Strategic Policing Requirement

Metropolitan Police Service

October 2014

ISBN: 978-1-78246-519-5

www.justiceinspectorates.gov.uk/hmic

Contents

Introduction

The *Strategic Policing Requirement* (SPR) was issued in July 2012.[1] This document sets out the Home Secretary's view of the national threats that the police must prepare for and the appropriate national policing capabilities that are required to counter those threats. The SPR respects the operational independence of the police service, advising what, in strategic terms, it needs to achieve, but not how it should achieve it.

The particular threats specified in Part A of the SPR, and referred to as the national threats in this report, are:

- terrorism;
- civil emergencies;
- organised crime;
- public order threats; and
- large-scale cyber incidents.

Part B specifies the policing response that is required nationally, in conjunction with other national agencies, to counter these threats. This policing response is described in the SPR as follows:

> *"the combined national **capacity** of all police forces to respond to these threats, expressed in terms of the outcomes sought – these are drawn, wherever possible, from publicly available national government strategies. Police and crime commissioners and chief constables must have regard to this aggregate capacity when considering the respective **contributions** they will make to it;*
>
> *the **capabilities** that police forces, often working collaboratively, need to maintain in order to achieve these outcomes; the requirement for **consistency** among forces for certain key specialist capabilities where the resources from more than one police force need to be integrated with, or work effectively alongside, each other. In some instances this requirement for consistency may need to involve other key emergency services and agencies; and*
>
> *the **connectivity** arrangements by which resources from several police forces may effectively be co-ordinated or mobilised, together and with those of other agencies – such as the Security Service and, from 2013, the National Crime Agency. The combination of consistency and*

[1] In accordance with section 37A Police Act 1996. Available from https://www.gov.uk/government/publications/strategic-policing-requirement

connectivity forms the basis for interoperability between police forces and with other partners."

We report the findings from this inspection of the Metropolitan Police Service (MPS) which took place during September 2013 against each of these requirements.

The breadth of requirements that are set out in the strategic policing requirement are outside the scope of a single inspection. Therefore, it has been necessary to plan a series of inspections over three years so that the police response to all the national threats can be examined individually and in-depth over that period.

This year, HMIC has examined how well police forces have established arrangements to respond to strategic policing requirement threats and has conducted in-depth examinations of the police response to two of the national threats: the threat to public order; and the threat of a large-scale cyber incident.

We have produced the following three national reports, available at www.hmic.gov.uk:

- The Strategic Policing Requirement: An inspection of the arrangements that police forces have in place to meet the requirement;
- The Strategic Policing Requirement: An inspection of how police forces in England and Wales deal with threats to public order; and
- The Strategic Policing Requirement: An inspection of how police forces in England and Wales deal with threats of a large-scale cyber incident (including criminal attack).

This report sets out what we found when we examined the arrangements that the MPS has in place to meet the strategic policing requirement and follows the format of the first of the national reports listed above.

Capacity and contribution

Terrorism

The force has the capacity to support all four strands of the government's counter-terrorism CONTEST[2] strategy.

Counter-terrorism policing in England and Wales is co-ordinated by the national counter-terrorism network, which is formed of dedicated counter-terrorism policing units providing functions such as the gathering of intelligence and evidence to help prevent, disrupt and prosecute terrorist activities. The MPS is responsible nationally for investigating crimes linked to terrorism, and an assistant commissioner from the force is the national lead police officer for counter-terrorism and allied matters and leads the counter-terrorism network.

The Commissioner of the MPS understands his role in tackling the threat of terrorism and the force has the capacity it needs to contribute to the national counter-terrorism effort.

A number of intelligence documents and briefings satisfactorily provide the force with ongoing assessments from which senior leaders are able to understand terrorism threats, risks and harm.

The force uses information which describes the terrorism threat to decide the allocation of funding to different counter-terrorism functions; what roles need to be established or retained and how many staff are required. These decisions are taken at fortnightly security review committee meetings, chaired by a commander.

The counter-terrorism command has 1700 staff and is the force's counter-terrorism network capability. Funding for the counter-terrorism command is provided by a government grant.

Civil emergencies

The MPS, together with the London Resilience Partnership, has the capacity to respond to civil emergencies locally and to contribute to national emergencies. The London Resilience Partnership is a coalition of organisations including the MPS, who have a role in preparing for, responding to and recovering from emergencies in London. The Partnership is made up of more than 170 organisations.

[2] CONTEST – the government's counter-terrorism strategy. The four strands are: pursue, prevent, protect and prepare.

The local resilience partnership assesses the hazards and threats to London, understanding their potential impacts and identifying the capabilities that are needed to deal with them.

The London Resilience team supports the work of the London Resilience Partnership by planning for, and co-ordinating responses to, emergencies requiring more than one organisation. Its responsibilities include the development of risk assessments. The MPS contribute staff to the London Resilience team and is also represented at 11 panels and six sub-groups that manage activity on behalf of the partnership.

The four police forces with a presence in London – the MPS, City of London Police, British Transport Police and the Ministry of Defence Police – have agreed how they commit resources to respond to incidents faced by either one of them under a protocol called 'Operation Benbow'.

The MPS has sufficient specialist skills required for dealing with civil emergencies. These include more than 1,200 officers trained to respond to chemical, biological, radioactive and nuclear incidents.

Organised crime

The force has prepared a strategic crime assessment of the threat, risk and harm related to organised crime. The assessment considers organised crime groups and their involvement in supplying firearms and drugs to gangs; supplying drugs to crime hotspots and handling property stolen by drug users; crime in town centres; and exploitation of young people.

The force applies the nationally-approved method to disrupt organised crime groups.[3] There is a task-allocation process known as 'One-Met tasking' which is co-ordinated centrally. This ensures appropriate measures are taken against organised crime groups in accordance with the force's assessment of the potential threats, risks, harm and demands that they pose.

Senior leaders are confident that the force's capability to tackle organised crime will continue to be effective in the current climate of austerity. The force has recognised that the London Regional Organised Crime Unit could be further developed with greater collaboration with the City of London Police and the British Transport Police.

[3] The UK law enforcement approach to tackling serious organised crime is based upon the identification of organised crime groups, assessment of the harm posed by them and management by disruption, investigation and prosecution.

Public order

The Commissioner understands his role to provide police support units[4] to deal with public order incidents across force boundaries and to make a contribution to the national requirement.

The force maintains a comprehensive public order risk register, which outlines risks linked to training equipment and policy, football, and emergency planning. This document was updated regularly with entries that recorded action to manage, mitigate or minimise risks. MPS staff recognised the need to develop public order strategic threat and risk assessments, in the format set out in national guidance.

Two committees, one of which is tactical and the other strategic, co-ordinate the provision of the force's public order capability. The Public Order Strategic Committee informs, advises and assists the force's senior leader responsible for public order to make sure that public order operations, training, policy and resources are appropriately supported.

The Public Order Advisory Committee reviews information about changes and proposed changes to public order policy, procedures and capability. For example, the specification for personal protective equipment, public order vehicles and public order training. A regional public order committee, chaired by an assistant commissioner, provides strategic co-ordination for London's public order capability. This includes representation from the City of London Police and the British Transport Police. The chair of the regional public order committee represents the London region on national police public order committees.

For each force, HMIC compared the number of police support units they declared they had, with the number of police support units that they told us they needed to respond to local outbreaks of disorder. The force assessed that it needed 75 police support units to respond to local threats and could provide 100 police support units. The force can also provide the 24 police support units that is has assessed it requires to contribute towards national mobilisation and has sufficient specialist public order staff[5] and senior officers to command responses to public order incidents.

---

[4] Police Support Units are the basic formations used by the police service for the policing of major events. The composition of a police support unit is standardised across all of the 43 police forces in England and Wales and consists of one inspector, three sergeants and 18 police constables, plus three drivers trained and equipped to carry out public order tactics to national standards, with three suitably equipped personnel carriers. Formations of a sergeant and six constables are referred to as serials.

[5] In addition to public order trained police officers, forces have specialists who are trained in a number of capabilities. These include liaison with protestors to facilitate peaceful protest and the removal of uncooperative protestors causing obstructions.

The use of mutual aid – the provision of support between police forces – is another indicator of the extent to which police forces either have or do not have sufficient trained public order resources. Data provided by forces on their provision and receipt of mutual aid for 2011/12 and 2012/13 show that the MPS was one of 31 forces that were net providers of public order policing mutual aid.

Large-scale cyber incident

The capacity of the force to respond to the threat of a large-scale cyber incident was in transition. National arrangements were changing with lead responsibility for tackling cybercrime moving from the force to the National Crime Agency.

Following the transfer of lead responsibility for this area of business, the MPS developed FALCON (Fraud and Linked Crime On-line), a unit of dedicated Cyber / Fraud investigators to investigate volume fraud and acquisitive cyber crimes. Phase 1& 2 of the implementation will be complete by the end of 2014. This will increase the number of officers and staff focused on this area of work to 392.

FALCON will:

- Build four FALCON hubs with dedicated Cyber / Fraud investigators to investigate volume fraud and acquisitive cyber crimes. Removing responsibility from Boroughs and addressing current MPS unsatisfactory detection rates;
- Create an industry task force to proactively target cyber criminals and fraudsters;
- Improve victim care and work with National Fraud Intelligence Bureau and Action Fraud to ensure referrals are effectively responded to, encouraging businesses to work with us and report crimes and share intelligence;
- Merge complex Fraud and Cyber Crime units and focus on stemming the harm caused by the most prolific Organised Crime Groups and;
- Undertake targeted prevention work with industry partners that designs out crime, tackles the enablers of cyber crime & fraud and raises the awareness within the public and businesses.

The MPS are doubling the number of staff tackling complex and serious cyber crime including denials of service and malware attacks.

The directorate of information is responsible for developing business continuity plans for the technology infrastructure and information and technology systems. All of the major systems have business continuity plans[6]. The force has a target to review 75 percent of its business plans and test them annually but the latest figures demonstrated only 43 percent compliance.

[6] Business continuity plans set out how the force will operate following an incident and how it expects to return to business as usual in the quickest possible time afterwards.

Capability

Terrorism

The MPS has the necessary capability to conduct complex investigations into terrorism. It has the systems in place to manage the training of counter-terrorism officers to maintain the necessary skills to provide specific counter-terrorism capability.

The counter-terrorism command has a comprehensive capability to undertake complex investigations, respond to critical incidents (including command and control) and provide specialist equipment and training to national standards.

Staff from the counter-terrorism command, work within local boroughs to provide effective links between front-line staff and the counter-terrorism network. Their responsibilities include the provision of briefings about counter-terrorism and domestic extremism and passing intelligence to the counter-terrorism command. The deployment of staff within local policing units supports all four strands of the government's counter-terrorism CONTEST strategy and particularly 'pursue' and 'prevent'.

The counter-terrorism command leads national police counter-terrorism daily meetings. Representatives of the national counter-terrorism network dial in to daily meetings, discuss continuing intelligence about counter-terrorism threats and agree how they will be dealt with. The force also contributes to weekly task-allocation meetings where intelligence is shared between the Security Service and the police. This meeting also reaches agreements about the use of police counter-terrorism resources. Counter-terrorism staff also contribute to the force tasking process.

The force has a comprehensive capability to train and accredit counter-terrorism staff to fulfil their roles and the MPS has access to sufficient trained staff to support all four strands of the counter-terrorism CONTEST strategy.

Civil emergencies

The force has the capability to deal with civil emergencies including those that span the borders with surrounding forces.

The London Resilience team provide a 24/7 liaison point for central government, other local resilience forums in the United Kingdom and bodies performing similar roles overseas. The MPS has staff in that team. As part of its responsibilities, the London Resilience team takes action as agreed by local resilience partners and manages effective sharing of information between them. The team uses a range of information to record events and action in their community risk register.

The MPS together with local resilience partners regularly practice multi-agency responses to major events and have conducted a number of tests.

There is a dedicated unit available to respond to chemical, biological, radioactive and nuclear incidents and sufficient numbers of trained staff within the force. Training records are maintained that enable force leaders to know who can be deployed to respond to these incidents.

MPS officers have, in the previous year, dealt with an incident involving chemical, biological, radioactive and nuclear risks and the force has reviewed the effectiveness of its response.

Senior MPS leaders are also contributing to a Home Office review of the capability of forces to deal with chemical, biological, radioactive and nuclear incidents.

Organised crime

The MPS has the capability to meet the threats from serious organised crime.

The force analyses the capability of organised crime groups' and the numbers and severity of crimes that they are believed to be committing, to decide on priorities. The analysis takes into account information from a range of organisations, including the Mayor's Office for Policing and Crime, other partner organisations and business groups. The tasking process uses the analysis to assist the allocation of resources. This helps to ensure that resources are deployed against the organised crime groups posing the greatest levels of threat, risk and harm.

The MPS monitor their effectiveness in dealing with the seizures of criminal assets, numbers of people stabbed and firearms discharges. This information is used by the force to decide upon resources and also informs their tasking process. Senior leaders also use performance information to move resources to meet longer-term crime threats, for example, adjustments were made to provide resources for tackling child exploitation and crimes committed by gangs.

Public order

The MPS has the capabilities required to respond to public order threats.

Staff are trained in accordance with national standards, including the use of tactics to end incidents of disorder before they escalate. The MPS has a specialist facility to train its officers in public order skills, including the command of public order incidents. The force has trained a significantly larger number of staff for public order than is required to meet its assessment of local threat, or to meet national mobilisation requirements. Senior leaders state that these numbers of staff provide the force with resilience.

Records of officers' public order training are maintained locally, and the public order command record numbers of trained officers within each policing area.

The force has recognised the potential to improve its capability to use intelligence linked to public order. Staff are employed within the force intelligence bureau, which is the central unit which is responsible for intelligence management for the organisation, to identify and manage public order intelligence.

Improvements have been made to the monitoring of social media in response to events such as the 2011 disorders where people used it to communicate where disorder was taking place. The force is investing in software to improve this capability. During heightened tension resulting from serious incidents, the force has undertaken 24-hour monitoring to enable it to anticipate potential disorder and respond if necessary. The force has the capability to provide current intelligence to operational leaders during the policing of major public order events. This enables them to use up-to-date information to plan tactics and deploy resources.

The force makes effective use of preventive measures to stop disorder taking place by taking action in advance of planned events. These include arresting people suspected to be conspiring to commit crimes connected to those events and using legislation to seek the prohibition of public processions that are likely to result in serious public disorder.

The force has introduced new debriefing arrangements using an electronic system, which will collect information from police officers before they go off duty. The method will also include contributions from the force's legal services. There are plans for lessons learned from the new way of debriefing to be used to train staff.

The force has tested its mobilisation plans four times over a twelve-month period. These were both paper-based tests and live mobilisation tests that were undertaken without prior notice. The live mobilisation tests demonstrated that the force could mobilise more than the nine police support units within the timescale expected by the national mobilisation plan.

HMIC tested, without notice, the force's capability to mobilise and conduct mutual support across boundaries to outbreaks of public disorder. The MPS control room staff demonstrated effective ways of responding to the scenario given in the test.

The force demonstrated that it could mobilise six fully-equipped police support units within 30 minutes. Information is available from the computer-aided despatch system about the availability of territorial support units that would provide this response. Control room staff were aware of the process for local mobilisation and of the protocol used for regional mobilisation. They had access to information about the availability of senior leaders and specialists who could

be called upon to assist. The computer-aided despatch system also included contingency plans that could be used to plan the police response.

A police support unit personnel carrier was seen by the inspection team and found to be fully functioning and equipped to national standards.

Large-scale cyber incident

The MPS has the capabilities required to respond to large-scale cyber incidents.

The force recognises that a large-scale cyber incident is a significant risk and has had a capability to respond to the threat since 2008. A senior leader has been appointed to be responsible for the force's response to any such threat.

The police central e-crime unit had some capability to deal with malware attacks[7] against online banking, system intrusion, distributed denial of service attacks and destructive computer hacking. To deal with these threats, the unit had enforcement, technical, intelligence and investigative capabilities. There are a number of examples when the unit demonstrated its capabilities, identified sources of attack on large organisations, then isolated and protected their systems.

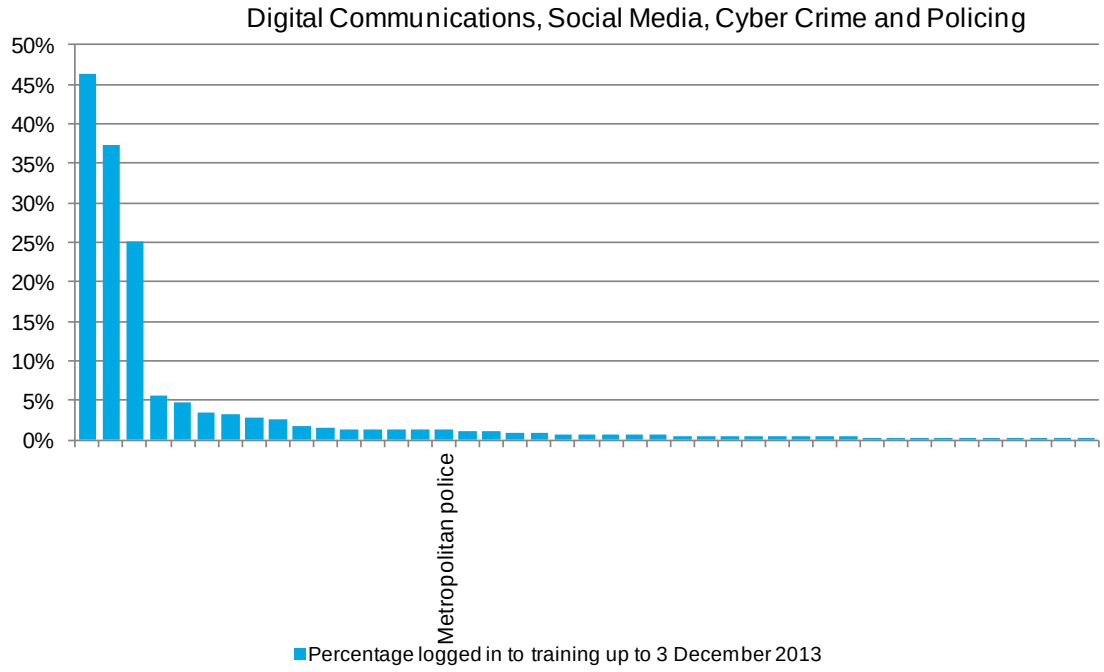
With the transition in national arrangements, a significant proportion of the police central e-crime unit's capability has moved to the National Cyber Crime Unit. Police central e-crime unit leaders have identified that they now need to train additional forensic analysts to fill the shortfall left following the transition.

The College of Policing has developed eight computer-based training courses to improve the police service's knowledge and to deal with cybercrime. Data has been provided and analysed to understand the proportion of the workforce who have sought the training up to the beginning of December 2013[8]. Tables that show the proportion of staff, for each force, that have started the training are included in our national report on the police service's response to cyber threats. The following charts demonstrate how many of the workforce enrolled for three of the eight e-learning courses designed to improve awareness. The courses were selected to be representative of the force's commitment to this aim for both general front-line policing (Digital Communications, Social Media, Cyber Crime and Policing introduced in April 2013 and Cyber Crime and Digital Policing – Introduction, introduced in August 2013) and for investigators (Introduction to Communications Data and Cybercrime introduced in July 2011).

[7] A computer program designed specifically to damage or disrupt a computer, mobile device, computer systems or computer network and can include programs designed to gain unauthorised access to data held on these devices.

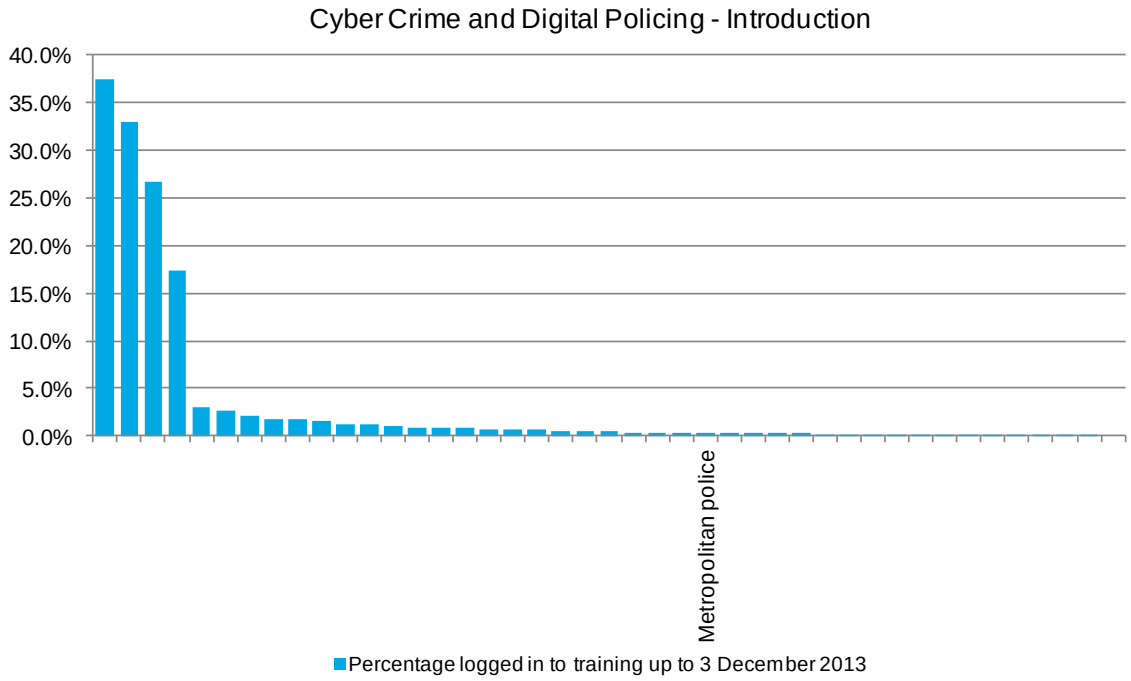
[8] Information provided by the College of Policing dated 10 February 2014 – completion figures for communication data and cyber crime modules (period ending 31 January 2014).

Figure 1: Digital Communications, Social Media, Cyber Crime and Policing[9]



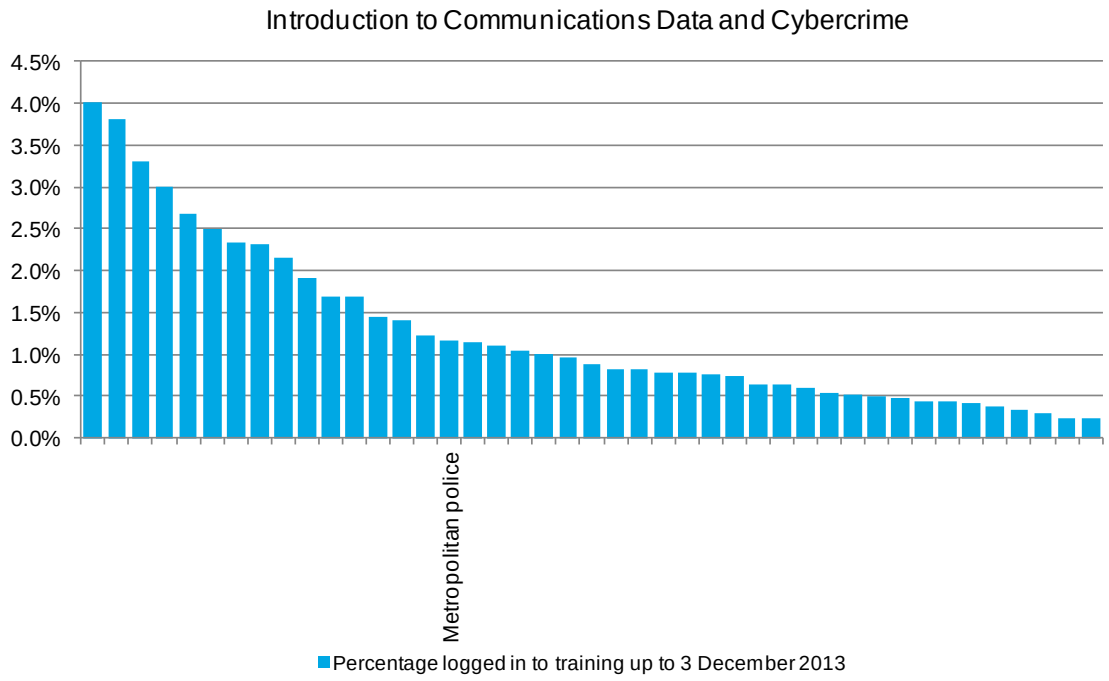
[9] This course, designed for all staff, aims to develop awareness of digital communications technology and its impact on different areas of cyber crime, social media, law enforcement and policing.

Figure 2: Cyber Crime and Digital Policing – Introduction[10]



[10] This course is designed for all police officers, special constables and other individuals in a law enforcement community. It is aimed at helping them develop a general awareness of the types of emerging threats and risks from criminals exploiting technology. The training is linked to relevant legislation and also covers cybercrime prevention.

Figure 3: Introduction to Communication Data and Cybercrime[11]



[11] This course is aimed at investigators and demonstrates the skills needed for a basic level of understanding of the uses of communications data within law enforcement including guidance on cybercrime prevention.

Consistency

Public order

Arrangements to train public order officers and procure public order equipment within the MPS are consistent with national standards.

The MPS purchases public order protective equipment in accordance with national standards and uses some contracts that have been agreed nationally for the procurement of equipment.

The force's police support units have been deployed, on numerous occasions, with those from other forces. Force senior leaders are confident that, their officers worked well with other forces' units. They identified differences in the types of shields used by forces outside London as the cause of some difficulties in interoperability.

The force has identified some differences in the training of public order commanders and how they fulfil their responsibilities. These differences include the way that leadership of overall tactical responses is organised. The MPS uses one overall tactical commander for each event. Some other forces use more than one to perform the same role.

The force trains senior police officers to command the policing of public order events at three levels – strategic command; leading the overall tactical response; and commanding the policing of geographic areas or specialist capabilities. Public order commanders are provided with training and development to become competent at all three levels. The national lead police officer with responsibility for public order policing and the College of Policing are reviewing the way that the force develops its public order commanders.

Officers from police forces outside London attend training at the MPS public order training centre. Exercises at the end of the training provide opportunities for MPS police support units and ground commanders to work with those from outside London.

Responding to chemical, biological, radioactive and nuclear incidents

The MPS is able to operate effectively, together with other emergency services, to respond to chemical, biological, radioactive and nuclear incidents.

Specifications for equipment used to respond to chemical, biological, radioactive and nuclear incidents are mandated nationally and the MPS uses the national procurement framework. MPS officers receive nationally agreed training for responding to incidents. This makes sure that practices used by the force are consistent with other police forces and emergency services. The

Home Office is currently reviewing specifications for police chemical, biological, radioactive and nuclear equipment and the force's senior leaders are contributing to this review. This review has led recently to the issue of an initial operational response, which has to be implemented across England and Wales.

Connectivity

Terrorism

The force has effective ways to co-ordinate and mobilise resources to deal with incidents of terrorism. These are supported by secure IT and radio communications.

The MPS counter-terrorism command has a full range of technical capabilities for the pro-active investigation of terrorist crimes. In cases where there is a need to co-ordinate large numbers of resources for investigations against groups posing high levels of threat, there is a plan for using the force's central communications centre. The force has sufficient trained staff to co-ordinate investigations across boundaries with other forces.

The force is capable of sharing information securely with the security and intelligence services, government agencies and other police forces. There is effective communication using the Airwave radio system.

The force has daily counter-terrorism management meetings where information about counter-terrorism and domestic extremism activity is discussed and measures are agreed to deal with them. There is also an effective weekly task-allocation meeting that co-ordinates the use of police resources to support the objectives of the Security Service and counter-terrorism network.

Civil emergencies

The MPS is able to communicate with other local resilience partners in the planning of the response to civil emergencies.

The force has strong links with other category 1 responders[12] across London. Staff from the fire and rescue and ambulance service attend training at the MPS public order training centre to work with police officers where there is public disorder. Ambulance and fire and rescue service staff can also communicate with the police using the same radio channels.

There are facilities for ambulance and fire and rescue services to work within the force's control room. The force can also open a strategic co-ordination centre, within which strategic leaders can work together. This facility is supported by an extensive technology infrastructure including a joint computer system to record actions and decisions.

[12] Category 1 responders are described by the Cabinet Office as organisations at the core of the response to most emergencies (the emergency services, local authorities, National Health Service) defined by the Civil Contingencies Act 2004) – www.gov.uk.

The local resilience partnership has undertaken two theoretical exercises for strategic commanders from each of the main member agencies. Scenarios have been based upon assessments of threats that the forum is facing, for example, flooding.

Reviews of these exercises have identified improvements that could be made in the co-ordination of responses including the force notifying others earlier of incidents that may affect their responsibilities. The force special operations room co-ordinates the initial response to incidents and deals with crisis management. It can be activated quickly, but the strategic co-ordination centre is not activated as quickly to manage the longer-term consequences arising from incidents.

The force is involved in the joint emergency services interoperability programme that is aimed at improving the way that emergency services work together across the country. There are still questions that need to be resolved about the role that the force will play, what training is provided to whom and timescales. These discussions are continuing but the force assesses that the programme will need to train 600-700 people.

Organised crime

The force communicates effectively with other police forces about the mobilisation of resources, sharing of equipment and tactics, and communication with other partners. Also, it is participating actively in the national tasking arrangements.

The force has an effective way to prioritise organised crime issues that require operational activity, the allocation of tasks to officers and the co-ordination of activity with the National Crime Agency. There are a number of forums within which senior leaders from different law enforcement agencies meet and discuss potential overlaps in activity. These have been used to discuss and agree strategies between the different organisations. There was evidence that resources are prioritised to deal with the most serious organised crime groups.

The force has a full range of technical capabilities to tackle those involved in organised crime. A central communications centre, with sufficient trained staff, is used to co-ordinate cross-border proactive operations. The force can also share intelligence securely with other forces and the National Crime Agency.

Public order

The MPS co-operate with the national arrangements for cross-border mobilisation of officers to deal with public order incidents.

The MPS has a dedicated unit that deals with the planning and provision of resources for public order events. This unit is effective and co-operates with the National Police Coordination Centre in fulfilling its national mobilisation

responsibilities. The force has a mobilisation plan, which is regularly tested and exercised and has proven effective on a number of occasions.

Cyber connectivity

The police central e-crime unit dealt with a number of large-scale cyber incidents within London and other force areas. Arrangements for the provision of cross-border support to forces were still being developed following the transition of responsibility to the National Cyber Crime Unit.

With the transfer of responsibilities to the National Cyber Crime Unit, there is a need for agreement about what is dealt with by each organisation. Acceptance criteria for cases that would be investigated by the Met e-crime unit have been written and shared with the National Cyber Crime Unit.

Staff in the National Cyber Crime Unit staff have access to MPS IT. MPS staff also work within the national unit. There is effective sharing of information between the force and the National Cyber Crime Unit.