



TO: Business Co-ordination Board

FROM: Chief Constable

DATE: 22 May 2013

THE NATIONAL POLICING REQUIREMENT

1. Purpose of Paper

This paper provides an overview of the National Policing Requirement and the local response within Cambridgeshire Constabulary.

2. Introduction

In July 2012 the Home Secretary issued the Strategic Policing Requirement (SPR) which set out the five strategic threats to the country. These threats have been assessed and selected from the National Security Risk Assessment on the basis that they either affect multiple police force areas or may require action from multiple forces, resulting in a national response.

As part of the response to the SPR, the National Policing Requirement has been developed by the police service and college of policing. This document details the capacity and contribution, capability, consistency and connectivity required to counter the identified threats.

3. Recommendation

The BCB is recommended to note the report.

4. National Threats

The five identified strategic threats are:

- Public Disorder

- Civil emergencies
- Organised crime
- Terrorism
- Large scale cyber incidents

5. Responsibilities

The purpose of the National Policing Requirement is to allow chief constables and police and crime commissioners to effectively plan for challenges that go beyond their force boundaries. In doing so, they must satisfy themselves that they:

- understand their respective roles in preparing for and tackling shared threats, risks and harm;
- agree, where appropriate in agreement and collaboration with other forces or partners, the contribution that is expected of them; and
- have the capacity and capability to meet that expectation, taking properly into account the remit and contribution of other bodies (particularly national agencies) with responsibilities in the areas set out in the Strategic Policing Requirement.

6. Public Disorder

- 6.1. Threats to public order come from a number of sources. These are identified primarily through the National Domestic Extremism Unit's Strategic Threat Assessment and the National Public Order Strategic Threat and Risk Assessment. Effective monitoring of community tension that may escalate into disorder is crucial to these assessments.
- 6.2. The Police Service should be prepared to deal with three separate seats of significant disorder simultaneously for a period of seven days within the UK. This planning assumption is based on information and experience of historical events (eg, G8, G20, EDL), and is reinforced by the disorders of August 2011.
- 6.3. Each force's contribution to the national mutual aid capacity of 297 PSUs is defined by the Public Order Mobilisation Formula. While delivering against this commitment, forces must complete an annual public order threat and risk assessment and have sufficient trained officers and equipment to support the deployment of their national mutual aid Police Support Units (PSUs).

- 6.4. Forces need to have sufficient accredited public order commanders at gold, silver and bronze level to ensure public order operations are commanded only by these officers.
- 6.5. PSU capability is managed both at a local level and, collaboratively through the three force Operational Planning Unit.
- 6.6. The regional commitment to PSU has recently been agreed within the strategic alliance. The six regional forces can meet the required national commitment while also ensuring sufficient residual capacity remains within each local force as a contingency.

7. Civil Emergencies

- 7.1. The Civil Contingencies Act 2004, places a legal responsibility on the Police Service, as Category 1 responders, to provide an appropriate response to emergencies. An emergency is defined under the Act as a situation or series of events that threatens or causes serious damage to human welfare, the environment or security in the UK.
- 7.2. Within the National Security Strategy, civil emergencies are assessed as Tier 1, 2 and 3 risks. Tier 1 risks are judged to be the highest priorities for UK national security over the next five years, taking into account both their likelihood and impact.
- 7.3. Local responders are expected to be the building blocks of response for an emergency of any scale. Most arrangements for this are delivered through Local Resilience Forums (LRFs), which are multi-agency partnerships made up of representatives from local public services, including the emergency services, local authorities, the NHS, the Environment Agency and other partners. Successful functioning of the LRF is fundamental to achieving interoperability between emergency responders.
- 7.4. At the national level, the Police Service should be prepared to deal with a major accident or natural hazard which requires a national response. Examples include severe coastal flooding affecting three or more regions of the UK, or an influenza pandemic.
- 7.5. Forces should be able to contribute sufficient specialist trained officers to support any deployments, including appropriate command structures.
- 7.6. Through the LRF mechanism, forces will assess the risk of emergencies occurring and use this information to inform the community risk register and contingency planning as well as support multi-agency co-operation. Each LRF has arrangements in place to deal with civil emergencies.

7.7. Cambridgeshire can evidence capability in delivering effective emergency planning and business continuity responses through the actions of the Force Resilience Unit and the established LRF.

8. Serious and Organised Crime

8.1. The current, key Serious and Organised Crime (SOC) threats identified in the UK Threat Assessment are:

- trafficking of controlled drugs
- organised immigration crime
- financial crime (fraud)
- organised acquisitive crime.

8.2. All regions have now developed regional organised crime units (ROCU) and, while these vary in their capacity, capability and strategic approach, they all provide an operational policing platform beyond the local level and in support of national agencies. Generally these teams provide a range of specialist operational, surveillance, covert and technical functions, all of which are required to attack the most problematic organised offenders successfully.

8.3. Cambridgeshire is served by the Eastern Region Specialist Operations Unit (ERSOU).

8.4. In 2013 the National Crime Agency (NCA) will be established to spearhead a national crime-fighting response to SOC. The NCA will consist of four commands which will cover:

- organised crime
- border crime
- fraud and cyber crime
- protection of children and young people.

8.5. The threat from organised crime is managed operationally through the Integrated Operating Model (IOM). The IOM enables UK law enforcement agencies to evaluate and tackle organised crime effectively. The IOM describes the capabilities, capacity, systems, processes and standards required by all policing, law enforcement agencies and partners to ensure that the total threat from SOC is identified, assessed, managed and coordinated effectively.

- 8.6. The capacity and contribution delivered by each force against the threat posed by SOC differs for each region, preferred partnership or multi-force collaboration. Their functionality should have a capacity and capability commensurate to the threat presented by SOC.
- 8.7. Forces should have, or have access to, assets to aid their response to the threat posed by organised crime. Forces need to demonstrate that they have a multi-agency intelligence capacity which feeds into the regional and national model perspective.
- 8.8. Cambridgeshire either have, or have access to the necessary range of specialist functions and capabilities to deliver against the commitments of this area.

9. Counter Terrorism

- 9.1. Counter terrorism (CT) policing contributes to the management of threat and risk from terrorism across all four workstreams of the government's CT strategy (CONTEST). The key objectives for the police and partners relate to the four themes of; Pursue, Prevent, Protect, Prepare.
- 9.2. The CT network is intrinsically linked to local policing. While not always the seat of operational activity, command and control is positioned within lead forces, whereas tasking and co-ordination is delivered nationally via the ACPO Counter Terrorism Coordination Centre (ACTCC).
- 9.3. The Police Counter Terrorism Network provides a local, regional and national structure to ensure that the Police Service has the capacity to meet the threats identified.
- 9.4. National strategy and policy is delivered through the ACPO Business Area for Terrorism and Allied Matters (ACPO TAM). Specialist regional units link policing at a national and local level.
- 9.5. At a local level, CT/DE intelligence and response are delivered through Special Branch and Local Policing.
- 9.6. Locally, forces must ensure that they can provide sufficiently trained CBRN, officers to meet the national requirement together with search officers and security coordinators, on a proportionate basis and according to local assessments.
- 9.7. Locally, Cambridgeshire are able to evidence a commitment to meeting the responsibilities within the area of CT through the collaborated CT/DE Unit which manages the specialist officers while also providing access to collaborated

resources across three forces. In addition, delivery of the Contest strategy is managed through bespoke delivery plans at a local level.

10. Large Scale Cyber Incidents

- 10.1. Cyber security is defined as one of four top priorities for UK national security. The term 'cyber attack' covers anything from small-scale email scams to sophisticated large-scale attacks driven by diverse political and economic motives.
- 10.2. The National Security Risk Assessment identifies a large-scale cyber incident and the risk of a hostile cyber attack by other states as Tier 1 risks. It is important to note that a cyber incident may not necessarily result from a criminal attack but could be caused by a technological issue or failure.
- 10.3. The ACPO National e-Crime Programme (NeCP) delivers the police response to the National Cyber Security Programme and through the Police Central E-Crime Unit (PCeU), assist forces in defining what is needed to provide a local, regional and national response to cyber crime, while also promoting standards for training and providing a centre for knowledge and best practice. The PCeU are due to merge with SOCA-cyber this year to form a new National Cyber Crime Unit within the National Crime Agency.
- 10.4. The national and regional network of CT policing units have a range of capabilities to address terrorist use of the internet. The role of CT policing regarding cyber-related threats is developing and has close links with the roles and capabilities of other national agencies.
- 10.5. The PCeU has established three regional hubs based in the North West, East Midlands, and Yorkshire and the Humber. The PCeU hubs are a national asset but regionally based. Their primary role is to deal with national cyber incidents but, where capacity allows, they will also deal with regional issues.
- 10.6. Local forces must have their own capacity for managing cyber crimes reported to them locally. In the event of a large-scale cyber incident, whether motivated by crime, terrorism or caused by a natural disaster, local forces may be asked to contribute specialist officers and staff to assist the PCeU.
- 10.7. A capability framework is currently under development by the portfolio lead in conjunction with the College of Policing. This sets out the arrangements a force needs to have, or have access to, in order to provide a local response to cyber crime. These include arrangements for governance, response, knowledge, security and collaboration.
- 10.8. As part of the national response, forces need to ensure they have, or have access to:

- a digital forensic capability
- a covert technical capability
- a lead SIO who is able to take on parts of an investigation involving a large-scale cyber incident.

10.9. Forces need to have governance and command structures for cyber crime investigations. They need to ensure that there are governance arrangements in place which link to regional and national structures. They should establish a command structure to deal with cyber-related incidents both within force and those requiring a cross-border response. Staff dealing with cyber crime need to be provided with appropriate training and continuous professional development. Suitable HR and financial management should exist to support work on cyber-related incidents.

10.10. This is a developing area of business within Cambridgeshire in line with the changing national structures and priorities.

10. Recommendation

10.1 The BCB is recommended to note the report.