critical',
- 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 in place if options impact on staff working practices (terms and conditions).

The Operational Requirement to consider when reacting to an increase in threat level to 'Critical' is:

- To escalate and engage quickly with key stakeholders to react when the threat level increases to 'critical',
- 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 for alarm,
- Implement communication strategy to provide advice to staff around changes to planned events/deliveries/changes to access points etc.
- Only react to information from official sources such as the Government, Security Services and Police as there is a lot of misinformation available through unsubstantiated sources,
- 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 Strategic, Tactical and Operational (formerly Gold/Silver/Bronze system),
- **STRATEGIC** is in overall control of the organization's resources at the incident and will formulate the strategy for dealing with the incident,
- **TACTICAL** manages tactical implementation following the strategic direction given by Gold and makes it into sets of actions that are completed by Bronze,
- **OPERATIONAL** 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 now to support an increase in threat level to 'Critical' or following an incident or attack.

This is not an exhaustive list and there may be other site specific options which are relevant to your site. The key to any change is that security patrols should remain unpredictable. Feedback from security services has proved that this is a real deterrent when planning an attack.

A Agree strategy and document all decisions (to include rationale regarding for change or preserving status quo).

B Ensure lock down procedures are tried and tested.

C Implement emergency change to shift patterns (extended shift patterns, change to rotation etc. – Agree plan with staff in advance).

D Review patrol strategy (be unpredictable). Adopt high visibility clothing. (Deployment in Hi-vis will be dependent on the intelligence available and the perceived risk to the site).

E Brigade resources with neighbouring contracts (rotate and share external patrols with other security companies and widen patrol area).

F Report any suspicious activity in a timely manner.

G Implement communication links with surrounding premises to pass on information about suspicious activity/behaviour.

H Consider closing non-essential access and egress points.

I Focus CCTV on all communal areas and vulnerable points.

J Ensure CCTV is fit for purpose.

K Review immediate parking areas and access to them.

L All visitors must give 24 hours' notice.

M Implement search regimes (people, vehicles, baggage, etc.)

N 100% staff ID checks (challenge ALL staff).

O All staff and visitors to wear ID (if this is not usual practice).

P Visitors to be accompanied at all times.

Q	Security officers must check all personnel and vehicles including emergency services – do not assume they are who they say they are!).
S	Consider cancelling or postponing events.
T	Cancellation of all non-essential training ensuring staffing levels are maintained.
U	Staff are briefed on response and threat levels.
V	Restrict deliveries to essential deliveries only (out of hours only).
W	Couriers – Essential deliveries only.
X	Post: ✓Where possible 100% scan ✓Ensure postal procedures are robust

Remember, there is evidence to support that strong, 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;

http://www.cpni.gov.uk

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

http://www.nactso.gov.uk

http://www.mi5.gov.uk

https://www.gov.uk/government/publications/crowded-places-guidance