Inspecting policing
in the **public interest**

The Strategic Policing Requirement

An inspection of the arrangements that police forces have in place to meet the Strategic Policing Requirement

ISBN: 978-1-78246-386-3

www.hmic.gov.uk

Contents

Glossary

ACPO	Association of Chief Police Officers
Action Fraud	the single point of reporting for fraud and financially-motivated internet crime
AEP	attenuating energy projectiles (often referred to as rubber bullets or baton rounds)
Airwave	the nationally connected, secure radio network used by the police and other emergency services
Association of Chief Police Officers	a professional association of police officers of Assistant Chief Constable rank and above, and their police staff equivalents, in England, Wales and Northern Ireland; leads and coordinates operational policing nationally; a company limited by guarantee and a statutory consultee; its President is a full-time post under the Police Reform Act 2002
authorised professional practice	professional practice that is authorised for use by the police in the course of their duties; APP is available in various subject areas that are relevant to the Strategic Policing Requirement
blue-light services	ambulance, fire and police services
bronze commander	a member of staff from one of the emergency services who controls an aspect of the incident response, implementing the silver commander's tactics
Capabilities	what forces are able to do to counter the Strategic Policing Requirement threats, often working collaboratively with other police forces and national agencies

capacity	the combined number of police assets and resources available to respond to SPR threats, expressed in terms of the outcomes sought, drawn from local, regional and national strategies
casualty bureau	temporary facility created during incidents involving large numbers of casualties; functions alongside disaster victim identification to assist in identifying casualties; manages enquiries from those anxious to learn whether specific people are amongst the casualties
CBRN	the threat of chemical, biological, radiological, or nuclear attack
CCA 2004	Civil Contingencies Act 2004
CERT-UK	the UK's national Computer Emergency Response Team, which works closely with industry, Government and academia to enhance UK cyber-resilience
Chief Constables' Council	Is the senior operational decision-making body for the Association of Chief Police Officers; brings together chief constables of police forces in the United Kingdom
chief officer	in police forces outside of London: assistant chief constable, deputy chief constable and chief constable; in the Metropolitan Police: commander, deputy assistant commissioner, assistant commissioner, deputy commissioner and commissioner; in the City of London Police: commander, assistant commissioner, commissioner
CII	an appropriately trained law enforcement officer, deployed on an authorised investigation who, via the internet, seeks to obtain information, intelligence or evidence against an individual, group of individuals or organisation

collaboration	activity where two or more parties work together to achieve a common goal, which includes activity between forces and with the public and private sectors, including contractors and business partners
College of Policing	the professional body for policing; its principal areas of responsibility include supporting police forces and other organisations to work together to protect the public and prevent crime.
commoditised information technology	Information technology where there is almost a total lack of meaningful difference between the hardware from different manufacturers
confidential unit	An organisational unit responsible for managing the sharing of protectively marked information
connectivity	the requirement for resources to be connected locally, between forces, and nationally; this should include being able to communicate securely, access relevant intelligence mechanisms and link effectively with national co-ordinating arrangements
consistency	the ability of the main specialist capabilities (whether in the police service or in other emergency services and agencies) to work together to ensure an effective response to the SPR threats
contribution	what forces supply to the national capacity which is aggregated to meet the national threats
control room	force facility that receives and manages emergency and non-emergency calls and manages the deployment of officers

CT	counter-terrorism
CTU	Counter-terrorism unit
Cyber	a term used to indicate that a computer is involved
Cybercrime	crime that involves the use of a computer
decontamination	to make (an object or area) safe for unprotected personnel by removing, neutralizing or destroying any harmful substance
DVI	disaster victim identification; a function carried out by trained personnel in incidents involving a large numbers of casualties
economies of scale	advantages that larger organisations have on cost because of their size; cost per unit decreases as the fixed costs are spread out over more units
ESMCP	Emergency Services Mobile Communication Programme, which will replace the Airwave system from 2016
fieldwork	inspection carried out within police forces at their premises or in their areas
front line	members of police forces who are in everyday contact with the public and who directly intervene to keep people safe and to enforce the law
go-forward tactics	tactics used by the police in public order situations that go beyond the containment of disorder; they allow the police to take positive action to end incidents of disorder before they escalate; tactics include advancing to disperse crowds, making arrests and using attenuating energy projectiles (AEPs)

gold commander	the person in overall charge of an incident; not usually at the scene but in a control room known as gold command, where they will develop an appropriate strategy for the emergency services to adopt when dealing with the incident
Government security classifications	Introduced in April 2014 to classify information assets to: ensure they are appropriately protected; support public sector business and the effective exploitation of information; and meet the requirements of relevant legislation and international / bilateral agreements and obligations. It applies to all information that government collects, stores, processes, generates or shares to deliver services and conduct business, including information received from or exchanged with external partners
industry standard	an established standard, norm, or requirement in a particular area of business
Interoperability	the ability of one force's systems and procedures to work with those of another force or forces
GAIN	Government Agency Intelligence Network: a network of police, national law enforcement agencies and other agencies such as Trading Standards and the Environment Agency that shares information about serious and organised crime
JESIP	Joint Emergency Services Interoperability Programme: a government initiative that aims to help the emergency services improve how they work together
LRFs	local resilience forums: partnerships made up of representatives from local public services, including the emergency services, local authorities, the NHS, the

	Environment Agency and others
Mercury	a computer system used by the National Policing Co-ordination Centre and police forces that assists in managing the mutual aid deployment of police resources across force geographic boundaries
mutual aid	provision of police officers or other assistance by one police force to another for the purpose of meeting any special demand, either on the application of the chief officer of the force receiving the assistance, or at the direction of the Home Secretary; the system was recommended by Desborough
National Fraud Intelligence Bureau	the National Fraud Intelligence Bureau identifies serial fraudsters, organised crime gangs and emerging and established crime threats by analysing millions of reports of fraud
National policing business areas	there are 11 national policing business areas, each led by a chief constable: uniformed operations, crime, terrorism and allied matters, criminal justice, equality, diversity and human rights, finance and resources, futures, information management, local policing and partnerships, performance management, and workforce development
national threats	the five threats referred to in Part A of the *Strategic Policing Requirement:* terrorism, civil emergencies, organised crime, public-order threats and large-scale cyber incidents
National Crime Agency	new agency established in 2013, responsible for tackling organised crime, border security, fraud and cybercrime, and protecting children and young people
NCCP	National Cyber Capabilities Programme

NCCU	National Cyber Crime Unit – part of the National Crime Agency
NPL	National Policing Lead – a police officer, usually a chief officer, who is responsible for developing policy and standards for defined areas of policing
NPoCC	National Police Co-ordination Centre
NPR	*National Policing Requirement*: issued by ACPO in 2012. It is a document that details the capacity and contribution, capability, consistency and connectivity required in response to the Strategic Policing Requirement
NRA	National Risk Assessment - a record, prepared by the Government, of the most significant emergencies that the UK could face. It also lists the most likely consequences of these emergencies, describing the maximum scale, duration and impact that could reasonably be expected
NRPA	National Resilience Planning Assumptions
NSRA	National Security Risk Assessment – a document that records the Government's assessment of the major risks faced by the UK. Risks are categorised according to tiers that indicate their priority in terms of criticality
organised crime	serious crime planned, coordinated and conducted by people working together on a continuing basis; their motivation is often, but not always, financial gain; includes drug trafficking, human trafficking, and organised illegal immigration, high value fraud and other financial crimes, counterfeiting, organised acquisitive crime and cybercrime; organised crime is characterised by violence or the threat of violence and by the use of bribery and

	corruption
organised criminal	a member of an organised crime group
Organised Crime Co-ordination Centre	a part of the National Crime Agency; co-ordinates law enforcement activity against organised crime groups
OCG	organised crime group: a group of people committing organised crime together
OSCT	Office for Security and Counter Terrorism in the Home Office
Part A threats	the five threats referred to in Part A of the Strategic Policing Requirement: terrorism, civil emergencies, organised crime, public order and large-scale cyber incidents; sometimes referred to as national threats
PCC	police and crime commissioner: statutory officer established under the Police Reform and Social Responsibility Act 2011, elected for a police area after the abolition of police authorities; the PCC is required to secure the maintenance of the police force for that area and its efficiency and effectiveness; he or she holds the chief constable to account for the performance of the force, and appoints and may, after due process, remove the chief constable from office
PND	Police National Database: a computer system to which police forces supply intelligence and information; PND enables intelligence held by different police forces to be linked
POA	Police Objective Analysis: a method of collecting data from police forces, used by the Chartered Institute of Public Finance

	and Accountancy in order to compile police workforce statistics
Police Professional Body	the body set up to increase professionalism in policing, now called the College of Policing
police regions	the nine police regions are: London, South East, South West, Wales, West Midlands, Eastern, East Midlands, North East, and North West
Procurement	the acquisition of goods, services or works from an external supplier
Professional Committee	a core part of the College of Policing's infrastructure; its members are the heads of national policing business areas and representatives from across policing, including PCCs
PSU	police support unit is a formation of resources for public order policing; the composition of a PSU is standardised across all of the 43 police forces in England and Wales and consists of: one inspector; three sergeants; eighteen constables; and three drivers; all trained and equipped to national standards with three suitably equipped personnel carrier vehicles
RICCs	regional information coordination centres: units in each police region that work with the National Police Co-ordination Centre to facilitate the mobilisation of police resources on mutual aid
ROCU	regional organised crime unit: there is a ROCU in each of the ACPO regions in England and Wales. In eight of the regions there is one region-wide ROCU. In the Northeast region the ROCU is split into two sub-regional units. ROCUs provide capability to investigate organised crime across police force boundaries.

Special Branch	police unit that deals with terrorism and domestic extremism threats; usually works closely with a CTU
silver commander	the person who takes the strategic direction from a gold commander and creates tactics that are implemented by bronze commanders
SIM	senior identification manager: senior officer trained to manage disaster victim identification processes
SPR	Strategic Policing Requirement
STRA	strategic threat and risk assessment: a process by which police forces analyse information about threats and risks against which they are required to commit resources

1. Preface

1.1. The breadth of requirements that are set out in the Strategic Policing Requirement (SPR)1 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 of the national threats can be examined individually and in-depth over that period.

1.2. This report is one of three reports about how forces comply with the SPR which is being published by Her Majesty's Inspectorate of Constabulary (HMIC) this year. It examines how well police forces have established the arrangements that the SPR requires them to have in place to counter a number of specified threats to national security and public safety.

1.3. Two further reports, due this year, will provide an in-depth examination of how well the police service has met the requirements of the SPR in relation to two of the national threat areas: public order and a large-scale cyber incident.

[1] *Strategic Policing Requirement,* HM Government, July 2012

2. Summary

2.1. The introduction of police and crime commissioners[2] (PCCs) across England and Wales represented a significant reform of the way in which the police are accountable to the public. PCCs are democratically elected individuals who set the policing priorities which chief constables[3] must have regard to. These new arrangements are part of the Government's programme to improve local accountability. The Government recognised, however, that there were some aspects of policing that required a national response, and that there was a need for a balance between localism and meeting national requirements.

2.2. As a result the *Strategic Policing Requirement* (SPR) was published in July 2012. 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.

2.3. 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.

[2] The term "police and crime commissioners" is used as shorthand so as to make reference to police and crime commissioners, the Mayor's Office for Policing and Crime in the Metropolitan Police District and the Common Council of the City of London.

[3] Reference in this document to a "chief constable" is intended to apply to every chief constable in England and Wales, the Commissioner of Police of the Metropolis, and the Commissioner of the City of London Police

2.4. Part B specifies the policing response that is required nationally, in conjunction with other national agencies, to counter these threats.[4] 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 connectivity forms the basis for interoperability between police forces and with other partners."*[5]

[4] *Strategic Policing Requirement,* HM Government, July 2012,SPR paragraph 1.6
[5] Op cit

HMIC's role and purpose

2.5. This report examines how well police forces have responded to these requirements since the SPR was published in July 2012. The SPR specifically directs HMIC to "provide assurance that the preparation and delivery [of SPR requirements] have been subject to a proportionate and risk-based testing and inspection regime".[6]

2.6. HMIC has no authority to inspect PCCs. Therefore, this report is focused on the duty of the chief constable, which is set down in the SPR in the following terms: "Chief constables must have regard to both the police and crime plan and the SPR when exercising their functions. Their police and crime commissioners will hold them to account for doing so." [7]

2.7. The meaning of 'have regard to' is explained in the SPR in the following terms: "It is not uncommon for legislation to require public bodies to 'have regard to' guidance, codes of practice or other material. The effect is that the police and crime commissioner and chief constable should follow the Strategic Policing Requirement unless they are satisfied that, in the particular circumstances, there are good reasons not to. It does not mean that either the police and crime commissioner or the chief constable has to follow the requirement blindly, but they should not depart from it without good reason (and should be prepared to be able to justify any departure from it on a case by case basis)."[8]

Methodology

2.8. In order to give proper consideration to the expectations set out in the SPR, HMIC is undertaking a series of inspections over the next three years to provide appropriate, in-depth, evidence-based review and analysis. This report is the first of a series of reports as to forces' responses to the SPR.

2.9. This first report is based on data and documentary evidence provided by all 43 police forces in England and Wales in July 2013. It includes supporting fieldwork, conducted in 18 forces, between September and November 2013

[6] SPR paragraph 1.15
[7] SPR paragraph 1.11
[8] SPR paragraph 1.9

and fieldwork conducted in nine Regional Organised Crime Units (ROCUs) during January and February 2014. It provides a broad outline of how police forces, individually and collectively, have responded to the SPR to date.

2.10. Two further reports to be published by HMIC this year will provide more detailed examinations of police force responses to the threats from public order and large-scale cyber incidents. HMIC will give more detailed consideration to the other national threats in the next three years.

2.11. The methodology used in this inspection is explained in more detail in the introduction to this report.

Findings: Capacity and contribution

Terrorism

2.12. There is a well-established national police counter-terrorism (CT) structure called the CT network, which consists of regionally-based units of dedicated staff that are funded by a Home Office grant, which is ring-fenced. We found that all forces worked constructively with the CT network to respond to the threat. We also found that the locally funded CT capacity (normally within force special branches) had been maintained in almost all the forces visited. There was a very small reduction in CT capacity which was a result of forces collaborating with each other to cut costs while maintaining capability.

2.13. However, we found that fewer than half of all 43 forces considered terrorism in their own assessments of local threats. This had an impact on their ability to make effective decisions about the capacity they should have in place to counter the threat of terrorism.

Civil emergencies

2.14. Usually a civil emergency will require a response by several ‘Category 1 responders’ as defined by the Civil Contingencies Act 2004. The planning for reacting to a civil emergency is undertaken by local resilience forums (LRFs). All the forces we visited demonstrated their commitment to working with partners and planning for civil emergencies. However, across all 43 forces,

only 16 submitted documents that demonstrated forces had any understanding of the threat, risk and harm. It was clear that most forces were not using a systematic understanding of risk and threat to decide on the capacity and contribution they should provide to meet their civil emergency obligations.

2.15. HMIC found that the very local nature of partnership organisations made it more difficult for police forces to collaborate with them to provide the full capability needed. As a result, there were very few examples of police forces collaborating on a joint response to civil emergencies. However, we did find some good examples of police forces working together to provide individual elements of the emergency response capability.

2.16. Police forces have sufficient capacity to respond to a chemical, biological, radiological or nuclear (CBRN) incident. The level of capacity to respond to this threat was defined nationally some years ago and has been centrally funded since then. However, the expensive specialist equipment required for a CBRN response is now reaching the end of its useful life. We found that forces were replacing equipment in different ways. A Home Office review of the police response to a CBRN incident was underway. This review had begun to provide information that forces needed to make decisions about their CBRN capacity and future requirements for new equipment.

Organised crime

2.17. This national threat covers a diverse range of criminal activity most of which is motivated by profit but there are exceptions such as child sexual exploitation. The police face challenges in developing a full understanding of the threat.

2.18. Nationally, law enforcement activity against organised crime groups (OCGs) is co-ordinated by the National Crime Agency (NCA) which was established in October 2013, part way through our fieldwork. OCGs are identified and assessed in terms of their level of intent, capability and criminality and this information is used to prioritise the law enforcement response.

2.19. Although most forces had considered organised crime in their local strategic threat and risk assessments (STRAs) or in some other form of assessment, four forces had not. Of those that had considered it, too many had STRAs that were not of sufficient quality to be used to make decisions on resources needed. This problem was compounded by the fact that too many forces were making judgments based on the personal experience of a small group of officers rather than on an objective assessment of threat, risk, harm and demand.

Public order

2.20. We found that chief constables understood their role to provide sufficient trained officers to respond to the national threat to public order. HMIC confirmed that they were meeting the national requirement of 297 Police Support Units (PSUs).

2.21. We also examined the level of capacity that forces had assessed as necessary to respond to a local threat. For each force, HMIC compared the number of PSUs they declared they had with the number of PSUs that they told us they needed to respond to local outbreaks of disorder. We found that in five forces, while they complied with the national requirement, they did not have enough PSUs to meet their assessments of the local threat. On the other hand, we found that 14 forces had numbers of trained PSUs at a level at least twice the number that they had assessed as necessary to meet their local threat.

2.22. Most forces, 38 of the 43, considered public order in their STRAs, although only 33 STRAs were sufficiently robust to inform force decisions about capacity. It is disappointing to find that there are a number of police forces that are either still not using the threat assessment process to its full effect or are not using it at all. Even if forces do assess threats, risks and harm, they do not always use the information to decide on what resources are needed.

Large-scale cyber incident

2.23. This is the newest of the national threats to require a national response by the police service. A large-scale cyber incident could be caused by either the aggregation of individual cybercrimes or the commission of a single attack. Therefore we believe that the police response should be concerned with both types of incident.

2.24. Digital technology and the internet are providing criminals with new opportunities to commit crime. This is either where criminals use computers to help them commit crimes that would have been committed previously without the benefit of such technology, for example fraud and theft, or where they commit new crimes that were not possible before, such as an attack on government online services using malicious software. These two categories of cybercrime are respectively known as cyber-enabled and cyber-dependent crimes.[9]

2.25. We expected to find police forces had sought to understand the threat and their role in tackling it. But HMIC found that only three forces (Derbyshire, Lincolnshire and West Midlands) had developed comprehensive cybercrime strategies or plans and only fifteen forces had considered cybercrime threats in their STRAs.

2.26. Senior leaders across police forces were unsure of what constituted a large-scale cyber incident. We found that, where they existed, STRAs and plans were focused only on investigating cybercrime; they were silent about preventing it and protecting people from the harm it causes. The publication of the new Serious and Organised Crime Strategy in October 2013 provides an opportunity for police forces to incorporate all four themes of 'pursue, prevent, protect and prepare'[10] in future plans and STRAs.

2.27. The Government and PCCs are increasing their investment in ROCUs to establish fully the range of capabilities that are necessary to support police

[9] *Serious and Organised Crime Strategy*, October 2013, HM Government, Cmnd 8715, paragraph 2.54

[10] The serious and organised crime strategy uses the same framework as the Government's counter-terrorism strategy, comprised of four themes: prosecuting and disrupting people engaged in serious and organised crime (Pursue); preventing people from engaging in this activity (Prevent); increasing protection against serious and organised crime (Protect); and reducing the impact of this criminality where it takes place (Prepare)

forces. However, at the time of our inspection, we found that most ROCUs had not yet developed the necessary cyber capability to assist police forces. We also found that police forces' capacity and contribution was limited to the deployment of a small number of specialist investigators.

2.28. The fact that forces are not yet able to demonstrate that they understand their roles in tackling this threat of a large-scale cyber incident is fully understood as a problem by the police, the Home Office and the NCA. We found evidence that across these bodies, and wider partners, work is underway to help provide the clarity that is needed for police forces and PCCs about their roles and the capacity and capability they need to put in place to respond to the threat effectively.

Findings: Capability

Terrorism

2.29. The arrangements for countering terrorism are well-developed and resourced, with a national CT network providing the majority of the capacity and capability. Police forces provide sufficient capability to provide armed support to CT operations and gather, assess and report intelligence to inform national and local understanding of the CT threat. There are national standards for training officers in the skills required in CT policing; in all of the forces visited, we found evidence that forces were complying with these standards of training officers. HMIC's fieldwork in the 18 forces that we inspected revealed that police forces have sufficient officers trained to national standards who can deliver their contribution to the national response to terrorism.

Civil emergencies

2.30. The development of forces' capabilities to respond to civil emergencies is relatively mature. It pre-dates the publication of the SPR, particularly in the police involvement in LRFs. There is a training curriculum that covers specific roles, and the necessary training is provided by forces. There are national standards for certain aspects of specialist training, including disaster victim identification (DVI) and casualty bureau roles. HMIC considers that forces are

meeting the requirement of the SPR in providing the necessary capability to respond to cross-border civil emergencies.

Organised crime

2.31. The Government and the police service's approach to tackling organised crime in England and Wales involves maintaining capabilities in police forces and a network of ROCUs. In March 2013, the Home Office announced an increase in the level of financial support it provides to ROCUs in order to help them "*mature into the consistent and effective network that forces and the NCA will rely on as they work together to fight organised crime*".[11] The additional investment is to pay for an increase in ROCU capabilities, specifically in the areas of: intelligence collection and analysis, asset recovery, fraud, cybercrime, prison intelligence, and providing witness protection.[12] Forces in all regions agreed to match the additional Home Office investment. Home Office funding for ROCUs remains is allocated on an annual basis, which makes it difficult for forces to plan for the longer term.

2.32. HMIC visited each of the nine ROCUs to examine the rate of progress and levels of consistency between them. HMIC found that, in all regions except London, chief constables and PCCs had agreed their plans for ROCU development.

2.33. However, we also discovered that in five ROCUs, the underpinning legal agreements[13] between the contributing forces and PCCs were either in draft, under review, or not signed. This means that the ROCUs have not yet established themselves fully as a consistent and effective network. We saw strong evidence that ROCUs were making progress to create the capabilities required, but at the time of HMIC's visits to ROCUs, none of them had the full range of capabilities they need to collect and analyse intelligence in the most

[11] Letter from Home Secretary to Chief Constables and police and crime commissioners dated 12 March 2013
[12] *Serious and Organised Crime Strategy*, HM Government, October 2013, Cmnd 8715, paragraph 4.11
[13] section 22A Police Act 1996

effective way; five ROCUs had no fraud team and in three of the ROCUs there was no dedicated government agency intelligence network (GAIN) co-ordinator in post. These findings reflect the position at the time of our visits; progress is being made and HMIC has subsequently been informed that all ROCUs have now appointed fraud teams and GAIN co-ordinators.

2.34. We found that the training for the specialist roles required by police forces to tackle organised crime were well defined and, for some roles, standardised and accredited. However, there were still some areas of training which were not adequate. These were to provide accredited training for senior investigating officers to manage covert investigations of OCGs; and authorising officers for undercover operations.[14] The national policing crime business area lead had recognised these issues prior to the inspection and was dealing with them.

2.35. In summary, forces and ROCUs either have the capabilities required to tackle organised crime, or have plans to deliver them in the near future. The plans for ROCUs to have a standard set of capabilities are taking longer to implement than was intended; success will rely on PCCs in each region completing the formal legal agreements that are required.

Public order

2.36. All officers who carry out public order policing require specialist training to standards defined in the College of Policing curriculum. We found that forces had 769 PSUs trained to this standard in July 2013, which is sufficient to meet the national requirement of 297 PSUs.

2.37. Public order commanders must also be trained to nationally agreed standards and accredited as operationally competent. There is not a national requirement for the number of public order trained commanders in the same way as there is for PSUs – forces decide the number and level of commanders that they require. Our analysis of the data returned by forces

[14] Evidence obtained by HMIC's inspection of undercover policing, which reports in May 2014

indicated that sufficient levels of accredited public order trained commanders to provide cover during widespread disorder were not always in place. For example, three forces had only one trained and accredited gold commander. These forces were at risk of not having the necessary command capability should a public order incident occur. Also there was not a formal agreement in place as to how forces should request assistance from other forces.

2.38. There is a sound understanding of national capabilities to respond to public order threats and what needs to be done to develop and maintain this capability. This understanding was assisted by work commissioned by the national policing lead for public order and delivered by the College of Policing. This work asked forces to complete a self-assessment of their public order capability levels.

2.39. In the 18 forces we visited, we checked the public order equipment used in their PSUs and found that in all cases they had the necessary equipment. However, we found that different specifications meant that the equipment was not always compatible for use with equipment from other forces.

2.40. The National Policing Co-ordination Centre (NPoCC) was proving to be effective in co-ordinating national resources. It had sufficient information to understand what resources were available to deal with public order incidents and to mobilise resources to respond to threats. The NPoCC tests national mobilisation of resources through the co-ordination of regional mobilisation exercises against targets set in the Police National Public Order Mobilisation Plan. We found that the plan did not specify what the term 'mobilised' actually meant in practice and this led to forces interpreting what it meant differently. A revised plan clarifying the term 'mobilised' has been prepared but not yet issued to police forces. This raised doubt over how useful comparisons were between forces about how fast they are able to mobilise their resources. Our analysis of six national[15] mobilisation exercises co-ordinated by the NPoCC identified that in half of them, the National Public Order Mobilisation Plan target of ten percent of the national PSU requirement for mutual aid to be

[15] The six mobilisation exercises were conducted in the following police regions: London, Wales. South East, East, North East and North West

mobilised within one hour was not met. The reasons for not meeting the target were not provided in two of the three exercise debriefs completed by the forces.

2.41. Our unannounced visits to force control rooms to test in-force mobilisation showed significant failings. Only a third of the 18 forces visited could respond effectively to a test scenario that required them to identify and muster the required trained and equipped public order personnel. In the remainder, unacceptable delays were caused by the time it took to locate and contact the trained staff. This is not satisfactory – the police service must be able to respond swiftly to the requirement for national mobilisation.

Large-scale cyber incident

2.42. Research shows that cybercrime is significantly under-reported, and of those crimes reported to Action Fraud[16], only 20 percent are passed to police forces.[17] This means that police forces do not have sufficient information to identify and understand the threats, risks and harm associated with cybercrime.

2.43. It is now essential that police officers have the capability to deal confidently with the cyber element of crimes as it is fast becoming a dominant method in the perpetration of crime. But more than that, it is becoming a part of everything that the police have to deal with because the internet and digital technology are part of most peoples' lives now. For example, an officer dealing with a missing person might need to access their presence on the internet as part of his or her enquiries. The police must be able to operate very soon just as well in cyberspace as they do on the street.

2.44. During the past year, national police leaders have started to take steps to improve the skills of police forces' staff to deal with cyber threats. There is a

[16] Since April 2013, Action Fraud has received all reports of fraud and computer misuse offences from the public and businesses on behalf of police forces. These are screened for opportunities to investigate and also used in prevention and disruption activity.
[17] National Fraud Intelligence Bureau throughput statistics: 9 months to 31 December 2013.

new College of Policing framework on capability which forces can use to assess their progress in establishing resources, practices, processes and skills to tackle cybercrime; there are now eight e-learning packages designed to increase awareness and develop investigation skills. However, we found that the take-up of this training was disappointingly poor, with only a few forces demonstrating a real commitment to improve the skills of their staff to tackle cybercrime. The average take-up for this training in 37 forces was less than two percent of staff.

2.45. A National Cyber Capabilities Programme assessment of capabilities described low level of skills in the regions to deliver their remit and a very low level of capability in local forces. The assessment reported that, where a number of crime allegations are linked or where activity crosses several force boundaries, the ROCU Cyber Crime Units will co-ordinate investigations and provide expertise for local forces. Forces may also be required to support complex national or regional-level investigations. The capability to do this was not yet in place in forces during our inspection and most ROCUs did not yet have any cyber capability in place.

Findings: Consistency

2.46. The SPR describes consistency as:

> *"...the requirement for certain key specialist policing capabilities to be delivered in a consistent way across all police forces or, in some cases, with other partners such as other 'blue-light' emergency services or national agencies*." [18]
>
> "*Chief constables and police and crime commissioners must have regard to the need for consistency in the way that their forces specify, procure,*

[18] SPR Introduction to section 5

implement and operate in respect of the following policing functions [later referred to as the 'key functions']:

- *Public order;*
- *Police use of firearms;*
- *Surveillance;*
- *Technical surveillance; and*
- *Chemical, Biological, Radioactive and Nuclear (CBRN) incidents.*"[19]

"*These are the areas of policing in which the need for consistency (or as a basis for 'interoperability') has been adjudged to be the most critical, at this time, by the Association of Chief Police Officers. Consideration should also be given to developing functions such as cyber. This consistency should be reflected in common standards of operating and leadership disciplines, acknowledged by the Police Professional Body from 2013.*"[20]

2.47. The police professional body is now called the College of Policing and is the organisation that sets the standards of professional practice for the police. The primary way of doing this is through a body of what it calls 'consolidated guidance for policing' which is published in the form of Authorised Professional Practice (APP).

2.48. The College helps the police service bring about a consistent approach by: accrediting training providers; developing learning outcomes within a standardised national framework; and identifying and promoting good practice based on evidence of what is effective.

2.49. Due to the scale of the inspection undertaken this year it was not possible to examine all five of the 'key functions' listed above in this report. We examined how consistent forces were in responding to public order and CBRN. We will cover in detail the remaining 'key functions' in future reports in the SPR series.

[19] SPR paragraph 5.1
[20] SPR paragraph 5.2

Public order

2.50. HMIC found public order professional practice was consistent and generally good; it was strongest in regions where PSUs from different forces trained together. Except in a small number of forces, we found that officers were trained in and used the same public order tactics. The ability of forces to work together is improving as a result of joint training, carrying out exercises together and joint deployments. We were told by some officers that minor differences in training and practice between forces cause problems for joint working.

2.51. HMIC looked at procurement and how consistently this was carried out in all forces. HMIC found that the Home Office's regulatory framework did not take into account the procurement requirements in the SPR specifically. We interviewed procurement managers who considered that a consistent approach could only be achieved if forces agree a common specification; this agreement has so far proved difficult to secure. We found that some forces were trying to address this by creating regional groups that could help deliver greater consistency in procurement.

Chemical, biological, radiological and nuclear (CBRN) incidents

2.52. Nationally funded and procured equipment has enabled CBRN trained officers to be fully interoperable at a regional and national level. Some forces expressed concern that they were still waiting for central direction about how they should replace their equipment and whether the cost of the new equipment will be met from central or from force budgets. The current review by the Office for Security and Counter Terrorism should clarify the position on buying new equipment later this year.

Findings: Connectivity

2.53. The SPR requires forces to be able to work effectively together and with national agencies. It states that:

- *"In response to the threats from terrorism, cyber and organised crime, chief constables must have regard to the requirement for resources to be connected together locally, between forces, and nationally (including with national agencies) in order to deliver an integrated and comprehensive response. This should include the ability to communicate securely, access intelligence mechanisms relevant to the threat and link effectively with national co-ordinating mechanisms."*[21]

2.54. In this section we examine the requirements made concerning 'connectivity' in section 6 of the SPR.

"An integrated and comprehensive response."

2.55. We found evidence that there were effective arrangements for connecting forces' resources to tackle organised crime groups assessed as presenting the greatest threat and/or risk. There were clear links between forces' co-ordination of resources and those of ROCUs. We heard that arrangements were less effective when complicated organised criminality did not fit easily within force and regional geographic boundaries.

"To communicate securely"

2.56. The nationally connected, secure radio network used by the police and other emergency services, known as 'Airwave', provides effective connectivity in the majority of situations. However, interviewees did highlight that a high concentration of both users and radio traffic can challenge the network's capacity at times. There were some problems connecting resources between the emergency services caused by each organisation still operating under different working practices.

"Accessing intelligence mechanisms relevant to the threat"

[21] SPR paragraph 6.1

2.57. We found that forces used the Police National Database (PND), the national system designed to enable forces to share police intelligence, differently from each other; also it varied between forces how well they kept the intelligence on the database up to date.

2.58. Intelligence relevant to national threats is held by the police, the NCA and other national agencies on disparate IT systems. In addition, the IT systems used by the police for routine business such as command and control, crime recording, custody, intelligence and case preparation are not well-connected across the 43 forces. It remains difficult for investigators to connect all the valuable items of intelligence in these systems.

2.59. HMIC found that police forces are developing what they call 'confidential units' as part of a programme to increase ROCU capabilities.[22] These units, operating to particularly high standards of information security, will connect police force intelligence systems, the NCA systems and those of the counter-terrorism units. Plans are progressing well and the 'confidential units', once they are in place, will have the necessary infrastructure and security arrangements to enable them to handle such material and share it across units working at different Government Security Classifications (GSC) levels.

2.60. In conclusion, there is clear progress towards improved connectivity and there are signs that police forces and ROCUs will find it easier in the future to share sensitive intelligence. That said, the structures, systems and processes that were in place at the time of the inspection were not yet fully functioning to allow safe and effective intelligence-sharing.

"***Police co-ordination arrangements for countering terrorism.***"[23]

[22] *Serious and Organised Crime Strategy*, HM Government, October 2013, Cmnd 8715, paragraph 4.11

[23] SPR paragraph 6.2

2.61. HMIC found it was evident that there was connectivity within the CT network and between the network and forces.

"*Co-operation with tasking arrangements led by the National Crime Agency*."[24]

2.62. These arrangements involve a national tasking meeting that is chaired by the NCA and regional tasking meetings that are chaired by forces. HMIC found that forces were fully engaged in the national tasking arrangements which were led by the NCA. This was confirmed by NCA regional organised crime co-ordinators (senior NCA managers who work closely with ROCUs) and leaders in the ROCUs who we interviewed; they reported positive engagement by both sides and that this had led to good outcomes.

"Cross-boundary mobilisation"[25]

2.63. The problems faced by forces as they responded to the August 2011 disorder, using the structures in place at the time, led to the creation of the NPoCC. HMIC found that all forces were working with the NPoCC through a network of co-ordinators in regional units known as Regional Information Co-ordination Centres (RICCs). Interviewees in various roles across six of the 18 forces provided information that described a co-operative relationship with the NPoCC that led to effective mobilisation of resources at times of need.

2.64. The NPoCC also co-ordinates a programme of mobilisation exercises undertaken by police forces and regions. These exercises enable the Centre to understand the availability of resources and how quickly they can be deployed to respond to incidents. Overall we found that chief constables are co-operating with the arrangements for mobilising resources across force boundaries.

2.65. Our inspection has led us to conclude that HMIC can provide assurance that chief constables are having regard to the SPR "*when exercising their*

[24] SPR paragraph 6.3
[25] SPR paragraph 6.4

functions"[26]. We found that the levels of resources dedicated to the police response to the national threats have not changed appreciably following the publication of the SPR. The total number of posts that were dedicated to responding to the five national threats in England and Wales for 2013/14 was 11,265.

2.66. That said, the capacity and capability of the police to respond to the national threats is stronger in some areas than others – with the police response to the cyber threat being the least well developed. The lack of a clearly articulated approach to the SPR by the collective leadership of the police service in England and Wales was disappointing, especially some 18 months after its publication. During our inspection we found that the *National Policing Requirement* (NPR), which was written by the police to describe how forces should collectively respond to the SPR, was not being used as it was intended. Forces were uncertain about the NPR's currency and value and, as a result, we found very little evidence that it was being used to help them establish a collective and effective response to the national threats. Also, we could find no evidence that it had been subject to an annual review as promised in paragraph 1.3.3 of the NPR document.

2.67. Our findings lead us to conclude that chief constables need to immediately establish a collective leadership approach that is committed to securing the required level of preparedness to respond to the national threats - in a way that is consistent across England and Wales.

[26] SPR paragraph 1.11

Recommendations

1. Chief constables should, immediately, establish a collective leadership approach that is committed to securing the required level of preparedness to respond to the national threats - in a way that is consistent across England and Wales. This should be done by:

    - re-establishing their commitment to a National Policing Requirement that fully describes the response that chief constables are committed to providing to the tackle the national threats;

    - providing the capacity and capability necessary to contribute to the collective response by all forces to tackle the national threats;

    - monitoring how well forces are fulfilling their obligations to the National Policing Requirement and formally reporting the results to Chief Constables' Council - at least annually;

    - fulfilling their promise[27] to annually review the National Policing Requirement.

Capacity and contribution

2. Chief constables should conduct an evidence-based assessment of the national threats (as described in the SPR), at least annually, and make it part of their arrangements for producing their strategic threat and risk assessments. This should start immediately because it is essential to understand the threat and risks before deciding upon the level of resources that are necessary to respond.

3. Chief constables and PCCs should, as part of their annual resource planning, explicitly take into account their strategic threat and risk assessments when they make decisions about the capacity and capability required to contribute to the national response to those threats. This should start with immediate effect.

[27] *National Policing Requirement*, ACPO, 2012, paragraph 1.3.3

4. Chief constables should work with the College of Policing to create national guidance that describes how forces should establish the number of PSUs they need to respond to their assessment of the local public order threat. This should be completed within six months.

5. Chief constables should work with the Home Office, the National Crime Agency and CERT-UK (following its launch in March 2014) better to understand their roles in preparing for, and tackling the shared threat of a large-scale cyber incident. Their roles should cover the 'pursue, prevent, protect and prepare' themes of the Serious and Organised Crime Strategy.

6. Recognising the fact that both the understanding of the national threats and the police response to them are continually changing, the Home Office should regularly review the SPR to make sure its requirements remain relevant and effective.

Capability

7. The College of Policing should work with chief constables to establish and specify the capabilities necessary (in a capability framework) for forces to use to assess whether or not they have the required capabilities to respond to the threat of terrorism. This should be completed within a year.

8. Chief constables should regularly, at least every two years, complete the College of Policing's capability frameworks to help them assess whether or not they have the capabilities necessary to respond to the national threats.

9. Chief constables should work with the College of Policing to establish formal guidance to forces about how they should mobilise public order commanders between forces. This should be done within three months.

10. Chief constables should agree, and then use a definition that specifies exactly what the term 'mobilised' means in relation to the testing of the police response required by the Police National Public Order Mobilisation Plan. This should be done within three months.

11. Chief constables should provide those whose duty it is to call out public order trained staff with the information they need, 24 hours a day, seven days a week, so that they can mobilise the required number of PSUs within the timescales set out in the Police National Public Order Mobilisation Plan.

Consistency

12. Chief constables should work with the College of Policing to agree and adopt a standard specification for all equipment that is necessary for the police to be able to respond to the national threats.

13. Once standard specifications are in place, the Home Office should support national procurement arrangements and, if police forces do not adopt them, mandate their use through regulation.

Connectivity

14. Chief constables should demonstrate their commitment to the objectives of the Joint Emergency Services Interoperability Programme by, wherever practicable, aligning their operational procedures with the other emergency services.

15. Chief constables and the Director General of the NCA should prioritise the delivery of an integrated approach to sharing and using intelligence.

3. Introduction

3.1. This report sets out the findings of an inspection by Her Majesty's Inspectorate of Constabulary (HMIC),[28] which examined how well police forces have established the arrangements that the *Strategic Policing Requirement* (SPR) requires them to have in place so they can respond to a number of specified threats to national security and public safety (hereinafter called the 'national threats').

3.2. The introduction of police and crime commissioners[29] (PCCs) across England and Wales represented a significant reform of the way in which the police are accountable to the public. PCCs are democratically elected individuals who set the policing priorities which chief constables must have regard to. These new arrangements are part of the Government's programme to improve local accountability. The Government recognised, however, that there were some aspects of policing that required a national response, and that there was a need for a balance between localism and meeting national requirements.

3.3. As a result the *Strategic Policing Requirement* (SPR) was published in July 2012.[30] 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.

[28] Her Majesty's Inspectorate of Constabulary (HMIC) is an independent inspectorate. It has a legal responsibility under section 54 of the Police Act 1996 to inspect forces in England and Wales, and to report on their efficiency and effectiveness.

[29] The term "police and crime commissioners" is used as shorthand so as to make reference to police and crime commissioners, the Mayor's Office for Policing and Crime in the Metropolitan Police District and the Common Council of the City of London. Reference in this document to a "chief constable" is intended to apply to every chief constable in England and Wales, the Commissioner of Police of the Metropolis, and the Commissioner of the City of London Police

[30] Issued pursuant to section 37A Police Act 1996

3.4. Part A of the SPR specifies those threats to national security and safety that either affect multiple police force areas, or may require resources to be brought together from multiple police force areas. The SPR acknowledges that many of these threats overlap, but for the sake of clarity the SPR presents them separately as:

- *"terrorism, which the National Security Risk Assessment [31] identifies as a Tier One risk;*
- *other civil emergencies that are defined as a Tier One risk in the National Security Risk Assessment and require an aggregated response across police force boundaries;*
- *organised crime, which the National Security Risk Assessment identifies as a Tier Two risk. The UK threat assessment of organised crime identifies that offending is mostly motivated by financial profit, but there are exceptions, such as child sexual exploitation. Large scale cybercrime, border security, and economic crime may have an organised crime dimension;*
- *threats to public order or public safety that cannot be managed by a single police force acting alone;*
- *a large-scale cyber incident, which the National Security Risk Assessment identifies as a Tier One risk (together with the risk of a hostile attack upon cyberspace by other states). The crime threat at the national level may be a major incident, such as a criminal attack on a financial institution to gather data or money, or it may be an aggregated threat, where many people or businesses across the UK are targeted. It includes the response to a failure of technology on which communities* depend and which may also be considered a civil emergency."[32]

[31] The *National Security Risk Assessment* is a classified document produced by the Cabinet Office. It is partly reproduced in the *National Security Strategy* (https://www.gov.uk/government/uploads/.../national-security-strategy.pdf) and the *National Risk Assessment* (https://www.gov.uk/risk-assessment-how-the-risk-of-emergencies-in-the-uk-is-assessed).

[32] SPR paragraph 2.2

3.5. For the purposes of this inspection, HMIC considers 'threat' to mean: the likelihood of an incident occurring that involves terrorism, organised crime, public disorder, civil emergency or large-scale cybercrime. 'Risk' refers to how factors such as population density in relation to crime and terrorism, or houses on flood plains in relation to the likelihood of civil emergencies, would alter the threat. The SPR also refers to 'harm', which HMIC takes to mean the impact of a crime or event, for example, injury, damage or fear among the public.[33]

3.6. Part B specifies the policing response that is required nationally, in concert with other national agencies, to counter these threats.[34] This policing response is described in the SPR in the following terms:

- "*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*

[33] These are definitions created by HMIC solely for the purposes of this report. Different definitions exist elsewhere.
[34] SPR paragraph 1.6

connectivity forms the basis for interoperability between police forces and with other partners."[35]

3.7. This report examines how well police forces have responded to these requirements since the SPR was published in July 2012. Our inspection responds directly to the expectation contained within the SPR that, "Her Majesty's Inspectorate of Constabulary will provide assurance that the preparation and delivery of those requirements set out within the Strategic Policing Requirement have been subject to a proportionate and risk-based testing and inspection regime." [36]

3.8. Although both PCCs and chief constables are required to 'have regard to' the SPR in the execution of their respective duties, HMIC has no authority to inspect PCCs. Therefore, this report is focused on the duty of the chief constable, which is set down in the SPR in the following terms: "Chief constables must have regard to both the police and crime plan and the Strategic Policing Requirement when exercising their functions. Their police and crime commissioners will hold them to account for doing so." [37]

3.9. The meaning of 'have regard to' is explained in the SPR: "*It is not uncommon for legislation to require public bodies to 'have regard to' guidance, codes of practice or other material. The effect is that the police and crime commissioner and chief constable should follow the Strategic Policing Requirement unless they are satisfied that, in the particular circumstances, there are good reasons not to. It does not mean that either the police and crime commissioner or the chief constable has to follow the requirement blindly, but they should not depart from it without good reason (and should be prepared to be able to justify any departure from it on a case-by-case basis).*"[38]

[35] SPR paragraph 1.6
[36] SPR paragraph 1.15
[37] SPR paragraph 1.11
[38] SPR paragraph 1.9

4. Methodology

4.1. The breadth of requirements made by the *Strategic Policing Requirement* (SPR) are outside of the scope of a single inspection. It has therefore been necessary to plan a series of inspections over three years so that the police response to all of the national threats can be examined individually and in depth over that period.

4.2. This report is one of three reports on compliance with the SPR which will be published by Her Majesty's Inspectorate of Constabulary (HMIC) this year. It examines how well police forces have established the arrangements that the SPR requires them to have in place in order to counter the national threats.

4.3. In addition to assuring the SPR arrangements, this year's inspection includes an in-depth examination of the police response to two of the national threats: first, the threat to public order; second, the threat of a large-scale cyber incident (these are the subject of two separate inspection reports due to be published later this year as part of this inspection programme). To do this, we requested the 43 forces of England and Wales to provide us with information and data that would allow us to see how well they had responded to the requirements of the SPR. For example, we asked for data that would allow us to assess the capacity that each force had established to contribute to countering each of the national threats.

4.4. HMIC also conducted fieldwork in 18 forces in England and Wales between September and November 2013. We intend to conduct fieldwork in the remaining 25 forces over the next two years. The forces visited are listed in Annex A.

4.5. The fieldwork consisted of interviews with chief officers and those leading the responses to national threats; and a review of relevant policies, strategies and legislation. We verified the information contained in the documents sent to us by forces, and what we were told during our visits to forces, by physically checking that the arrangements were actually in place.

4.6. HMIC also interviewed officers and staff in government departments, policing units with specialist national roles, and also senior police officers with national responsibilities that were relevant to the SPR.

4.7. The analysis and review of the data and evidence gathered during this inspection has been used by HMIC to inform the judgments and recommendations contained within this report.

Roles and responsibilities

4.8. The Government's National Security Council (NSC) commissioned the *National Security Risk Assessment* (NSRA), which catalogues and prioritises the major threats faced by the country. These include those threats that affect the safety of people in England and Wales.

4.9. In response to those NSRA threats, government departments create and implement strategies within which they outline the nature of the threats that police forces are expected to work against, and what they want to be achieved. Senior police officers develop strategies that interpret national intentions and outline how the police service will contribute. Police forces are expected to support those strategies.

4.10. Chief constables are responsible for the 'direction and control' of the 43 police forces in England and Wales and must carry out their duties "*in such a way as is reasonable to assist the relevant police and crime commissioner to exercise the commissioner's functions.*"[39]

4.11. PCCs must "*secure the maintenance of the police force for their areas and ensure that their police forces are efficient and effective*".[40] They must hold chief constables to account for their functions and for the performance of the staff within their forces.

4.12. The College of Policing is the professional body for policing. Its core areas of responsibility include *"supporting police forces and other organisations to work*

[39] s2 Police Reform and Social Responsibility Act 2011
[40] s1 Police Reform and Social Responsibility Act 2011

together to protect the public and prevent crime".[41] The College's Professional Committee now oversees national policy and practice for policing. Its terms of reference are to *"identify gaps, threats or opportunities across policing where capability may need to be built, (including the need to review or develop national standards, policy or practice)*".[42] Working with chief constables, the College of policing creates national standards for professional practice, which are published as Authorised Professional Practice (APP).

4.13. The Chief Constables' Council is the senior operational decision-making body for national policing. It comprises chief constables of police forces in the United Kingdom and it is responsible for coordinating operational policing needs and leading the implementation of national standards set by the College of Policing and/or the Government.

4.14. There are 11 national policing business areas that provide the direction and development of policing policy and practice in specific areas. The chief constables who lead these business areas are members of both the College's Professional Committee and the Chief Constables' Council. For the SPR, the most relevant business areas are uniformed operations, crime, and terrorism and allied matters. Within each business area, there are a number of portfolios and working groups led by chief police officers who act as national policing leads for specific issues. For example, within the crime business area, there are national policing leads for serious and organised crime and e-crime (another term for cybercrime); within uniformed operations, there are national policing leads for public order and civil emergencies. The role of national policing business areas is subject to change in the light of the independent ACPO review.[43]

[41] *Our Strategic Intent*, College of Policing, September 2013, paragraph 1.1.
[42] *Professional Committee Terms of Reference*, College of Policing, 11 July 2013, paragraph 1.2
[43] *Independent review of ACPO*, General Sir Nick Parker KCB, CBE, 14 November 2013

5. Capacity and contribution

Introduction

5.1. This section sets out HMIC's findings on how well forces have established the necessary capacity to make a contribution to countering each of the national threats.

5.2. The SPR states that:

- *"...chief constables must consider the areas set out in this Strategic Policing Requirement...* [and] *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*[44] *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."*[45]

5.3. It also states that chief constables "are advised to consider other professional assessments made by the police, including national planning assumptions, when considering the appropriate policing capacity to respond to the threats…" [46]

5.4. Following the SPR's publication, the College of Policing conducted an assessment of the capabilities and capacity that the police service needed. This resulted in the creation of the *National Policing Requirement*[47] (NPR). During our inspection we found that the NPR, which was written by the police to describe how forces should collectively respond to the SPR, was not being

[44] Capability is covered separately in its own section of this report
[45] SPR paragraph 3.1
[46] SPR paragraph 3.3
[47] *National Policing Requirement,* ACPO, 2012

used as it was intended. Forces were uncertain about the NPR's currency and value and as a result, we found very little evidence that it was being used to help them establish a collective and effective response to the national threats. Also, we could find no evidence that it had been subject to an annual review as promised in paragraph 1.3.3 of the NPR document.

5.5. HMIC analysed data[48] to establish how many 'full-time equivalent' (FTE) posts in police forces were dedicated to roles that were specific to the national threats and whether this number had changed over time, particularly since the SPR's publication.

5.6. Our data analysis indicated that resource levels for dedicated SPR functions have not changed appreciably following the SPR's publication. The total number of dedicated SPR posts in England and Wales in 2013/14 was 11,265.

Terrorism

5.7. The SPR expectations for the police service's response to terrorist threats are:

- *"...they must demonstrate that they have taken into account the need for appropriate capacity to contribute to the Government's counter-terrorism strategy ("CONTEST") by:*
- *identifying, disrupting, and investigating terrorist activity, and prosecuting terrorist suspects;*
- *identifying and diverting those involved in or vulnerable to radicalisation;*
- *protecting the UK border, the critical national infrastructure, civil nuclear sites, transport systems, and the public; and*

[48] Police Objective Analysis (POA) data 2013. For the purposes of this exercise, HMIC considered the 'dedicated SPR functions' to be those in POA level 2 categories: 5f - Level 1 Advanced Public Order; 5i - Civil Contingencies and Planning; 7e - Serious and Organised Crime Unit; and 9b - Counter Terrorism/Special Branch. Due to limitations in the way the data is collected, HMIC's findings from this exercise must be considered as indicative rather than definitive

- *leading the immediate response after or during a terrorist attack, including responding to incidents involving chemical, biological, radiological, nuclear, firearms and explosive material."*[49]

5.8. The policing response to terrorism is delivered through the Counter Terrorism (CT) network, which is a group of dedicated CT policing units: The Metropolitan Police Counter Terrorism Command (CTC), four Counter Terrorism Units (CTUs) and four Counter Terrorism Intelligence Units (CTIUs) across England and Wales.[50] The CT network is funded centrally by a ring fenced Home Office grant and resources are allocated to police forces according to assessments of what is necessary to tackle the threat of terrorism.

5.9. CTUs and CTIUs are regionally-based and responsible for gathering intelligence and evidence to help prevent, disrupt and prosecute terrorism-related offences. These units were actively supporting forces in their regions.

5.10. We found numerous examples where CTU resources had assisted police forces by identifying, disrupting and investigating terrorist activity, which would have been difficult for forces to deal with alone. We found that police forces worked closely with the CT network to provide the capacity necessary to respond to the national threat.

5.11. There are also a number of CT roles in forces that are centrally funded:

- police officers exercising terrorism powers at international air, rail and sea ports;
- armed police officers who may be required to support CT operations;
- counter-terrorism security advisers; and
- police officers who work with communities to prevent people becoming radicalised in violent extremism.

[49] SPR paragraph 3.2
[50] A description of the CT network can be found at: www.acpo.police.uk/ACPOBusinessAreas/TerrorismandAlliedMatters.aspx

5.12. As in the CT network itself, decisions about these resources are made centrally and are linked to the national understanding of the threat, risk and harm that is associated with terrorism. Chief constables apply for funding, and deploy and oversee these resources. However, decisions about the provision of capacity and contribution are ultimately taken by the Office for Security and Counter Terrorism (OSCT) within the Home Office, usually with advice from senior police leaders.

5.13. Against a backdrop of a high level of national control over the funding and deployment of CT resources, there are certain groups, notably special branch officers that are funded by forces. Special branches provide a critical intelligence link between CTUs and local forces and there were concerns that these resources might be vulnerable to the austerity-related cuts that forces must, of necessity, impose. We found that special branch capacity had been maintained in almost all the forces visited; there was a very small reduction which was a result of forces collaborating with each other to cut costs while maintaining capability.

5.14. The national policing business area for terrorism and allied matters has started the CT Futures Programme to develop an evidence-based approach to match CT policing resources with terrorism-related demand, threat and risk.

5.15. One area of concern was that only 16 of the 43 police forces in England and Wales were able to provide us with a locally produced strategic threat and risk assessment (STRA) that considered threats from terrorism. HMIC understands that other information, held at higher levels of security classification, is routinely made available to a restricted group of people within forces and that it is commonly used by forces to inform their risk assessment processes. However, the fact that 27 forces could not provide a STRA meant that we did not have the information necessary to provide assurance that they have considered "*other professional assessments*"[51] as required by the SPR.

5.16. In conclusion, chief constables understand their role in tackling the CT threat. They work with other police forces to host CTUs and maintain special branch

[51] SPR paragraph 3.3

units to work with the CT network to investigate, disrupt and prosecute terrorist suspects. Forces and the CT network have the capacity to tackle the CT threat.

Civil emergencies

5.17. For civil emergencies, the SPR states:

- *"Chief constables must demonstrate that they have taken into account the need for appropriate capacity to respond adequately to civil emergencies requiring a national response as set out in the National Resilience Planning Assumptions for events threatening serious damage to human welfare as defined in the Civil Contingencies Act 2004. This should include incidents causing mass fatalities on a significant scale, and chemical, biological and radiological incidents."*[52]

5.18. PCCs are also reminded by the SPR *"of the responsibilities of their chief constable as a category 1 responder under the Civil Contingencies Act 2004 and the duties this confers, including a duty on chief constables in local resilience forums and strategic co-ordination groups."*[53]

5.19. The *National Risk Assessment* (NRA) is a record, prepared by the Government, of the most significant emergencies that the UK could face. The Government also lists the most likely consequences of these emergencies, describing the maximum scale, duration and impact that could reasonably be expected. These consequences are referred to in the *National Resilience Planning Assumptions* (NRPAs).[54]

5.20. Only seven of the police STRAs provided to HMIC by the 43 police forces included considerations of threats from civil emergencies. In our opinion, one of those seven documents was not detailed enough to aid the planning process. However, we found that Local Resilience Forums (LRFs) produce independent risk assessments, called community risk registers. LRFs make

[52] SPR paragraph 3.2
[53] SPR paragraph 3.4
[54] The rationale for, and description of, national resilience planning assumptions can be found at www.gov.uk/risk-assessment-how-the-risk-of-emergencies-in-the-uk-is-assessed

use of the community risk registers to plan for emergencies and prepare for joint exercises. The risk registers and plans are frequently 'owned' by agencies other than the police – for example, local authorities or fire and rescue services. When we took these risk registers into account (in addition to the STRAs) we found that 16 out of 43 police forces submitted documents that demonstrated any understanding of the threat, risk and harm. That left 27 forces that did not provide any documents to demonstrate that they were considering the threat, risk or harm when deciding the required capacity to respond to the civil emergency threat.

5.21. We found that there was clear leadership commitment to LRFs in the 18 police forces we visited. Senior police officers of chief officer rank attend executive group meetings, which provide the strategic direction for LRFs. There was evidence that police forces' staff actively took part in and managed sub-groups and working groups that supported executive groups. In Wiltshire, for example, the police worked with their LRF partners to run regular workshops where LRF practitioners worked through practical scenarios linked to incidents that the partnership was likely to face.

5.22. We found that the resources committed by police forces to emergency responses had not changed since publication of the SPR. These resources include officers trained:

- to command the responses to incidents, including managing joint strategic co-ordination groups;
- to perform roles in the identification of victims from incidents where there are large numbers of casualties: senior identification managers (SIMs); disaster victim identification officers (DVIs); temporary mortuary staff; casualty bureau staff; and
- to work in areas believed to be contaminated by chemical, biological, radiological or nuclear material (CBRN).

5.23. Interviews with police officers in the South West, Eastern and East Midlands regions revealed that the availability of staff with specialist skills required to

support police responses to civil emergencies was co-ordinated by Regional Information and Co-ordination Centres (RICCs). The South East has established a disaster victim identification (DVI) board that co-ordinates DVI capability for forces across the region. RICCs work with the NPoCC to maintain an up-to-date record of information about police officers with specialist skills, helping to provide sufficient capacity to contribute effectively to this threat. The role of the NPoCC, in mobilising resources across police force geographic boundaries, is explored more fully in the Connectivity section later in this report.

5.24. HMIC found that the highly local nature of responses by partner agencies to this threat made it difficult for police forces to collaborate with each other to provide the full range of civil emergency response capabilities. Only Bedfordshire and Hertfordshire had done so. However, there were some good examples of police forces co-operating to provide individual elements that support emergency responses. For example, Gwent and South Wales police forces share the use of strategic command centres, necessary for the co-ordination of emergency responses. There is also an 'All Wales Joint Emergency Planning Steering Group'.

5.25. Following a threat assessment of CBRN-related terrorism in 2005, police forces were funded to develop capabilities in terms of trained staff using appropriate equipment, to deal with CBRN incidents. The NPR states that "*the capacity for CBRN is set at 8,475 trained officers, which equates to 339 PSUs. A review by the Office of Security and Counter Terrorism is currently underway to re-examine the threat and risk of CBRN incidents and the appropriate policing response."*[55] This inspection has not checked the capacity that forces have to respond to a CBRN incident. This will be done when HMIC conducts an in-depth civil emergencies inspection.

5.26. Some forces reported that CBRN equipment was reaching the end of its useful life. Of the 18 forces visited, one was replacing its equipment as it reached the expiry date. In six forces, CBRN staff reported that they were not replacing equipment. Two forces reasoned that, because the national policing lead for

[55] *National Policing Requirement,* ACPO, 2012, paragraph 4.3.3

CBRN was engaged in discussions about the future role of the police at CBRN incidents, they could assume that the police would not, in the future, be required to operate within hazardous areas. This would remove the need to replace their equipment.

5.27. A review by the OSCT of the police response to a CBRN incident is underway with the police service taking part. One element of this review has been completed and significant change is being implemented. The detail of the change was described in a letter to chief constables in October 2013. To help police forces implement these changes, new e-learning material, explanatory DVDs and guidance have been issued to forces. HMIC is satisfied that forces are being kept informed of the review's progress and that it will help them make informed decisions about their CBRN capacity and equipment requirements in the future.

5.28. In addition to the basic CBRN roles, police forces have to carry out some specialist CBRN roles: for example decontamination and detection. Police forces in the South West region have shared responsibility for these roles among themselves in a way that makes sure the region has the full range of CBRN capabilities.

5.29. In conclusion, chief constables are working in the LRFs to prepare for a civil emergency. The absence of documents that demonstrated a shared understanding of threat, risk and harm from 27 forces and an absence of STRAs in all but seven forces is a matter of concern to HMIC. The review by the Home Office will redefine the police response to a CBRN incident and clarify the contribution needed by police forces. We will look more closely at the capacity that forces have made available to deal with civil emergencies and the quality of emergency plans in a future stage of the SPR inspection programme.

Organised crime

5.30. This section examines how well police forces provide the capacity necessary to contribute to the national effort to tackle organised crime. This national threat covers a diverse range of criminal activity, most of which is motivated

by profit but there are exceptions such as child sexual exploitation. The police face challenges in developing a full understanding of the threat.

5.31. The SPR states that:

- *"Chief constables must demonstrate that they have taken into account the need for appropriate capacity to contribute to the Government's organised crime strategy – by working with partners to:*
  - *work with communities to stop people being drawn into organised criminality;*
  - *strengthen enforcement against organised criminals, including through the Integrated Operating Model; and*
  - *raise awareness of organised crime and work with private sector and civil society partners to develop safeguards from organised crime."*[56]

5.32. In October 2013, the Government issued a revised *Serious and Organised Crime Strategy* that superseded the strategy referred to above. The new strategy is based on four strands:

- Pursue – prosecute and disrupt people engaged in serious and organised criminality;
- Prevent – prevent people from engaging in serious and organised crime;
- Protect – increase protection against serious and organised crime; and
- Prepare – reduce the impact of this criminality where it takes place.[57]

5.33. The police service has a role to play in all of these strands in order to achieve the strategy's aim, which is to '*substantially reduce the level of organised crime in this country and the level of serious crime that requires a national response'*.[58] Nationally, law enforcement activity against organised crime

[56] SPR paragraph 3.2
[57] *Serious and Organised Crime Strategy*; HM Government, Cmnd 8715, October 2013, page 8
[58] *Serious and Organised Crime Strategy*; HM Government, Cmnd 8715, October 2013, paragraph 1.5

groups (OCGs) is co-ordinated by the National Crime Agency (NCA) which was established in October 2013, part way through our fieldwork. The majority of activity against OCGs is at force and regional level. OCGs are identified and assessed in terms of their level of intent, capability and criminality and this information is used to prioritise the policing and law enforcement response.

5.34. All police forces have taken steps to identify, assess and map OCGs within their force areas. While the NCA and senior police leaders acknowledge that there is inconsistency in the way that police forces (and other law enforcement agencies) map their OCGs, they do have an understanding of the OCGs that they have to disrupt.[59] Some forms of organised crime are easier for forces to map than others.

5.35. Twenty-seven police forces had considered threats from OCGs within their STRA. However, of those documents, two were still in draft form, a further two were dated 2011 or earlier; three did not contain sufficient detail to help with planning resources. Amongst the remaining sixteen forces, a variety of different methods had been used to consider threats from OCGs. Evidence from these forces suggested differing levels of understanding of the threat. Four forces provided HMIC with little or no evidence of an assessment of the threat from organised crime. Reflecting learning from counter-terrorism (notably the development of what are known as counter-terrorism local profiles) police forces and the NCA are now encouraged to develop and share local profiles of serious and organised criminality.[60]

5.36. We found that there was no single arrangement which would decide the capacity that should be created in police forces to tackle organised crime. Each force approaches it differently. We found that, too often, forces relied too much on the personal experience of a small group of officers and not enough on an objective assessment, based upon a number of relevant criteria.

5.37. A good approach was found in the Metropolitan Police Service, where decisions about the capacity it required were based on a rounded

[59] The NCA is leading a multi-agency review of the OCG mapping process.

[60] *Serious and Organised Crime Strategy*, HM Government, October 2013, Cmnd 8715, paragraph 4.18

consideration of the organised crime threat, risk, harm and demand. Using information from OCG mapping and other sources, the force considers:

- the number of organised crime groups in the area;
- the seriousness of their offending;
- levels of 'coverage' (the number of organised crime groups under close and regular police attention);
- availability of specialist resources to tackle the most serious threats;
- how quickly the force was able to disrupt or disable organised crime groups; and
- volumes and trends in offence types such as firearms discharges and drug-dealing.

5.38. We found this to be a comprehensive approach that worked well.

5.39. The Government has provided funding to develop regional organised crime units (ROCUs). Further detail about these units is in the Capability section of this report.

5.40. HMIC found that, in addition to the well-established and mature arrangements in the East Midlands, some forces were also collaborating separately from the ROCUs to tackle serious and organised crime threats. These include: Bedfordshire, Cambridgeshire and Hertfordshire; West Mercia and Warwickshire; Norfolk and Suffolk; and Kent and Essex. Plans are being developed for collaboration between Surrey and Sussex in 2015 on organised crime capability.

5.41. Too many STRAs were not of sufficient quality to be relied on with enough confidence to make decisions about planning resources. This problem is compounded by the fact that too many forces are making resourcing decisions based too much on the personal experience of a small group of officers, and not enough on an objective assessment of threat, risk, harm and demand.

Public order

5.42. The SPR states that:

- *"Chief constables must demonstrate that they have taken into account the need for appropriate capacity to respond adequately to a spontaneous or planned event, or other incident, that requires a mobilised response in order to keep the peace, protect people and property, and uphold the law…and chief constables need to ensure they can keep the peace by preventing and managing public disorder and both facilitate peaceful protest and protect the rights and safety of wider communities when responding to large-scale public protests."*[61]

5.43. Thirty-eight of the 43 forces provided their public order STRA to HMIC. Of these, 33 were considered to be of sufficient quality and detailed enough to inform forces' decisions about allocating resources. The public order STRAs of the City of London Police, Derbyshire, Dyfed-Powys, North Wales, North Yorkshire and Northamptonshire were considered by HMIC to be particularly good examples. The others were either incomplete, out-of-date or did not have sufficient detail to inform decisions about the capacity that is required to respond to a national threat. This represents a significant weakness.

5.44. Following the 2011 disturbances, chief constables in England and Wales agreed that, together, they needed to have 297 police support units (PSUs) to respond adequately to the threat of public disorder in the future. They considered this sufficient to deal with three separate areas of significant disorder happening simultaneously in England and Wales for a period of seven days. Each of the nine police regions is required to contribute a proportion of the 297 PSUs. Regions' contributions are calculated using a formula agreed by chief constables based on the size of each force within the region.

5.45. HMIC asked all police forces in England and Wales to provide the following data:

[61] SPR paragraph 3.2

- the number of PSUs that they were required to provide towards the national requirement;

- the number of PSUs that they needed to respond to local outbreaks of disorder in their force area (referred to hereinafter as the force's local threat);

- the number of PSUs they had trained and equipped currently to national public order standards; and

- details of each officer they had trained to the national public order standard for operating in a PSU.

5.46. The reason we asked for details of both the number of PSUs needed to the meet the national requirement and the local one was because the police service is expected to be prepared for both.

5.47. All 43 forces provided the number of PSUs that they had in July 2013 which, once aggregated, made a total of 769 PSUs. This confirms that, together, forces have enough capacity to meet the national requirement of 297 PSUs.

5.48. Next we examined the level of capacity that forces had assessed as necessary to respond to a local threat. When added together, the total number of PSUs that forces had assessed they required was 587.

5.49. We also aggregated the total number of trained public order officers police forces had. The total trained was 26,611, which is significantly more than the total number of officers required to form the 769 PSUs that forces collectively say they have.

5.50. For each force, HMIC compared the number of PSUs they declared they had with the number of PSUs that they told us they needed to respond to local outbreaks of disorder. This is illustrated in the graph in Figure 1 where the red line represents the level required and the blue bars represent the level of PSUs (as a percentage of the requirement) that is present in each force. We found that in five forces, while they complied with the national requirement, they did not have enough PSUs to meet their assessments of the local threat.

On the other hand, we found that in 14 forces had at least twice the number of trained PSUs (represented by 200 percent in Figure 1) they had assessed as necessary to meet their local threat.

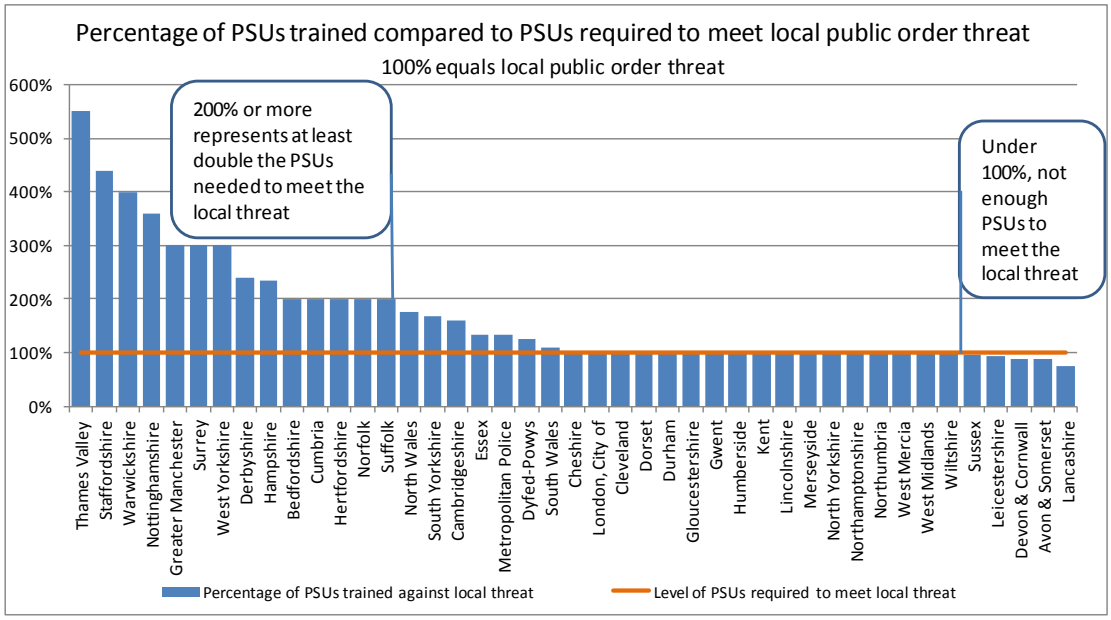

Figure 1: Percentage of PSUs trained compared with PSUs required to meet local public order threat.

5.51. This finding is corroborated by a self-assessment[62] carried out by all forces in October 2013, where approximately one-fifth of forces assessed that they did not, on their own, have sufficient levels of resources to meet their assessment of local threats.[63] This suggested they may be more reliant on mutual aid than other forces.

5.52. While the national requirement is clear, and every force and region is complying with the requirement, it is much less clear how forces should provide sufficient capacity to meet both the national and the local requirement. This lack of clarity has resulted in very different approaches being used by forces to assess the capacity needed to deal with the local threat.

[62] *Public Order Capability Framework v1.2*, College of Policing, March 2013
[63] *Ibid*, capability APP/13/PO/02

5.53. HMIC explored why forces were training vastly different numbers of staff compared to those required by their local threat assessment. For four[64] out of the 14 forces highlighted it is because their national requirement for PSUs is greater than their local threat and they have resourced to their national requirement. This leaves 10 forces where it is not readily evident to HMIC why they had at least twice the number of trained PSUs they had assessed as necessary to meet their local threat. Evidence gained from HMIC interviews with the forces' leaders indicated that they used different methods to determine the number of police officers to be trained for public order duties. Where numbers exceeded those needed to meet local and national requirements, the extra staff were considered necessary to provide for absence through sickness, court appearances, secondment and training, as well as helping to deploy PSUs quickly.

5.54. West Midlands Police officers described how they had used a series of calculations to decide the numbers of public order-trained staff needed. These were based on maximum numbers of PSUs mobilised in the past, the effect of shift patterns, absentee levels and the degree of attrition through injury during prolonged public order deployment. Kent Police described its use of an 'industry standard' for the number of staff they needed, above the level required to respond to their local threat, to cover absences and deploy quickly.

5.55. We understand that forces will need to take into account factors such as absentee levels and the effect of shift patterns on availability in assessing the capacity they need. However, we do not understand why 10 forces had decided to have at least twice their required level, or how five forces have decided to have a lower level of resource than their own assessments say they need.

5.56. The use of mutual aid is another indicator of the extent to which police forces either have or do not have sufficient trained public order resources. As part of the inspection we asked all forces to provide us with details of the number of PSUs they had received from other forces during the period 2011/12 and 2012/13. HMIC was unable to verify the accuracy or completeness of this data

[64] Thames Valley, Hampshire, Surrey and Norfolk

supplied by forces and therefore considers our findings as indicative rather than conclusive. The data indicated that 12 forces were net recipients of mutual aid for public order policing and 32 forces were net providers.[65] This is illustrated in Figure 2 below.

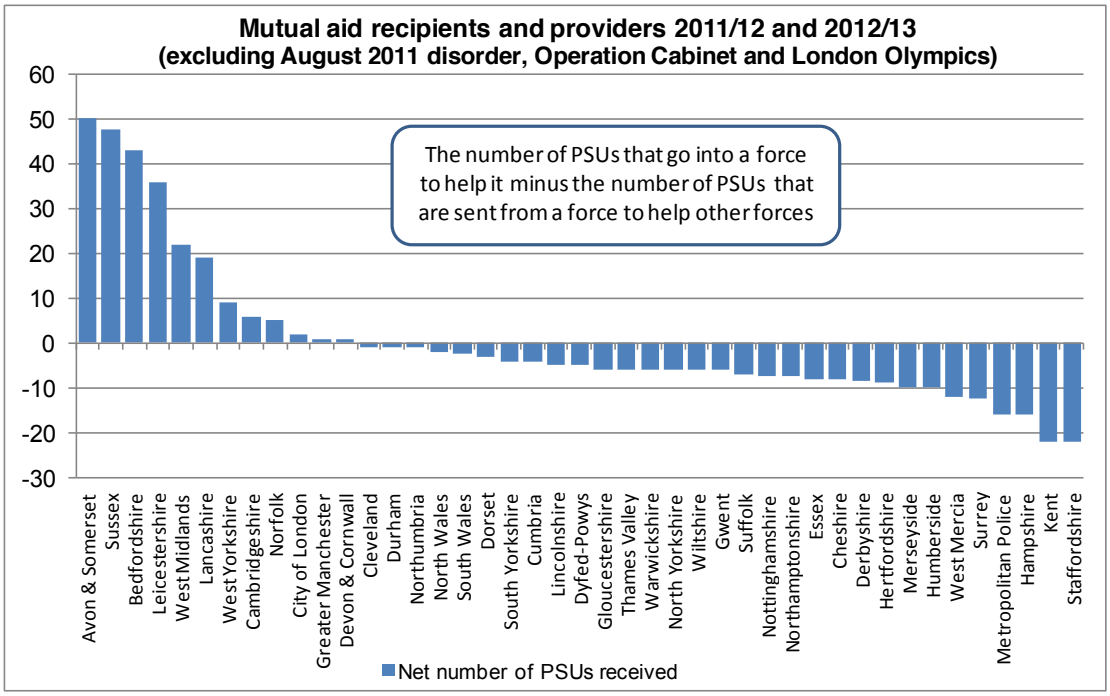

Figure 2: Mutual aid recipients and providers 2011/12 and 2012/13.

5.57. This indicates that forces do not always have sufficient public order-trained staff available to respond to outbreaks of disorder in their force area. Requirements for mutual aid should be expected, but the national requirement relies on every force playing their part; an excessive reliance on mutual aid could indicate that a force has insufficient capacity to do this.

5.58. In conclusion, chief constables understand their role to provide PSUs to respond to public disorder across force boundaries and to make a contribution to the national requirement of 297 PSUs. Our inspection confirms that all forces have the capacity to make this contribution. It is disappointing to find that there are a number of police forces that are either still not using the threat assessment process to its full effect or not using it at all. Even if forces do

[65] This analysis excluded three major policing operations - the 2011 widespread disorder experienced in England in August 2011, the London Olympics 2012 and the removal of the residents at Dale Farm, Essex in 2012 (Operation Cabinet) - as they were exceptional incidents that skewed the results

assess threats, risks and harm, they do not always use the information to decide on what resources are needed. Finally, HMIC does not understand the rationale for 10 forces to train double or greater levels of public order trained staff than they say are required to meet their local threat.

Large-scale cyber incident

5.59. This section examines how well police forces provide the capacity necessary to contribute to the national effort to tackle a large-scale cyber incident.

5.60. The SPR states that:

- "*Chief constables must demonstrate that they have taken into account the need for appropriate capacity to respond adequately to a major cyber incident through the maintenance of public order and supporting the overall incident management and response, recognising that the police response to cyber-related threats needs to develop further*."[66]

5.61. As acknowledged by the SPR, the threat of a large-scale cyber incident is the newest of the national threats to require a national co-ordinated response by the police and the national law enforcement and intelligence agencies. Before carrying out our inspection, we sought first to understand the nature of the threat so that we could properly scope our work. Our discussions with government officials and other specialists in this field of work helped us to understand that the police response should be to counter the fast-increasing volume of crime in cyberspace and a single determined cyber attack on national security interests. This is because a large-scale cyber incident could be caused by either the aggregation of individual crimes or the commission of a single attack (as well as by a computer failure not attributable to crime).

5.62. Digital technology and the internet are providing criminals with new opportunities to commit crime, either where criminals use computers to help them commit crimes that would have been committed previously without the benefit of such technology, for example, fraud and theft; or where they commit

[66] SPR paragraph 3.2

new crimes that were not possible before, such as an attack on government online services using malicious software.

5.63. These two categories of cybercrime are respectively known as cyber-enabled and cyber-dependent crimes.[67]

5.64. With this in mind, we expected police forces to have sought to understand the threat and their role in tackling it. We expected this to incorporate a growing level of capacity and capability to deal with those volume cybercrimes which, when aggregated, could constitute a large-scale cyber incident as well as contributing to the development of a national intelligence picture about any criminal activity aimed at attacking national systems and infrastructure.

5.65. We found that only three forces (Derbyshire, Lincolnshire and West Midlands) had developed cybercrime strategies or plans that included a comprehensive plan to tackle cybercrime. We expected to find plans about how forces intended to tackle this threat, for example by investigating and preventing cybercrimes.

5.66. Fifteen police forces had considered cybercrime threats within their STRA. The West Midlands Police strategic assessment was particularly good; it was detailed and included considerable information about the nature of cyber threats and the challenges it faced in planning responses.

5.67. Senior leaders in each force were asked to define what they believed constituted a large-scale cyber incident; the responses varied greatly across the forces we visited. This reflects the relative immaturity of the response to this threat which is improving rapidly. Even during the short life of this inspection we witnessed significant progress by the Home Office, National Crime Agency and the police service in development of definitions, policy and plans. Also, on 31 March 2014 the Government launched the UK national Computer Emergency Response Team (CERT-UK). The responsibilities of this team include national cyber-security incident management. CERT-UK will

[67] *Serious and Organised Crime Strategy*, HM Government, October 2013, Cmnd 8715, paragraph 2.54

be the lead body for co-ordinating cyber-incident responses at the national level.

5.68. There was a generally held mistaken view among those we interviewed that the responsibility for responding to a large-scale cyber incident was one for regional or national policing units and not for forces. There was very little understanding of the part forces should have in working together with regional and national organisations to respond to the threat.

5.69. Evidence of the poor understanding of the threat and the role of forces was also found when we examined the STRAs and strategic plans that we had been provided by forces, together with the national guidance that existed at the time of the inspection. We found these to be focused only on the investigation of cybercrime and not on protecting the public and preventing cybercrime at force level. The publication of the new *Serious and Organised Crime Strategy* gives an opportunity for forces and national agencies to structure their plans and guidance around the four themes of 'pursue, prevent, protect and prepare' to create a comprehensive approach to tackling cybercrime.

5.70. The development of new policy for the police response to the cyber threat is overseen by the National Cyber Capabilities Programme, which is jointly led by a senior leader from the NCA and the police.[68] At the time of the inspection, the NCCP was still in the early stages of development. Within a month of its introduction, the National Cyber Crime Unit, together with the national policing lead for e-crime, produced an assessment of national cyber capabilities describing the capabilities that should be established at force, regional and national levels to investigate cybercrime. Progress was being made very quickly.

5.71. The Government and PCCs have increased investment in ROCUs to establish fully the range of capabilities that are necessary to support police forces. These capabilities will include the investigation of complex cyber crimes and the co-ordination of other investigations that have a cyber element. The initial

[68] The Head of the National Cyber Crime Unit, part of the NCA and the (police) national business area lead for e-crime

investment from Government and PCCs will fund at least four posts to create cyber crime units within each ROCU. That said, although there were plans in place and recruitment underway, we found that six of the nine ROCUs did not yet have any cyber capability in place. Cyber capabilities were present in three ROCUs: East Midlands; South West; and the Yorkshire and Humber sub-region of the North East. We were advised that cyber capabilities previously available in the Northwest ROCU had been lost when staff transferred to the NCA.

5.72. We found in interviews with senior police leaders that their decisions about the number of staff required to investigate cybercrime were based on the volume and nature of crimes reported to their forces rather than the associated threat, risk and harm.

5.73. Furthermore, evidence from our interviews and the documents submitted by forces showed that police forces' capacity and contribution to the response against the national cyber threat is currently limited to the deployment of a relatively small number of specialists, who can be used to investigate any crime type including cybercrime. These are generally in the form of 'hi-tech crime' investigators who recover evidence from computers, covert internet investigators (CIIs), and those who deal with communications information (data about telephone and internet traffic). For example, Gloucestershire had three 'hi-tech' crime staff and there were only 43 across the six police forces within the Eastern Region. The Metropolitan Police had approximately 70[69] within its Police Central e-crime Unit (PCeU) and, with its responsibility for policing the capital city and high levels of cybercrime, will retain significantly larger cyber resources than other forces.

5.74. In conclusion, our findings confirm what was recognised in the SPR itself: "*the police response to cyber-related threats needs to develop further*". [70] This is because the rapid development of digital technology and the internet has created opportunities for communication that is beyond the majority of

[69] The Metropolitan Police hosted the Police e-Crime Unit (PCeU) that had national responsibility for investigating serious and complex cybercrimes. This responsibility, with a large proportion of PCeU staff, has since moved to the National Cyber Crime Unit within the National Crime Agency

[70] SPR paragraphs 1.5 and 3.2

people's understanding and imagination. It has created opportunities for criminals to perpetrate their crimes against victims across the world, operating freely and anonymously across state boundaries without much fear of being detected by international law enforcement agencies. The UK has acted as quickly as its international partners in developing a response to the cyber threat; it is not surprising that there is more for the police, working with the Government and others, to do in this area.

5.75. HMIC's finding that forces are not yet able to demonstrate that they understand their roles in tackling this threat is fully understood as a problem by the Home Office, the police and the NCA. We found evidence that across these bodies, and wider partners, work is underway. This should help provide the clarity that is needed for police forces and PCCs about their roles and the capacity and capability they need to put in place to respond to the threat effectively.

Recommendations in relation to capacity and contribution

Chief constables should conduct an evidence-based assessment of the national threats (as described in the SPR), at least annually, and make it part of their arrangements for producing their strategic threat and risk assessments. This should start immediately because it is essential to understand the threat and risks before deciding upon the level of resources that are necessary to respond.

Chief constables and PCCs should, as part of their annual resource planning, explicitly take into account their strategic threat and risk assessments when they make decisions about the capacity and capability required to contribute to the national response to those threats. This should start with immediate effect.

Chief constables should work with the College of Policing to create national guidance that describes how forces should establish the number of PSUs they need to respond to their assessment of the local public order threat. This should be completed within six months.

Chief constables should work with the Home Office, the National Crime Agency and CERT-UK (following its launch in March 2014) better to understand their roles in preparing for, and tackling the shared threat of a large-scale cyber incident. Their roles should cover the 'pursue, prevent, protect and prepare' themes of the *Serious and Organised Crime Strategy*.

Recognising the fact that both the understanding of the national threats and the police response to them are continually changing, the Home Office should regularly review the SPR to make sure its requirements remain relevant and effective.

6. Capability

6.1. In this section, we set out our findings in relation to how well chief constables secure the knowledge, skills and supporting equipment required to ensure that each force's capability is effective.

6.2. PCCs must hold chief constables to account for the provision of the following capabilities identified as critical to the planning for, mitigation of, and efficient and effective and proportionate response to the national threats. The capabilities are those needed to:

- *"identify and understand threats, risks and harms and ensure a proportionate and effective response (including at times of elevated or exceptional demand);*
- *gather, assess and (where appropriate) report intelligence – including the capability to do so across force boundaries and with national agencies;*
- *conduct complex investigations (including proactive or cyber investigations) – including the capability to do so across force boundaries;*
- *respond to critical incidents, emergencies and other complex or high impact threats, including cyber, in the National Risk Assessment;*
- *provide trained and competent command and control of major operations, including the co-ordination of joint multi-agency responses to emergencies;*
- *protect covert tactics, witnesses and resources;*
- *provide armed support, where necessary, to an operation through the use of firearms and less lethal weapons; and*

- *provide police support to major events, such as the Olympic Games."* [71]

6.3. The SPR goes on to specify: *"Forces should have the knowledge, skills and supporting equipment to operate effectively at the specialist levels required in respect of the capabilities outlined in paragraph 4.1 above. The police service should maintain a clear understanding of the location and availability of specialist policing assets in order to maintain the capability at very short notice to mobilise and conduct mutual support across boundaries. Where mobilisation or co-ordination of assets is required, these capabilities should be tested."* [72]

6.4. The College of Policing has developed a method of helping forces assess for themselves, by the use of a capability framework, how well their capabilities match what is needed to provide a particular operational response. They have been prepared for police responses to civil emergencies, serious and organised crime, public order and cybercrime, but not yet for terrorism. Completing these helps forces to identify gaps in the arrangements they have in place to respond to the national threats and, if every force completed them, could provide a national overview of police force capability.

Terrorism

6.5. As described in the 'Capacity and contribution' section of this report, arrangements for countering terrorism are well developed and resourced – with the national CT network providing the majority of capacity and capability to respond to the threat by:

- undertaking complex investigations;
- responding to critical incidents, including command and control;
- providing specialist equipment; and
- training staff to national standards.

[71] SPR paragraph 4.1
[72] SPR paragraph 4.2

6.6. Forces are expected to provide sufficient capability to provide armed support to CT operations and gather, assess and report intelligence to inform local and national understanding of the terrorism threats. Police use of firearms is outside the scope of this year's SPR inspection but will be covered fully in a later report in the series of our SPR inspections.

6.7. Force special branch (SB) officers, who are mainly funded from force budgets, gather intelligence that is then assessed and reported to the CT network. The CT network also assigns work to SB officers in forces to gather specific intelligence against particular subjects as set by national priorities. Some of these SB posts are centrally funded – such as those working at ports and airports. We checked in forces that the capability was in place to gather, assess and report intelligence across force boundaries.

6.8. Our inspection found numerous examples of how forces fulfil this part of the SPR. In Humberside, we found that the SB team had a specific intelligence management unit to assess the intelligence collected and to contribute to the understanding of the force-level and national CT threat. In Avon and Somerset, the force used a secure video conferencing system with the other forces in the South West region to conduct daily management meetings, at which details of terrorist intelligence and operational action to tackle terrorists could be discussed across force boundaries.

6.9. Skills for CT officers have been agreed and standards for training set by the College of Policing at a national level. We found that Greater Manchester, Nottinghamshire, Leicestershire, Wiltshire and Gwent police forces maintained a profile of each SB officer's skills that was kept up-to-date by staff interviews, and was a basis for deciding training needs. This allowed forces to "maintain a clear understanding of the location and availability of specialist policing assets"[73] as required by the SPR. All the forces we visited provided information that demonstrated that they complied with national training standards. This will be tested further in a subsequent inspection of terrorism capability as part of the SPR series of inspections.

[73] SPR paragraph 4.2

6.10. In conclusion, all of the 18 forces HMIC inspected had, in their SB officers, the necessary capability to gather, assess and report intelligence. The same forces had the systems in place to manage the training of SB officers to maintain the necessary skills to provide that specific capability at force level.

Civil emergencies

6.11. The national response to civil emergencies is co-ordinated by the Cabinet Office's Civil Contingencies secretariat. The *National Risk Assessment*[74] provides an assessment of the likelihood and potential impact of civil emergency risks. Each risk has a lead government department. For example, the lead for the risk of public disorder is the Home Office, while the lead for the risk of flooding is the Environment Agency.

6.12. The response to, and recovery from, a civil emergency is provided by a wide range of bodies including the emergency services, local authorities and government departments. These bodies work together through local structures called local resilience forums (LRFs). The police service is defined as a Category 1 responder[75] in the Civil Contingencies Act 2004 and has a legal responsibility to provide an appropriate response to emergencies and to attend the LRFs as far as reasonably practicable.[76] HMIC has reported the police force contribution to LRFs in the 'Capacity and contribution' section of this report.

6.13. The development of standards for civil emergencies is relatively mature. There is a national strategy, linked to the Civil Contingencies Act 2004. There is a training curriculum for specific roles, and the necessary training is provided by forces. There are national standards for certain aspects of specialist training, including disaster victim identification (DVI) and casualty bureau roles.

6.14. In the 18 forces we visited we checked the records and management information concerning which staff were trained in DVI and casualty bureau

[74] See https://www.gov.uk/government/publications/national-risk-register-for-civil-emergencies-2013-edition

[75] section 3(1) schedule 1(part1) Civil Contingencies Act 2004

[76] Civil Contingencies Act 2004 (Contingency Planning) Regulations 2005 (SI 2005/2042), reg 4(4) (as amended)

roles. We found that all of them maintained satisfactory records, usually as part of their HR systems. In some of these forces a further record was held by the senior responsible officer for civil emergency.

6.15. There is APP available for the response and recovery roles of the police service[77], and we consider that forces are able to provide the capability necessary to respond to cross-border civil emergencies. The police service is training staff for the most important response roles to a common standard and managing how they maintain these skills through accreditation and monitoring of training records.

Organised crime

6.16. The approach to tackling organised crime in England and Wales involves maintaining a network of ROCUs. These units vary in terms of their structure and composition. Their common features are that they provide a range of functions to the forces in their region to support efforts to tackle organised crime and they act as a point of connection between the NCA and the police forces. It is also the case that all 43 police forces maintain their own resources to tackle the organised crime threat.

6.17. In March 2013 the Home Office announced an increase in the level of financial support it provides to ROCUs from £16m per annum previously, to £26m for 2013/14, in order to help ROCUs *"mature into the consistent and effective network that forces and the NCA will rely on as they work together to fight organised crime*".[78]

6.18. This increase required a similar level of investment and commitment from PCCs and it was originally intended that "*we* [police forces and the Home Office] *work quickly to ensure ROCUs are ready for the start of the NCA in October* [2013]."[79] The additional investment was to pay for an increase in ROCU capabilities, specifically in the areas of intelligence collection and analysis, asset recovery, fraud, cybercrime, prison intelligence and the

[77] See http://www.app.college.police.uk/
[78] Letter from Home Secretary to Chief Constables and police and crime commissioners dated 12 March 2013
[79] Op cit

provision of witness protection. In October 2013 the Home Office, when publishing the new *Serious and Organised Crime Strategy*, indicated that it expected "*significant change by the end of 2014*".[80]

6.19. Forces in all regions agreed to match the additional Home Office investment. Arrangements for programme management were created under the leadership of a chief officer working to the national policing business area lead, with projects set up in each ROCU. The police ROCU programme has set a more detailed timeline for this work, from April 2013 to April 2015.

6.20. Home Office funding for ROCUs is allocated on an annual basis which makes it difficult for forces to plan for the longer term.

6.21. HMIC visited each of the nine ROCUs to examine the rate of progress and levels of consistency between ROCUs. HMIC found that, in all regions except London, chief constables and police and crime commissioners had agreed their detailed plans for ROCU development. It was clear to HMIC that reaching agreements had not been a straightforward process in all regions and there had been some delays.

6.22. HMIC heard concerns from some respondents about the viability of the annual funding arrangements. We also noted that, in five ROCUs, the underpinning legal agreements[81] between the contributing forces and PCCs were either in draft, under review or not signed.[82] Following our visits HMIC was informed that these agreements are now almost all resolved.

6.23. The absence of a legal agreement between participating forces had resulted in uncertainty about who would have responsibility for: the direction and control of police officers and staff working outside their home force area; occupiers' and employers' liability and liability to third parties; health and safety; and dealing with public complaints.[83]

---

[80] *Serious and Organised Crime Strategy*, HM Government, October 2013, Cmnd 8715, paragraph 4.11

[81] legal agreements made under section 22A Police Act 1996

[82] London, West Midlands, South East, Eastern, Yorkshire & Humber sub-region

[83] See *Statutory Guidance for Police Collaboration*, October 2012, Home Office, available at: https://www.gov.uk/government/publications/statutory-guidance-for-police-collaboration

6.24. Despite the lack of finalised legal agreements in five regions and practitioners' concerns about the grant funding arrangements, each of the ROCU projects is well underway and progress is being made. When we interviewed managers we found that they were well-engaged and committed. However, the ROCUs have not yet become the 'consistent and effective' network that the additional funds were intended to make possible.

6.25. All ROCUs had a regional intelligence unit and an asset recovery team, but at the time of our visits to the ROCUs: none had the full range of intelligence collection and analysis capabilities that are required; five had no fraud team; and three had no dedicated government agency intelligence network (GAIN) co-ordinator in post. These findings reflect the position at the time of our visits and we have been informed since then that all ROCUs have now appointed fraud teams and GAIN co-ordinators.

6.26. HMIC identified that some regions were taking a bold approach to collaboration as they were planning to rely solely on regional resources for some capabilities. This is the case with the East Midlands Special Operations Unit (EMSOU), which remains a good example of how a ROCU and police forces in a region can work together to secure the benefits of collaboration: economies of scale, improved resilience and a more consistent approach. Other, less ambitious examples included the North West and South East regions, where a range of functions presently carried out in each of the constituent forces is being absorbed into the ROCUs. Others, such as the North East region, intended to retain capabilities within individual forces as well as to build capabilities within the ROCU. In doing so, they are not taking full advantage of the benefits of collaboration.

6.27. The main challenges faced by leaders, as they tried to build a network with a consistent set of capabilities in each ROCU, were twofold: recruiting the personnel into the new posts provided by the extra funding; and providing accommodation sufficient to meet the needs of an expanding workforce. The former issue was exacerbated by a limited availability of skilled and experienced personnel to work in ROCUs. The latter has led to further projects and extra funding to create new accommodation for some ROCUs. Some of

these projects are taking good advantage of opportunities to co-locate ROCUs with Counter Terrorist Units (CTUs) and/or NCA teams, which should lead to greater efficiencies.

6.28. HMIC concluded that progress is being made and that the advanced state of planning and recruitment was encouraging. HMIC shares the concerns expressed by some respondents – that the annual recurring funding arrangements are problematic for forces. Chief constables would find it easier to commit to ROCU development if the Home Office funding came with more certainty around its availability for the longer term.

6.29. HMIC interviewed senior leaders with responsibility for organised crime capability in each of the 18 forces we inspected. With them, we explored the relationship between force and regional capabilities to undertake organised crime investigations, and to gather, assess and report intelligence on organised crime. These investigations required the ROCU either to provide all of the necessary capacity and capability to investigate the crimes, or only that which was needed to supplement the force's own resources. We found that in those forces where the threat from organised crime was assessed as the highest, the force level capability was greater than in forces with a lower threat. This is as it should be – with capability levels proportionate to the threat, risk and harm.

6.30. We found that the training requirements for the specialist roles employed by police forces to tackle organised crime were well defined and, for some roles, accredited to a published standard. The College of Policing has an organised crime training curriculum and APP is available for some of the roles. Police forces across England and Wales deliver different parts of the curriculum, with the more technical areas taught by external commercial providers.

6.31. We found that forces were collaborating within the regional structure to provide most of the necessary training. Areas of training where there was not yet adequate coverage were those relating to the provision of accredited training for senior investigating officers to manage covert investigations of

OCGs, and authorising officers for undercover operations.[84]. The national policing crime business area lead had recognised these issues prior to the inspection and was dealing with them.

6.32. In the 18 forces visited, we checked how records of skills and accreditation in organised crime specialist roles were managed and recorded. We found all 18 forces were keeping records and were therefore able to plan the training needs of their officers in relation to organised crime.

6.33. In summary, forces and ROCUs either have the capabilities required, or have plans to deliver them in the near future. The plans for ROCUs to have a standard set of capabilities are taking longer to implement than was originally intended. Success will rely on chief constables and PCCs in each region completing the formal legal agreements that are required.

Public order

6.34. All officers in a PSU must be trained to a standard as defined in the College of Policing's curriculum for public order training. This includes tactics to advance to disperse crowds, make arrests and work in situations where attenuating energy projectiles (AEPs) are being used by specially trained police officers to quell very serious disorder. These tactics go beyond the containment of disorder and allow the police to take positive action to end incidents of disorder before they escalate. Together, the proactive actions are known as 'go-forward' tactics.

6.35. We found that the 43 forces had 769 PSUs trained to this standard in July 2013 which, as we say in the 'Capacity and contribution' section above, is sufficient to meet the national requirement of 297 PSUs.

6.36. To command PSUs to respond to public order incidents, PSU commanders must be trained to nationally agreed standards and accredited as operationally competent.[85] There are three levels of command for public order – gold, silver and bronze. A new public order command course has been introduced,

[84] Evidence obtained by HMIC's inspection of undercover policing, which reports May 2014

[85] APP on public order command, which can be found here: http://www.app.college.police.uk/app-content/public-order/command/#accreditation-of-commanders

incorporating the new 'going- forward' tactics that were introduced after the 2011 disorder.

6.37. There is no national requirement for the number of public order trained commanders in the same way as there is for PSUs. Forces decide on this number. Current practice dictates, therefore, that commanders should be appointed to the incident from the force, based on the location of the incident. In forces that collaborate to provide PSUs, any commander from within the collaborating forces can be appointed. The theory is that, provided forces maintain sufficient levels of accredited commanders, the management of incidents can be allocated to suitably trained and experienced officers.

6.38. Our analysis of the data returned by forces indicated that sufficient levels of accredited public order trained commanders to provide cover during widespread disorder were not always in place. For example, three forces had only one trained and accredited gold commander each. These forces were at risk of not having the necessary command capability should a public order incident occur. This would require them to request assistance from other forces. There is not, at present, a formal agreement as to how this would work in practice. The issue is being considered by the national policing lead for public order; one option is to create a pool of public order commanders for forces to call on when necessary. This would also provide opportunities for forces to collaborate on providing public order commanders.

6.39. We found that the national policing lead for public order and the senior leaders across the service have a sound understanding of national capabilities to respond to public order threats and know what needs to be done to develop and maintain capability. This understanding was recently assisted by the completion, by all 43 forces, of a self-assessment of their public order capability – a worthwhile piece of work commissioned by the national policing lead and organised by the College of Policing. It found that, on average, 85 percent of the ten capabilities[86] required for public order policing were being

[86] *Public Order Framework Overview v1.2*, College of Policing, March 2013

met. This compares favourably with other specialist areas of policing that have been self-assessed, where the average is between 75 to 80 percent.[87]

6.40. In the 18 forces we visited, we checked the public order equipment they used in their PSUs. In all cases the equipment was present. However, we found that different specifications meant that the equipment was not always compatible for use with equipment from other forces. In the Consistency section below, we examine in more detail the issues concerning interoperability and procurement of public order equipment.

6.41. The SPR says *"...The police service should maintain a clear understanding of the location and availability of specialist policing assets in order to maintain the capability at very short notice to mobilise and conduct mutual support across boundaries..."*[88]

6.42. National mobilisation and maintaining an understanding of the location and availability of specialist public order assets is the role of the NPoCC. We interviewed the senior officers and operational staff of the NPoCC to assess the unit's capability, and we inspected the data held on its IT system (Mercury) to check it had sufficient information to carry out its role. We found that the unit had sufficient information for leaders to understand what resources were available to deal with public order problems and had in place a system to mobilise the resources.

6.43. All forces must be able to mobilise PSUs at very short notice to respond to outbreaks of disorder in their force area or, if requested, to assist in another force's area. As part of the fieldwork in the 18 forces, HMIC tested arrangements in place to respond to outbreaks of public disorder. We did this by sitting with control room supervisors as they responded to a theoretical scenario, set by HMIC, of escalating disorder. Forces were not told in advance of our plans to conduct this test. In six of the 18 forces,[89] control room staff demonstrated effective processes to respond to the scenario given in the test.

[87] College of Policing analysis presented to HMIC, 15 November 2013.
[88] SPR paragraph 4.2
[89] Avon and Somerset, Cambridgeshire, Leicestershire, Nottinghamshire, West Midlands and Wiltshire

In the other 12 forces, there were problems in one or more of the following areas: a lack of access to the information the control room supervisors needed to provide an effective response, such as who was public order-trained and to what level; unacceptable delays due to the time taken to identify who was available with the right skills to mobilise; and over-reliance on operations planning departments that were only open during office hours, Monday to Friday, to contact staff.

6.44. In each case, the control room supervisors were asked about the training they had undertaken. None had received specific public order mobilisation training. Some had taken part in mobilisation exercises and most had learnt from working with experienced colleagues.

6.45. We found that the successful mobilisation of public order-trained officers was reliant on the control room supervisors understanding their roles and having immediate access to the information they need 24 hours a day, 7 days a week. The *Police National Public Order Mobilisation Plan* (PNPOMP)[90] stipulates how quickly PSUs should be mobilised[91] and this plan is regularly tested by the NPoCC. However, we found that the plan did not specify what the term 'mobilised' actually meant in practice and this led to forces interpreting what it meant differently. A revised plan clarifying the term 'mobilised' has been prepared but not yet issued to police forces. These different interpretations raise doubts about the usefulness of comparisons that have been made between forces about how fast they were able to mobilise.

6.46. HMIC analysed the results of the six[92] national mobilisation exercises co-ordinated by the NPoCC between December 2012 and November 2013. In half of them, the PNPOMP target of 10 percent of the national PSU requirement for mutual aid to be mobilised within 1 hour was not met. In one region, the target of 10 percent took 1 hour 25 minutes and in another region took 2 hours for the forces to mobilise the necessary PSUs. In the third

[90] The *Police National Public Order Mobilisation Plan,* ACPO, November 2012, paragraph 4.2

[91] *Police National Public Order Mobilisation Plan* paragraph 4.2: 10% of national requirement within 1 hour, 40% of national requirement within 4 hours and 60% of national requirement within 8 hours.

[92] The six mobilisation exercises were conducted in the following police regions: London, Wales. South East, East, North East and North West

region, two of the contributing forces were unable to provide any PSUs due to a live operation and the impact of deployment over the previous weekend.

6.47. Some of the people we interviewed proposed that a reason for the failure to meet mobilisation targets was that they were not allowed to use their sirens to travel to the designated locations. It is our view that, given the distances involved in travelling to the designated locations, the use of sirens would not make up the more than 20 minutes that was required. The learning from each exercise was written onto standard templates and when we examined these, we found that they did not always explain why the target was not being met. We would have expected a report to have been made on the performance of each part of the process.

6.48. In conclusion, it is clear that police forces understand the capabilities they are required to have in relation to public order and this was assisted by the fact that all forces had completed the College of Policing capability framework.

6.49. Our checks of public order equipment had mixed results. Although we found that all the forces we inspected had the necessary equipment to police disorder, it was not always compatible with equipment in other forces.

6.50. Training to the curriculum standard for PSUs, and improved command training for gold, silver and bronze commanders in the use of 'go-forward' tactics, has brought about an improved public order command capability compared with that which was in place at the time of the disorder in August 2011. The NPoCC has the capability necessary to manage national mobilisation and maintains an accurate understanding of each force's specialist assets. However, concerns remain that mobilisation targets are not being met by forces.

Large-scale cyber incident

6.51. The capabilities listed within the SPR that apply directly to the cyber threat are to "*identify and understand threats, risks and harms and ensure a proportionate and effective response*"[93] and "*conduct complex investigations*

[93] SPR paragraph 4.1

(including proactive or cyber investigations) – including the capability to do so across force boundaries".[94]

6.52. Academic research,[95] interviews with senior officials and our review of Action Fraud and the National Fraud Intelligence Bureau[96] provided evidence that cybercrime is significantly under-reported.

6.53. Several reasons were cited which included:

- not perceiving that what had taken place was a crime (or worth reporting);
- not knowing where to report it to;
- believing that the police cannot do anything; and
- individuals not realising that they were actually a victim.[97]

6.54. Only 20 percent of crime reports received by Action Fraud during the first three quarters of 2013/14 were passed to police forces.[98] Financial institutions do not always report crimes committed against their customers because they are concerned about customers' losing their confidence in the security of the institutions' computer systems. This makes it difficult for police forces to effectively identify and understand threats, risks and harm posed by cybercrime as they do not have all of the necessary information they need.

6.55. Cyber threats were first highlighted within the 2010 *National Security Strategy*[99] and have been described in a number of subsequent reports.[100] Police forces' skills to respond to cybercrime have been limited to the training

---

[94] Op cit

[95] *UK Cybercrime Report* 2009, Fafinski and Minassian: Garlik–Invenio Research, September 2009

[96] The National Fraud Intelligence Bureau identifies serial fraudsters, organised crime gangs and emerging and established crime threats by analysing millions of reports of fraud: http://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/nfib/Pages/default.aspx

[97] *UK Cybercrime Report* 2009, Fafinski and Minassian: Garlik–Invenio Research, September 2009.

[98] National Fraud Intelligence Bureau throughput statistics: 9 months to 31 December 2013.

[99] *A Strong Britain in an Age of Uncertainty - The National Security Strategy,* HM Government, October 2010, Cmnd 7953, paragraph 3.27

[100] Examples include the *National Security Risk Assessment*, the *National Cyber Security Strategy* 2011, the *National Policing Requirement* 2012 and the *Serious and Organised Crime Strategy* 2013.

of certain specialists, as described within the 'Capacity and contribution' section above.

6.56. During the past year, police leaders have started to take steps to improve the skills of police staff to deal with cyber threats. The College of Policing has developed a capability framework against which forces will be able to assess their progress in establishing resources, practices, processes and skills to tackle cybercrime. It was issued to chief constables on 17 February 2014.

6.57. With the intention of improving the police service's understanding of cybercrime, the National Cyber Capabilities Programme is working with the College of Policing to review and improve cybercrime training by embedding it in various forms of police learning.

6.58. Eight e-learning packages have been produced, aimed at increasing awareness of cybercrime at all levels from new recruits through to detectives. In January 2014, the Chief Constables' Council agreed that the completion of the e-learning packages would be mandated for all designated staff.

6.59. Data showing the numbers of staff from each police force signing in to receive the training was provided to HMIC by the College of Policing. We found that, for the four e-learning packages aimed at raising the awareness and skills of all staff[101], the uptake was disappointing low. The highest uptake percentages were 7.1 percent in Dyfed-Powys and 6.6 percent in Dorset.

6.60. Data for the four e-learning packages targeted at investigators[102] indicated that uptake was varied. Five forces: Derbyshire; Dyfed-Powys; Leicestershire; Northamptonshire; and West Midlands each had over 25 percent of the workforce signing in to at least one of these four courses. The average take-up for all eight e-learning packages in 37 forces was less than two percent of staff. Detailed information about police forces' commitment to these e-learning packages will be included within the HMIC report of national police responses

[101] Digital communications, cybercrime, social media and policing; Cybercrime and digital policing - an introduction; Cybercrime and digital policing, first responder; and Cybercrime and Digital Policing - investigation.

[102] Introduction to communications data and cybercrime; Communications data in investigations; Communications data - introduction to the internet; and Communications data and cybercrime - introduction to law and procedure.

to cyber threats, to be published later this year as part of the SPR series of reports.

6.61. In addition to training opportunities, at least three police forces were aiming to improve their access to specialist information communication technology skills by entering into partnerships with universities. Police forces were also considering a further range of measures, including targeted recruitment and seeking the assistance of appropriately skilled volunteers to help them improve their skills in tackling cyber threats.

6.62. A National Cyber Capabilities Programme assessment of capabilities described low level of skills in the regions to deliver their remit and a very low level of capability in local forces. The assessment proposed that, where a number of crime allegations are found to be linked, or where activity crosses several force boundaries, the ROCU Cyber Crime Units will co-ordinate investigations and provide expertise for local forces. Forces may also be required to support complex national or regional-level investigations.

6.63. Although this demonstrates a commitment by the leadership of the relevant bodies to establish appropriate levels of capability in each region, this was not in place in all regions during the inspection.

6.64. In conclusion, police forces are not yet able to effectively identify or understand the threat, risk and harm posed by cybercrime. The SPR itself recognised that, as this is the newest of the national threats, there is much more to be done to understand it across all of the agencies involved. It is also a threat that suffers from significant under-reporting by businesses and the public. We were impressed by the recent joint work by the Home Office, police and the NCA, which aims to improve how the threat is understood so that the strategy for the police and other law enforcement agencies can be made much clearer. However, as we describe above, there has been disappointingly poor take-up of the training available to forces, with only a few of them demonstrating a real commitment to improve the skills of their staff to tackle cybercrime.

Recommendations in relation to capability

The College of Policing should work with chief constables to establish and specify the capabilities necessary (in a capability framework) for forces to use to assess whether or not they have the required capabilities to respond to the threat of terrorism. This should be completed within a year.

Chief constables should regularly, at least every two years, complete the College of Policing's capability frameworks to help them assess whether or not they have the capabilities necessary to respond to the national threats.

Chief constables should work with the College of Policing to establish formal guidance to forces about how they should mobilise public order commanders between forces. This should be done within three months.

Chief constables should agree, and then use a definition that specifies exactly what the term 'mobilised' means in relation to the testing of the police response required by the *Police National Public Order Mobilisation Plan*. This should be done within three months.

Chief constables should provide those whose duty it is to call out public order trained staff with the information they need, 24 hours a day, seven days a week, so that they can mobilise the required number of PSUs within the timescales set out in the *Police National Public Order Mobilisation Plan.*

7. Consistency

7.1. The SPR describes consistency as:

- *"...the requirement for certain key specialist policing capabilities to be delivered in a consistent way across all police forces or, in some cases, with other partners such as other 'blue light' emergency services or national agencies."*[103]

7.2. The SPR states that:

- *"Chief constables and police and crime commissioners must have regard to the need for consistency in the way that their forces specify, procure, implement and operate in respect of the following policing functions* [later referred to as the 'key functions']*:*
  - *Public order;*
  - *Police use of firearms;*
  - *Surveillance;*
  - *Technical surveillance; and*
  - *Chemical, Biological, Radioactive and Nuclear (CBRN) incidents."*[104]

7.3. The SPR adds that:

- *"These are the areas of policing in which the need for consistency (or as a basis for 'interoperability') has been adjudged to be the most critical, at this time, by the Association of Chief Police Officers. Consideration should also be given to developing functions such as cyber. This consistency should be reflected in common standards of operating and*

[103] SPR introduction to section 5
[104] SPR paragraph 5.1

leadership disciplines, acknowledged by the Police Professional Body from 2013."[105]

7.4. As we describe in the 'Roles and responsibilities' section, the College of Policing is the police professional body. The College of Policing helps the police bring about consistency by: creating APP; accrediting training providers; developing learning outcomes within a standardised national framework; and identifying and promoting good practice based on evidence of what is effective.

7.5. The SPR states that:

- *"Consistency requires police forces to be able to operate effectively together, for example, in ensuring officers can operate to acknowledged standards to 'go forward' and restore peace using a graduated range of tactics."*[106]

7.6. In this year's inspection, we examined consistency in forces in relation to public order and CBRN. We will cover in detail the remaining 'key functions' in future inspection reports in the SPR series.

Public order

7.7. Standards for policing tactics in response to large-scale disorder were originally published in the ACPO *Manual of Guidance on Keeping the Peace*. This has recently been superseded by the APP on public order.

7.8. HMIC found consistency of professional practice was generally good in relation to public order and was strongest in regions where PSUs from the various forces trained together. This was the case within the South West region, where ground commanders trained, exercised and were deployed with PSUs from other forces. We found similar evidence in the West Midlands region and in the collaborative arrangements between Bedfordshire, Cambridgeshire and Hertfordshire.

[105] SPR paragraph 5.2
[106] SPR paragraph 5.3

7.9. Apart from in a small number of forces, we found that the same public order tactics were being trained and used. The ability of forces to work together is improving as a result of joint training, exercising and deployment. However, interviewees in one force suggested that apparently minor differences in training and practice between forces can create uncertainty among officers on the ground; for example, where the oral commands used by commanders from one force differed from those used by other forces in the region.

7.10. To maintain consistent equipment between forces, ministers have made regulations to specify framework arrangements through which certain types of equipment must be procured.[107] This means that police forces must use nationally established frameworks with contractors to buy certain types of equipment. Currently, national frameworks exist for body armour, police vehicles and IT (commoditised hardware and off-the-shelf software). HMIC found that the national frameworks did not specifically take into account the requirements made about procurement in the SPR. A 2013 National Audit Office report found that police forces procured protective shields (used in disorder situations) to 16 different specifications.[108]

7.11. Procurement managers emphasised to HMIC that, even if SPR requirements were brought within the scope of the regulations, a significant challenge remains. It was their view that consistency could only be achieved if forces agreed a common specification; in their experience, agreement between forces had proved difficult to secure. HMIC found that forces were trying to address this through the creation of regional forums to help deliver greater consistency in procurement. For example, the Eastern region hosts a regional public order working group where joint equipment purchases are agreed within the relevant procurement framework. In addition, the South West region has developed a regional procurement unit that purchases public order and other equipment for forces in the region.

[107] Section 53(1A) of the Police Act 1996 allows the Home Secretary to make regulations requiring equipment provided or used for police purposes to satisfy such requirements as to design and performance as may be prescribed in the regulations. The Police Act 1996 (Equipment) Regulations 2011, regulation 2 (SI 2011/300) specifies the framework arrangements.
[108] *Police Procurement*, National Audit Office, March 2013, HC 1046, page 24

7.12. In summary, we found consistency was strongest in police regions where PSUs from constituent forces train and exercise together. Joint training and exercising, where the same tactics are used, and the experience of recent joint deployments are improving the ability of forces to work together in public order policing. In relation to procurement, there needs to be better alignment between the regulatory framework for procurement and the procurement requirement in the SPR.

Responding to chemical, biological, radiological and nuclear (CBRN) incidents

7.13. The SPR states that:

- *"Chief constables* [are required] *to fully consider the consistency of their capabilities as part of work to improve interoperability between the police and other 'blue-light' emergency services as well as with other partners, for example in responding to CBRN incidents or other significant emergencies."*[109]

7.14. A national strategy for CBRN was launched by the Government in 2005 and national standards in training, testing and exercising have been co-ordinated centrally by the Police National CBRN Centre, and hosted by the College of Policing.

7.15. Nationally funded and procured equipment has enabled CBRN-trained officers to be fully interoperable with officers from other forces at a regional and national level. There is a national procurement executive group which meets bi-monthly, and there are related meetings on standardisation. Heads of procurement for all forces in England and Wales are invited. Some forces expressed concerns that they are still waiting for central direction in terms of equipment replacement and cost, and also whether this will be provided from central Government or from force budgets. The current review by the OSCT should clarify the position on equipment later this year (2014).

7.16. In CBRN policing, HMIC found that relationships and interoperability with other emergency services, specifically the fire and rescue service, is effective. The

[109] SPR paragraph 5.4

central funding and procurement of CBRN equipment enables CBRN-trained officers from different police forces to be fully interoperable with each other.

Detail of national programmes developing consistency in policing

7.17. There are two national programmes developing consistency in policing. The first of these is the UK Police Interoperability Programme which seeks to achieve consistency in the way police forces operate. Its main objectives are consistent armed police officers' tactics and their interoperability with surveillance and public order officers. Governance of the programme is the responsibility of the national police uniform operations business area and is organised into priorities aligned to the SPR key functions,[110] each led by a chief officer.

7.18. The programme has developed the 'go-forward' tactics for PSUs described earlier in this report. The lack of such tactics was identified as a major weakness in the police response to the August 2011 disorder. The UK Police Interoperability Programme has also delivered improvements in the command and control of high-risk operations. Training for police leaders in positions of command during incidents has been standardised and a model[111] for effective decision-making, applicable during a spontaneous incident or a planned event, has been applied across the police service. HMIC was informed during this inspection that technical support has been improved and there are better communication links at the scenes of incidents.

7.19. The second programme is the Joint Emergency Service Interoperability Programme (JESIP), which was established in 2012. It is funded until October 2014 and is overseen by a Ministerial Oversight Board. It brings together the police, fire and ambulance services with a shared aim to "*improve the ways in which police, fire and ambulance services work together at major and complex*

[110] SPR paragraph 5.1. The 'key functions' are: Public order; Police use of firearms; Surveillance; Technical surveillance; and chemical, biological, radioactive and nuclear (CBRN) incidents. The UK Police Interoperability Programme has added 'operational learning' and 'command and control' to its priorities.

[111] *The Association of Chief Police Officers' National Decision Model*, ACPO, 2012

incidents".[112] JESIP's plans involve 13 areas of work grouped under three headings:

- doctrine – development of joint doctrine, to form the basis for training;
- training – of staff in the blue-light services, based on the joint doctrine; and
- legacy – creation of a framework that will replace the current governance structure after September 2014.

7.20. During this inspection we were told about concerns that some had about the viability of the JESIP training plan and the burden it was placing on forces. However, HMIC also heard positive commentary: interviewees in 3 of the 18 forces recognised some benefits from JESIP such as identifying gaps in training; new training for bronze commanders; and the production of a joint emergency manual.

7.21. The future governance of both the UK Police Interoperability Programme and JESIP is currently under consideration.

Recommendations in relation to consistency

Chief constables should work with the College of Policing to agree and adopt a standard specification for all equipment that is necessary for the police to be able to respond to the national threats.

Once standard specifications are in place, the Home Office should support national procurement arrangements and, if police forces do not adopt them, mandate their use through regulation.

[112] See: http://www.jesip.org.uk/about

8. Connectivity

8.1. This section sets out HMIC's findings in relation to how well forces connect locally, regionally, nationally and with national agencies to deliver an integrated and comprehensive policing response to each of the national threats. The requirement for connectivity cuts across the police response to all of the national threats and we have reflected this in the way we report our findings here.

8.2. The SPR states that:

- *"In response to the threats from terrorism, cyber and organised crime, chief constables must have regard to the requirement for resources to be connected together locally, between forces, and nationally (including with national agencies) in order to deliver an integrated and comprehensive response. This should include the ability to communicate securely, access intelligence mechanisms relevant to the threat and link effectively with national co-ordinating mechanisms."*[113]

"An integrated and comprehensive response"[114]

8.3. Interviews with senior managers suggested that there were effective arrangements for connecting up resources to tackle organised crime groups assessed as causing the most harm. There were clear links between forces' co-ordination of resources and those of ROCUs. However, we found that arrangements were less effective when crime threats did not easily fit within force and regional geographic boundaries.

8.4. An example of this is Operation Shrewd which is summarised below.

[113] SPR paragraph 6.1
[114] Op cit

Case study – Operation Shrewd

- In 2012, following the theft of valuable artefacts in a spate of burglaries at museums across England and Northern Ireland, the national policing lead recognised that a new organised crime threat was emerging. Approximately 21 crimes had been committed in 14 police force areas, with losses estimated to be well in excess of £50m. Many of the artefacts were from China and the crimes led to significant national interest. All chief constables agreed 'in principle' to support the investigation.

- However, without a framework or authority to compel forces to co-operate, all forces were asked to contribute £5,000 towards the cost of the investigation. Five forces declined. In light of this, a smaller number of forces and the Home Office were asked and they provided resources.

- The investigation had some success but the lack of resources and funding were believed to have delayed progress and caused evidential opportunities to be missed.

"To communicate securely"[115]

8.5. In addition to automated phone-dialling arrangements in police control rooms that connect neighbouring forces and emergency service partners, forces make extensive use of a nationally connected secure radio network known as 'Airwave'.

8.6. This has been used by the police and other emergency services for communication since 2001.

8.7. Interviewees reported that the 'Airwave' system was, on the whole, effective and it has been extensively tested in real-life and exercise scenarios. HMIC heard a range of examples of it being used effectively and these included:

- London Olympic and Paralympic Games 2012;

[115] Op cit

- Northern Ireland – in a large-scale policing operation for a G8 Summit, the "Airwave'' system worked effectively on the different communication network used by the Police Service of Northern Ireland;

- Eastern Region Specialist Operations Unit – in an exercise testing interoperability between communications equipment in vehicles and aircraft;

- Avon and Somerset – during the Glastonbury Festival and in a joint policing operation concerned with the badger cull; and

- Humberside – during a deployment into another police force area to support a large-scale policing operation concerned with a protest march.

8.8. However, there were problems in some locations, often determined by geography, obstruction or interference. Interviewees reported that a concentration of both users and high volumes of radio traffic can challenge the network's capacity. Examples of this were:

- Sussex Police – in a policing operation to maintain public safety during protests against a commercial drilling venture; and

- Metropolitan Police – New Year's Eve and Notting Hill Carnival.

8.9. An even more secure form of communication is available for covert operations requiring the deployment of surveillance, armed police operations and other forms of specialist support. Covert operations are typically required to counter the threats from terrorism and organised crime. Secure communication services available to the police (and other law enforcement agencies) employ high standards of encryption.

8.10. From interviews with officers and staff, it was apparent that the 'Airwave' system does not present any barriers to interoperability between the blue-light services – but the different ways in which each service uses it do. While the police rely heavily on 'Airwave' for voice transmission, the ambulance service tends to use 'Airwave' mainly for data transmission and the fire and rescue

service, while making some use of 'Airwave', tends to rely on other communication technology at the scene of incidents.

8.11. The Emergency Services Mobile Communication Programme (ESMCP) is intended to replace the 'Airwave' service with a new national mobile communication service for all three emergency services and other organisations that currently use 'Airwave'.[116] It is presently scheduled to be operational by September 2016. Between now and then, there are opportunities for the police and other users to align operational procedures and influence the design and delivery of the new service.

8.12. Other forms of secure communication are in use. The network of CTUs is connected via a system that enables the most sensitive information to be discussed openly in audio and video-conferencing. A confidential intelligence system is also in place connecting CTUs and police force SB offices.

8.13. To conclude, we found that, with the exception of a number of small problems, the 'Airwave' system was effective. However, there were still problems with connectivity between the emergency services caused by each organisation still using different working practices – even after they had committed to improving interoperability through the Joint Emergency Services Interoperability Programme.

"Accessing intelligence mechanisms relevant to the threat"[117]

8.14. The Police National Database (PND) was introduced in response to the findings and recommendations of the *Bichard Inquiry*.[118] The database provides a national platform to share police intelligence and information. Our interviews indicated that forces used PND differently and that there was variation in how well forces kept the intelligence on the database up to date. Some interviewees told us that this was improving. HMIC is inspecting

[116] See https://www.gov.uk/government/publications/the-emergency-services-mobile-communications-programme

[117] SPR paragraph 6.1

[117] The Bichard Inquiry reviewed the circumstances leading to the murder of Holly Wells and Jessica Chapman by Ian Huntley, about whom police forces had information but systems hindered the sharing of intelligence. See the *Bichard Inquiry Report*, HMSO, and June 2004.

information management and its wider effects on the PND separately, as part of the *Building the Picture – Information Management* inspection.

8.15. Intelligence generated by the police, NCA and other national agencies engaged in the fight against terrorism, cyber and organised crime is held on various disparate systems by each of the organisations concerned. Systems that the police rely on for routine business – such as command and control, crime recording, custody, intelligence and case preparation – are not well-connected across the 43 forces. HMIC has previously highlighted the difficulties this creates.[119] These systems all contain potentially valuable items of intelligence that remain difficult for investigators to connect together.

8.16. Depending on the level of sensitivity surrounding each item of intelligence and its source, restrictions are applied to protect the intelligence. The overarching framework that governs this process is called the Government Security Classifications (GSC), which sets three levels of classification:Top Secret, Secret and Official.[120] The effect of these classifications is to control carefully the extent to which intelligence can be shared.

8.17. HMIC found that police forces are developing 'confidential units' as part of a programme to increase ROCU capabilities.[121] These units, operating to particularly high standards, provide the necessary connectivity between police force intelligence systems, the NCA systems and those of the CTU. The 'confidential units' will have the necessary infrastructure and security arrangements in place to enable them to handle such material and share it across units working at different GSC levels. A Home Office-led Confidential Unit Operating Model programme is underway to standardise and improve the way 'confidential units' function across England and Wales. It is enabling 'confidential units' to make use of the same secure communications technology as employed in CTUs. Our inspection found that significant levels of investment were involved in providing the encrypted IT systems and

[119] *Mistakes were made: HMIC's review into allegations and intelligence material concerning Jimmy Savile between 1964 and 2012*, HMIC, March 2013, chapter 8.
[120] See https://www.gov.uk/government/publications/government-security-classifications
[121] *Serious and Organised Crime Strategy*, HM Government, October 2013, Cmnd 8715, paragraph 4.11

necessarily high security standards required by the Confidential Unit Operating Model. In all regions the needs of its constituent forces could be met by one confidential unit, usually located within the ROCU, working on their behalf. HMIC encourages all regions to adopt this model.

8.18. HMIC also found that, when people at serious risk of retribution from violent criminals have to move from one region to another, case files concerning their safety and security have to be physically transferred between ROCUs as there is no integrated IT system to connect across force boundaries.

8.19. HMIC concluded that progress towards improved connectivity is evident and that when 'confidential units' are fully functional, police forces and ROCUs should find it easier to share sensitive intelligence. That said, the structures, systems and processes in place during our inspection were not yet fully effective for safe and effective intelligence-sharing.

"Police co-ordination arrangements for countering terrorism"[122]

8.20. The SPR states:

- *"Chief constables must have regard to the role of the Security Service and the national police co-ordination arrangements for countering terrorism. These include the regionally located assets, role of the senior national co-ordinator and the national co-ordination centre, and co-ordination mechanisms for the allocation of Security Service and police assets for countering terrorism."*[123]

8.21. These arrangements, most of which are under national rather than local control, will be explored in more detail in a future inspection of counter-terrorism, which will form part of the SPR series of inspections. There is evident connectivity within the CT network and between the network and forces.

[122] SPR paragraph 6.2
[123] Op cit

The "Co-operation with tasking arrangements led by the National Crime Agency"[124]

8.22. SPR states that:

- *"From the point of its introduction chief constables must co-operate with the national co-ordination and tasking arrangements led by the National Crime Agency (2013) in accordance with the provisions for co-operation, tasking and assistance that will be provided for by the NCA's legislation."*[125]

8.23. The NCA has introduced new national co-ordination and tasking arrangements. These align with and build on the previous police-led regional arrangements, which were described to HMIC as generally effective.

8.24. The arrangements include:

- daily briefing meetings (chaired by an NCA senior officer and conducted using telephone conferencing);
- four-weekly regional tactical tasking meetings (chaired by a regionally nominated chief police officer);
- eight-weekly national tasking meetings (chaired by the NCA Deputy Director General, and which participants attend in person); and
- six-monthly national strategic tasking meetings (chaired by the NCA Director General, and also attended in person).

8.25. HMIC found that, appropriately through the ROCUs, forces are actively participating in the national tasking arrangements. Managers (usually at detective inspector level) routinely dialled in for the daily meeting, which was described by some respondents as an effective way of identifying emerging crime problems. An example of this was the occasion when, at one of the daily briefing meetings, it became apparent that an incident highlighted by the West

[124] SPR paragraph 6.3
[125] Op cit

Midlands ROCU was linked to an incident of interest to the Yorkshire and Humber ROCU. Managers who took part in the tasking process described it as relevant, useful, easy to use and efficiently run. They were supportive of this process.

8.26. At the time of our fieldwork, two strategic tasking meetings had taken place, and, together with the tactical meetings, had been attended by the appropriate chief police officers and other law enforcement partners. We were impressed to find that the police, the NCA and other national agencies were working collaboratively to continue to develop these arrangements. For example, planned improvements to the way the national strategic threat assessment for organised crime is used to inform the tasking process.

8.27. HMIC also interviewed NCA regional organised crime co-ordinators (senior NCA managers who work closely with ROCUs) and leaders in the ROCUs. They reported positive engagement by both sides, which had led to good outcomes. One example was when the South East ROCU had acted on intelligence obtained via the NCA's international connections, disrupting the illicit production of amphetamine in the Thames Valley area. Another example was when the NCA's behavioural science team provided specialist advice on how to tackle a persistent organised crime group committing offences in Hampshire and Surrey.

8.28. In regions such as the East Midlands, Wales and the North West, plans have been agreed to co-locate entire police and NCA teams in shared buildings. HMIC considers that these arrangements are likely to result in material improvements in co-operation and assistance.

8.29. At the time of our inspection, the Director General of the NCA had not made use of his power to direct a chief officer of an England and Wales police force[126] and there was evidence of a constructive co-operation between him and chief constables in relation to the new tasking arrangements.

[126] section 5(5) of the Crime and Courts Act 2013

"Cross-boundary mobilisation"[127]

8.30. The inspection also focused on the cross-boundary mobilisation of force resources.

8.31. The SPR states:

- *"In response to incidents of public disorder, large-scale public protests and civil emergencies, chief constables must co-operate with arrangements that enable the effective cross-boundary mobilisation of force resources."*[128]

8.32. In August 2011, England and Wales experienced significant disorder across a number of towns and cities. The problems encountered by the mobilisation of the police response at that time led to the creation of the NPoCC, which was launched in April 2013. The NPoCC has various roles, which are to: support forces in responding to large-scale events; mobilise force resources effectively in emergencies; and co-ordinate and prioritise resources for police forces, while supporting senior officers and government crisis management structures.[129]

8.33. HMIC found that all forces were working with the NPoCC through a network of co-ordinators in regional units known as regional information co-ordination centres (RICCs). Of the nine police regions, six had functioning RICCs.[130] Where RICCs were not yet in place, police forces dealt directly with the NPoCC to request and supply resources. Forces routinely transferred information and communicated with the NPoCC, using a bespoke computer system called Mercury.

8.34. Interviewees in various roles described a co-operative relationship with the NPoCC, which resulted in effective mobilisation of resources at times of need. Our interviews revealed that requests for mobilisation were usually

[127] SPR paragraph 6.4
[128] Op cit
[129] See http://www.acpo.police.uk/NationalPolicing/NPoCC/home.aspx
[130] Exceptions are London, Wales and the North East

successfully met through negotiation between the NPoCC and the forces supplying resources, facilitated through the RICCs.

8.35. As we described in the 'Capability' section, the NPoCC also co-ordinates a programme of mobilisation exercises undertaken by police forces and regions. These exercises enable the centre to understand the availability of resources and how quickly they can be deployed to respond to incidents.

8.36. Taken together, our findings lead us to conclude that chief constables are co-operating with the arrangements for cross-boundary mobilisation.

Recommendations in relation to connectivity

Chief constables should demonstrate their commitment to the objectives of the Joint Emergency Services Interoperability Programme by, wherever practicable, aligning their operational procedures with those of the other emergency services.

Chief constables and the Director General of the NCA should prioritise the delivery of an integrated approach to sharing and using intelligence.

9. Conclusion

9.1. The availability of dedicated SPR-related resources, maintained since the SPR's publication, provided evidence that chief constables were having regard to the SPR requirements for **capacity**. That said, we were struck by how incomplete the police service's understanding of the national threats was. This, and the limited evidence of any efforts to link decisions on levels of resourcing to a detailed understanding of threats, led us to conclude that much greater attention is necessary from many police leaders to understand this area more fully.

9.2. We also concluded that the discipline of linking strategic threat and risk assessments to decision-making was very weak and needs to be strengthened by the police service as it continues to respond to the demands of austerity-related budget settlements. Our recommendations include regular production of strategic threat and risk assessments for all the national threats to help make resourcing decisions.

9.3. The evidence of agreements between chief constables for the **contribution** that is expected of them was persuasive in two areas in particular: the national and regional arrangements for PSU mobilisation; and the regions where strong collaboration arrangements were in place. Among the other national threat areas, and in the regions where there is less collaboration, the evidence was less persuasive. While some requirements for contribution from forces are imposed on chief constables (such as in counter-terrorism) there was little evidence available that would have helped us to conclude that chief constables have all reached agreements about the contribution that is expected of them. Examples such as Operation Shrewd and the uncertainty concerning the *National Policing Requirement* both illustrate this.

9.4. The **capabilities** that we found in place for: counter-terrorism, public order, civil emergencies, and those being built in Regional Organised Crime Units for organised crime, were in stark contrast with the capabilities, largely absent in police forces, for cyber-related threats. It is now essential that police officers have the capability to deal confidently with the cyber element of crimes as it is

fast becoming a dominant method in the commission of crime. But more than that, it is becoming a part of everything that the police have to deal with because the internet and digital technology are now part of most people's lives. The police must very soon be able to operate just as well in cyberspace as they do currently on the street.

9.5. The Chief Constables' Council and the Professional Committee need to play a much more prominent role in making sure that the police service has the capability to deal with cyber threats. This needs urgent attention as criminals are increasing their use of cyber methods to commit crimes at an increasingly rapid rate.

9.6. The levels of **consistency** we saw in forces were encouraging. The persuasive evidence, which included: national arrangements for counter-terrorism and CBRN; examples of collaboration; joint training; and two worthwhile national programmes, is balanced by the evident difficulties in obtaining consistency in the procurement of equipment and some reservations concerning JESIP's training plan. We concluded that consistency was improving, but was not yet fully developed.

9.7. In terms of **connectivity**, HMIC found mixed evidence. On the one hand, 'Airwave' stands as a clear example of a tried, tested and mostly effective communication system – capable of connecting police forces and their operational partners. Similarly, the NPoCC is effective at helping the police to mobilise across boundaries and indications were that chief constables co-operated with mobilisation arrangements, the NCA's tasking arrangements and the arrangements in place for counter-terrorism.

9.8. On the other hand, we found persuasive evidence that intelligence systems are not yet sufficiently joined up and, even taking account of the worthwhile progress evident in the Confidential Unit Operating Model programme, the police service and its operational partners remained unable to share sensitive intelligence as efficiently and effectively as they should. This inability is increasingly difficult to comprehend, given that the technology is available to enable this.

9.9. Our inspection has led us to conclude that HMIC can provide assurance that chief constables are having regard to the SPR "*when exercising their functions*"[131]. We found that the levels of resources dedicated to the police response to the national threats have not changed appreciably following the publication of the SPR. The total number of posts that were dedicated to responding to the five national threats in England and Wales for 2013/14 was 11,265.

9.10. That said, the capacity and capability of the police to respond to the national threats is stronger in some areas than others – with the police response to the cyber threat being the least well developed. The lack of a clearly articulated approach to the SPR by the collective leadership of the police service in England and Wales was disappointing, especially some 18 months after its publication. During our inspection we found that the *National Policing Requirement* (NPR), which was written by the police to describe how forces should collectively respond to the SPR, was not being used as it was intended. Forces were uncertain about the NPR's currency and value and, as a result, we found very little evidence that it was being used to help them establish a collective and effective response to the national threats.

9.11. Our findings lead us to conclude that chief constables need to immediately establish a collective leadership approach that is committed to securing the required level of preparedness to respond to the national threats - in a way that is consistent across England and Wales.

[131] SPR paragraph 1.11

10. Recommendations

1. Chief constables should, immediately, establish a collective leadership approach that is committed to securing the required level of preparedness to respond to the national threats - in a way that is consistent across England and Wales. This should be done by:

    - re-establishing their commitment to a National Policing Requirement that fully describes the response that chief constables are committed to providing to the tackle the national threats;
    - providing the capacity and capability necessary to contribute to the collective response by all forces to tackle the national threats;
    - monitoring how well forces are fulfilling their obligations to the National Policing Requirement and formally reporting the results to Chief Constables' Council - at least annually;
    - fulfilling their promise[132] to annually review the National Policing Requirement.

Capacity and contribution

2. Chief constables should conduct an evidence-based assessment of the national threats (as described in the SPR), at least annually, and make it part of their arrangements for producing their strategic threat and risk assessments. This should start immediately because it is essential to understand the threat and risks before deciding upon the level of resources that are necessary to respond.

3. Chief constables and PCCs should, as part of their annual resource planning, explicitly take into account their strategic threat and risk assessments when they make decisions about the capacity and capability required to contribute to the national response to those threats. This should start with immediate effect.

[132] *National Policing Requirement*, ACPO, 2012, paragraph 1.3.3

4. Chief constables should work with the College of Policing to create national guidance that describes how forces should establish the number of PSUs they need to respond to their assessment of the local public order threat. This should be completed within six months.

5. Chief constables should work with the Home Office, the National Crime Agency and CERT-UK (following its launch in March 2014) better to understand their roles in preparing for, and tackling the shared threat of a large-scale cyber incident. Their roles should cover the 'pursue, prevent, protect and prepare' themes of the Serious and Organised Crime Strategy.

6. Recognising the fact that both the understanding of the national threats and the police response to them are continually changing, the Home Office should regularly review the SPR to make sure its requirements remain relevant and effective.

Capability

7. The College of Policing should work with chief constables to establish and specify the capabilities necessary (in a capability framework) for forces to use to assess whether or not they have the required capabilities to respond to the threat of terrorism. This should be completed within a year.

8. Chief constables should regularly, at least every two years, complete the College of Policing's capability frameworks to help them assess whether or not they have the capabilities necessary to respond to the national threats.

9. Chief constables should work with the College of Policing to establish formal guidance to forces about how they should mobilise public order commanders between forces. This should be done within three months.

10. Chief constables should agree, and then use a definition that specifies exactly what the term 'mobilised' means in relation to the testing of the police response required by the Police National Public Order Mobilisation Plan. This should be done within three months.

11. Chief constables should provide those whose duty it is to call out public order trained staff with the information they need, 24 hours a day, seven days a week, so that they can mobilise the required number of PSUs within the timescales set out in the Police National Public Order Mobilisation Plan.

Consistency

12. Chief constables should work with the College of Policing to agree and adopt a standard specification for all equipment that is necessary for the police to be able to respond to the national threats.

13. Once standard specifications are in place, the Home Office should support national procurement arrangements and, if police forces do not adopt them, mandate their use through regulation.

Connectivity

14. Chief constables should demonstrate their commitment to the objectives of the Joint Emergency Services Interoperability Programme by, wherever practicable, aligning their operational procedures with the other emergency services.

15. Chief constables and the Director General of the NCA should prioritise the delivery of an integrated approach to sharing and using intelligence.

Annex A - Police forces visited during ‘fieldwork’ for inspection

Avon and Somerset Constabulary

Bedfordshire Police

Cambridgeshire Constabulary

Cheshire Constabulary

City of London Police

Greater Manchester Police

Gwent Police

Hertfordshire Constabulary

Humberside Police

Kent Police

Leicestershire Constabulary

Metropolitan Police

Northumbria Police

Nottinghamshire Police

South Wales Police

Sussex Police

West Midlands Police

Wiltshire Police