HMIC

Inspecting policing
in the public interest

The Strategic Policing Requirement

An inspection of how police forces in England and Wales deal with threats of a large-scale cyber incident (including criminal attack)

ISBN: 978-1-78246-402-0

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

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
instructions which have been approved by the College of Policing for use by the police in the course of their duties; authorised professional practice is available in various subject areas that are relevant to the Strategic Policing Requirement

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

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

CISP
the Cyber Security Information Sharing Partnership is a ‘portal’, managed by the Cabinet Office, where 650 industry and government partners share information about malware directed against their systems

Covert Internet Investigators
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

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

cyber
a term used to indicate that a computer is involved

cyber-crime
describes two criminal activities: cyber-dependent crimes, and cyber-enabled crimes

cyber-dependent
cyber-dependent crimes can only be committed using computers, computer networks or other forms of information communication technology

cyber-enabled	cyber-enabled crimes (such as fraud, the purchasing of illegal drugs and child sexual exploitation) can be conducted on or offline, but online may take place at unprecedented scale and speed
e-learning packages	training courses that are accessed and completed entirely on a computer
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
fieldwork	inspection carried out within police forces at their premises or in their areas
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
ICT	Information and Communication Technology
interoperability	the ability of one force’s systems and procedures to work with those of another force or forces
malware	a computer program designed specifically to damage or disrupt a computer, mobile device, computer systems or computer network and can include programs designed to gain unauthorised access to data held on these devices
National Fraud Intelligence Bureau	the National Fraud Intelligence Bureau identifies serial fraudsters, organised crime gangs and emerging and established crime threats by analysing 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 cyber-crime, and protecting children and young people

National Cyber Capabilities Programme
a programme to develop cyber capabilities in the police service led by the head of the National Cyber Crime Unit, part of the NCA, and the (police) national business area lead for e-crime

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

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

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 cyber-crime; organised crime is characterised by violence or the threat of violence and by the use of bribery and corruption

OCG
organised crime group: a group of people committing organised crime together

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

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

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.

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

Preface

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 so that the police response to all of the national threats can be examined individually and in-depth over that period.

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 the police service has met the requirements of the SPR in relation to the threat of a large-scale cyber incident (including criminal attack).

A report examining 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 was published by HMIC on 10 April 2014. [2] This report contains this year's recommendations about how forces can improve the way they comply with the SPR.

A further report examines how well the police service has met the requirements of the SPR in relation to the threat to public order. [3]

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

[2] *The Strategic Policing Requirement: An inspection of the arrangements that police forces have in place to meet the Strategic Policing Requirement,* HMIC, April 2014. Available from: www.hmic.gov.uk/publication/an-inspection-of-the-arrangements-that-police-forces-have-in-place-to-meet-the-strategic-policing-requirement/

[3] *The Strategic Policing Requirement: An inspection of how police forces in England and Wales deal with threats to public order*, HMIC, June 2014. Available from www.hmic.gov.uk

Summary

The introduction of police and crime commissioners[4] (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[5] 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.

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.

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 (including criminal attack) - the subject of this report.

[4] 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

[5] 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

Part B specifies the policing response that is required nationally, in conjunction with other national agencies, to counter these threats.[6] 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."*[7]

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

HMIC's role and purpose

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*".[8]

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*."[9]

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).*"[10]

Methodology

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 one of a series of reports as to forces' responses to the SPR.

This 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 and in nine regional police units tackling organised crime in January and February 2014. It looks

[8] SPR paragraph 1.15
[9] SPR paragraph 1.11
[10] SPR paragraph 1.9

in-depth at how police forces, individually and collectively, have responded to the SPR in relation to the threat of a large-scale cyber incident (including criminal attack).

A further report also published by HMIC provides a detailed examination of police force response to the threat to public order. [11] HMIC will give more detailed consideration to the other national threats in future years.

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

Findings

Capacity and contribution

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 cyber-crimes or the commission of a single attack. Therefore we believe that the police response should be concerned with both types of incident.

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 cyber-crime are respectively known as cyber-enabled and cyber-dependent crimes.[12]

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 cyber-crime strategies or plans and only 15 forces had considered cyber-crime threats in their Strategic Threat and Risk Assessments (STRA).

[11] *The Strategic Policing Requirement: An inspection of how police forces in England and Wales deal with threats to public order*, HMIC, June 2014. Available from www.hmic.gov.uk

[12] *Serious and Organised Crime Strategy*, Her Majesty's Government, Cmnd 8715, October 2013, paragraph 2.54

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 cyber-crime; 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 [13]provides an opportunity for police forces to incorporate all four themes of 'pursue, prevent, protect and prepare'[14] in future plans and STRAs.

Although we found that the forces we visited had in place dedicated staff that were responsible for the security of their information systems, including protecting them from malware attacks, we found that this was not accompanied with the necessary assessment of the threats and risks that they faced. This means that forces were not using the threat assessment process that they use in relation to the threat that organised criminals present to the public to help them understand the nature and likelihood of the threat these criminals present to themselves. As a result, their approach tended to be a reactive one and did not make enough use of intelligence provided by other organisations that are assessing the cyber threat and could provide information relevant to protecting police information systems from malware. For example, very few forces were engaged with the Cyber Security Information Sharing Partnership (CISP).

The Government and PCCs are increasing their investment in Regional Organised Crime Units (ROCUs) to establish fully the range of capabilities that are necessary to support police 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.

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

[13] *Serious and Organised Crime Strategy*, Her Majesty's Government, Cmnd 8715, October 2013

[14] 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)

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 of a large-scale cyber incident effectively.

Capability

Research shows that cyber-crime is significantly under-reported, and of those crimes reported to Action Fraud[15], just under 18 percent are passed to police forces.[16] This means that police forces do not have sufficient information to identify and understand the threats, risks and harm associated with cyber-crime.

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.

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 new College of Policing framework on capability which forces can use to assess their progress in establishing resources, practices, processes and skills to tackle cyber-crime; 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 cyber-crime. The average take-up for this training in 37 forces was less than two percent of the workforce.

[15] 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

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

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.

Consistency

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). However, there is no APP for cyber-crime at present, but one is in development and planned for publication in the third quarter of 2014.[17]

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. The College has provided accredited training opportunities for forces, but take up was very low indeed whilst at the same time forces were independently procuring specialist training from technology providers or other private contractors. This was not being done in a consistent way across forces and no thought had been given to how the capabilities developed would combine to form part of a national response to the cyber threat.

Connectivity

During our fieldwork, we found no evidence that police forces' high-tech crime investigation capabilities were connected. We discussed with police leaders responsible for forces' cyber-crime capabilities how their staff and equipment could work with those from other forces and the National Cyber Crime Unit (NCCU) in the

[17] College of Policing, Authorised Professional Practice, http://www.app.college.police.uk/

event of a need to respond jointly to a large-scale cyber incident. This scenario had not been considered and there was no plan for it.

“Accessing intelligence mechanisms relevant to the threat”

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.

Intelligence relevant to national threats is held by the police, the NCCU of 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.

HMIC found that police forces are developing what they call ‘confidential units’ as part of a programme to increase ROCU capabilities.[18] Police forces are collaborating to form regional confidential units and a new operating model is being implemented to increase standards of information security and connect police force intelligence systems to the NCCU systems in the NCA. 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 levels.

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.

[18] *Serious and Organised Crime Strategy*, Her Majesty’s Government, Cmnd 8715, October 2013, paragraph 4.11

“Co-operation with tasking arrangements led by the National Crime Agency.”[19]

The NCCU, as part of the NCA has a national responsibility for leading, supporting and coordinating the response to the most serious incidents of cyber-crime. Co-operation with tasking 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.

Conclusions

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*”[20]. However, in relation to the threat of a large scale cyber incident, we are led to conclude that the preparedness of the police is still in the very early stages of development. Our findings confirm what was recognised in the SPR itself: “*the police response to cyber-related threats needs to develop further*”.[21] This is because the rapid development of digital technology and the internet 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.

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.

[19] SPR paragraph 6.3
[20] SPR paragraph 1.11
[21] SPR paragraphs 1.5 and 3.2

Recommendations

All recommendations made as a result of the SPR inspection are contained in the report of HMIC's '*An inspection of the arrangements that police forces have in place to meet the Strategic Policing Requirement*' which is available at www.hmic.gov.uk.

Introduction

This report sets out the findings of an inspection by Her Majesty's Inspectorate of Constabulary (HMIC),[22] which examined how well police forces have met the requirements that the *Strategic Policing Requirement* (SPR) stipulates them to have in place so they can respond to a large-scale cyber incident (including criminal attack).

The introduction of police and crime commissioners[23] (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.

As a result the *Strategic Policing Requirement* (SPR) was published in July 2012.[24] 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.

[22] 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

[23] 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

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

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* [25] *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 cyber-crime, 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."*[26]

[25] 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)

[26] SPR paragraph 2.2

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 cyber-crime. '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.[27]

In this report we only consider the response required to meet "*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".*[28]

Part B specifies the policing response that is required nationally, in concert with other national agencies, to counter these threats.[29] 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;*

[27] These are definitions created by HMIC solely for the purposes of this report. Different definitions exist elsewhere.

[28] SPR paragraph 2.2

[29] SPR paragraph 1.6

- *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."*[30]

This report examines how well police forces have responded to these requirements in relation to a large-scale cyber incident (including criminal attack) 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*." [31]

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*." [32]

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*

[30] SPR paragraph 1.6
[31] SPR paragraph 1.15
[32] SPR paragraph 1.11

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).”[33]

[33] SPR paragraph 1.9

Methodology

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.

This report is one of a series of reports on compliance with the SPR which will be published by Her Majesty's Inspectorate of Constabulary (HMIC). It examines how well the police service has met the requirements of the SPR in relation to the threat of a large-scale cyber incident (including criminal attack).

In addition to assuring the SPR in relation to a large-scale cyber incident, this year's inspection includes an examination of the police response to the threat to public order (also published this year as part of this inspection programme) and an examination of how well police forces have established the arrangements that the SPR requires them to have in place in order to counter all of the national threats referred to in Part A of the SPR. This report has been published by HMIC on 10 April 2014. [34] To undertake this inspection, we requested in July 2013 that the 43 forces of England and Wales 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.

HMIC also conducted fieldwork in 18 forces in England and Wales between September and November 2013 and in nine regional police units tackling organised crime in January and February 2014. We intend to conduct fieldwork in the remaining 25 forces over the next two years. The forces visited are listed in Annex A.

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

[34] *The Strategic Policing Requirement: An inspection of the arrangements that police forces have in place to meet the Strategic Policing Requirement,* HMIC, April 2014. Available from: www.hmic.gov.uk/publication/an-inspection-of-the-arrangements-that-police-forces-have-in-place-to-meet-the-strategic-policing-requirement/

forces, and what we were told during our visits to forces, by physically checking that the arrangements were actually in place.

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.

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

Roles and responsibilities

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.

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.

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.*"[35]

PCCs must "*secure the maintenance of the police force for their areas and ensure that their police forces are efficient and effective*".[36] They must hold chief constables to account for their functions and for the performance of the staff within their forces.

The College of Policing is the professional body for policing. Its core areas of responsibility include *"supporting police forces and other organisations to work together to protect the public and prevent crime".*[37] 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)*".[38] Working with chief constables, the College of Policing creates national standards for professional practice, which are published as Authorised Professional Practice (APP).

[35] s2 Police Reform and Social Responsibility Act 2011
[36] s1 Police Reform and Social Responsibility Act 2011
[37] *Our Strategic Intent*, College of Policing, September 2013, paragraph 1.1
[38] *Professional Committee Terms of Reference*, College of Policing, 11 July 2013, paragraph 1.2

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.

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 cyber-crime); 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.[39]

[39] *Independent review of ACPO*, General Sir Nick Parker KCB, CBE, 14 November 2013

Findings

Capacity and contribution

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.

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*[40] *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."*[41]

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*…" [42]

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*[43] (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 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

[40] Capability is covered separately in its own section of this report

[41] SPR paragraph 3.1

[42] SPR paragraph 3.3

[43] *National Policing Requirement,* ACPO, 2012

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.

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."*[44]

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).

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

These two categories of cyber-crime are respectively known as cyber-enabled and cyber-dependent crimes.[45]

[44] SPR paragraph 3.2

[45] *Serious and Organised Crime Strategy*, Her Majesty's Government, Cmnd 8715, October 2013, paragraph 2.54

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 cyber-crimes 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.

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

Fifteen police forces had considered cyber-crime 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.

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

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.

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 cyber-crime and not on protecting the public and preventing cyber-crime 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 cyber-crime.

The development of new policy for the police response to the cyber threat is overseen by the National Cyber Capabilities Programme (NCCP), which is jointly led by a senior leader from the NCA and the police.[46] 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 cyber-crime. Progress was being made very quickly.

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 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.

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

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

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 cyber-crime. These are generally in the form of 'high-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 'high-tech' crime staff and there were only 43 across the six police forces within the Eastern Region. The Metropolitan Police had approximately 70[47] within its Police Central e-crime Unit (PCeU) and, with its responsibility for policing the capital city and high levels of cyber-crime, will retain significantly larger cyber resources than other forces even after the transfer of some of the force's responsibilities to the NCCU.

Police forces increasingly rely on ICT, whether to respond to calls from the public, co-ordinate responses to major incidents or outbreaks of public disorder, or to investigate serious crimes. They need to ensure their systems are kept secure to prevent the unauthorised disclosure of information, the release of which could be dangerous to individuals and compromise police operations. They must ensure the integrity of the information on their systems to maintain the chain of evidence and the validity of their investigative information. Within this section of the report we consider how well police forces are identifying threats to their ICT systems and we also consider how well police forces are ensuring they take action to protect themselves from these threats to in order to maintain the availability of their systems to continue to conduct their core business.

The *UK* C*yber Security Strategy* identified that nearly two-thirds of critical infrastructure companies report regularly finding malware designed to sabotage their

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

systems,[48] and that there are over 20,000 malicious emails on government networks each month, a thousand of which are deliberately targeted.[49]

Although no police force has suffered an attack that has disabled all of their ICT systems, one force had experienced a major disruption, this led to a 12-hour shutdown of internal systems, caused by an infected memory stick being used. At least two other forces had been subjected to a cyber-attack that disabled their public-facing websites. Assessment tools have been developed that can be used to test the robustness of organisations' processes and systems to minimise their vulnerability to cyber-attacks.[50] Although forces had prepared to respond to the consequences of attacks to their systems, none of the 18 forces visited could produce to us an assessment of the nature and likelihood of the threat they faced.

Five police forces, the Metropolitan, Surrey, Essex, Norfolk and Lancashire forces, are members of the Cyber Security Information Sharing Partnership (CISP) which is now part of CERT-UK. The CISP is a portal where 650 industry and government partners share information about malware[51] directed against their systems. The five forces that were members of CISP had access to a wide range of current information about threats from malware.

Force information security officers, who are responsible for the security of police forces' ICT systems, demonstrated an awareness of risks that their forces faced, and they were aware of the CERT-UK briefings. Forces, directly or through contractors, undertook practical penetration-testing that tested their security measures and took steps to ensure information security.

All of the forces visited had business continuity plans to ensure the delivery of critical services if an attack were to happen. For example, forces had back-up plans for their command, control, and communications systems should they fail due to flooding, electrical or any other failure (this could be caused by a cyber-attack). Whilst forces

[48] McAfee, *Critical infrastructure protection report*, March 2011, cited within the *UK Cyber Security Strategy*

[49] Iain Lobban, Director of Government Communications Headquarters, 2010 also cited within the *UK Cyber Security Strategy*

[50] For example PAS 555: 2013 cyber security risk – governance and management – specification. The British Standards Institution May 2013. ISBN 978 0 580 78755 3

[51] Malware is a term used to describe malicious software designed to damage ICT systems

had not specifically considered the potential impact of a cyber-attack, they were aware of the need to protect their systems and had plans to respond.

In conclusion, our findings confirm what was recognised in the SPR itself: "*the police response to cyber-related threats needs to develop further*". [52] This is because the rapid development of digital technology and the internet has created opportunities for communication that is beyond the majority of 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.

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.

[52] SPR paragraphs 1.5 and 3.2

Capability

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.

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."* [53]

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*

[53] SPR paragraph 4.1

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." [54]

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 cyber-crime, 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.

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*"[55] and "*conduct complex investigations (including proactive or cyber investigations) – including the capability to do so across force boundaries*".[56]

Academic research,[57] interviews with senior officials and our review of Action Fraud and the National Fraud Intelligence Bureau (NFIB)[58], which both deal with all cyber-crime as well as fraud, provided evidence that cyber-crime is significantly under-reported.

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;

[54] SPR paragraph 4.2
[55] SPR paragraph 4.1
[56] Op cit
[57] UK Cybercrime Report 2009, Fafinski and Minassian: Garlik–Invenio Research, September 2009
[58] 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

- individuals not realising that they were actually a victim;[59] and
- some businesses not reporting crime for fear of reputational damage.

During the financial-year 2013/14, just over 785,400 contacts were made with Action Fraud of which 230,845 were recorded as crimes.[60] Information is passed from Action Fraud to the National Fraud Intelligence Bureau (NFIB), which has links to financial institutions and will instigate measures to prevent further fraud being committed.[61] After the NFIB had reviewed the reports, just fewer than 18 percent were sent to police forces for action, whilst an additional two percent of crime reports were sent to other law enforcement agencies.

The decision to send reports to police forces is based on where it is most likely that the crimes will be solved and where offenders are most likely to be found (not necessarily where the victims are located). Reports received by forces from the NFIB are prioritised against other local policing problems. This means they are not always investigated. NFIB received feedback on outcomes from action taken in response to 21 percent of reports of fraud and cyber-crime sent to police forces. It is therefore not known what the outcome was of the other 79 percent of reports sent to police forces.

All other crimes notified to Action Fraud that are not sent as reports to police forces by the NFIB are made available to police forces within a secure database for ‘information’. Forces are not required to take any action in response to this information and there is little indication, from crime information and force strategic assessments, that police forces consider them or use them to inform their assessments of threat, risk and harm.

It is also the case that the NFIB does not receive any feedback from forces about how useful this information has been to them in the prevention and detection of fraud.

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

[60] Data provided by the National Fraud Intelligence Bureau to HMIC 15 May 2014

[61] The National Fraud Intelligence Bureau carries out disruption activity through requests to banks, telephone providers and web domain providers. For financial year 2013/14 a total of 81,520 requests for suspension (82,300 including emails) were made by the NFIB with an estimated potential value of fraud prevented of £305.1m

From October 2013 the NFIB issued quarterly profiles to forces detailing fraud offences committed within their areas, which included cyber-enabled fraud. In January 2014 the NFIB extended this process to include profiles of all cyber-crime. HMIC see this as a potentially useful initiative that, if the information is used, should help forces to understand the impact of fraud and cyber-crime within their areas.

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 cyber-crime as they do not have all of the necessary information they need.

Cyber threats were first highlighted within the 2010 *National Security Strategy*[62] and have been described in a number of subsequent reports.[63] Police forces' skills to respond to cyber-crime have been limited to the training of certain specialists, as described within the 'capacity and contribution' section above.

During the past year, police leaders have started to take steps to improve the skills of their workforce 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 cyber-crime. It was issued to chief constables on 17 February 2014.

With the intention of improving the police service's understanding of cyber-crime, the NCCP is working with the College of Policing to review and improve cyber-crime training by embedding it in various forms of police learning.

Eight e-learning packages have been produced; four aimed at increasing awareness of cyber-crime for all police staff; the other four aimed at increasing awareness of cyber-crime among police staff whose role it is to investigate crime. In January 2014, the Chief Constables' Council agreed that the completion of the e-learning packages would be mandatory for all designated staff.

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

[63] 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

Four of the eight e-learning packages are for all police officers and staff dealing with the reporting of crime:

1. Digital communications, social media, cyber-crime and policing;
2. Cyber-crime and digital policing - an Introduction;[64]
3. Cyber-crime and digital policing - first responder training;[65]and
4. Cyber-crime and digital policing - Investigation.[66]

Four of the eight e-learning packages are for police officers and staff responsible for investigating crime:

5. Communications Data in Investigations;
6. Introduction to Communications Data and Cyber-crime
7. Communications Data – introduction to the Internet; and
8. Communications Data and Cyber-crime – Introduction to Law and Procedure.

A full description of these e-learning packages can be found in Annex B

E-learning packages are training courses that are completed on a computer. To start the training an individual 'signs in' to the e-learning package and a record of this is kept by the College of Policing. The College provided us with the number of staff from each police force who had 'signed in' to receive the e-learning up to December 2013.

Table 1 displays the percentage of police officers and staff in each force who had 'signed in' to receive the e-learning. High rates of 'signing-in' are highlighted in bold green text.

[64] E-learning package available from 1 August 2013
[65] E-learning package available from 3 September 2013
[66] E-learning package available from 14 October 2013

	For all workforce				For workforce involved in cyber-investigations				Average uptake across the eight packages
	Digital Communications, Social Media, Cybercrime and Policing	Cybercrime and Digital Policing - Introduction	Cybercrime and Digital Policing – First Responder	Cybercrime and Digital Policing - Investigation	Communications Data in Investigations	Introduction to Communications Data and Cybercrime	Communications Data - Introduction to Internet	Communications Data and Cybercrime - Introduction to Law and Procedure	
Dyfed-Powys	**25.1%**	**32.9%**	**28.2%**	5.4%	**7.1%**	2.5%	**6.3%**	0.6%	**13.5%**
Leicestershire	1.4%	**37.5%**	**32.0%**	**27.4%**	0.9%	1.1%	0.9%	0.3%	**12.7%**
Lincolnshire	4.7%	17.4%	16.7%	12.7%	2.9%	2.3%	0.5%	0.4%	**7.2%**
Northamptonshire	0.5%	**26.7%**	24.8%	1.5%	0.7%	0.8%	0.5%	0.5%	**7.0%**
Derbyshire	**46.3%**	0.3%	0.3%	0.1%	1.4%	3.8%	0.8%	0.4%	**6.7%**
West Midlands	**37.2%**	1.2%	0.4%	0.2%	3.7%	1.4%	1.6%	0.7%	**5.8%**
South Wales	1.0%	2.7%	3.4%	1.6%	1.6%	1.2%	0.7%	0.2%	1.5%
Warwickshire	2.7%	0.2%	0.1%	0.1%	2.7%	3.3%	2.9%	0.2%	1.5%
Gloucestershire	0.6%	0.9%	0.4%	0.2%	3.9%	4.0%	0.6%	0.5%	1.4%
Dorset	0.3%	1.2%	1.1%	0.8%	**6.6%**	0.3%	0.3%	0.1%	1.3%
Cumbria	5.7%	1.7%	1.0%	0.9%	0.6%	0.4%	0.0%	0.0%	1.3%
Durham	1.7%	2.0%	1.3%	1.1%	1.0%	0.8%	1.4%	0.9%	1.3%
North Yorkshire	3.3%	1.6%	1.3%	0.1%	0.6%	1.7%	0.8%	0.2%	1.2%
West Mercia	2.9%	0.6%	0.5%	0.4%	1.3%	2.2%	1.3%	0.3%	1.2%
Staffordshire	1.3%	0.4%	0.2%	0.2%	0.6%	0.8%	2.8%	2.2%	1.1%
Wiltshire	0.3%	0.4%	0.2%	0.0%	3.2%	3.0%	0.3%	0.3%	1.0%
Cambridgeshire	1.4%	0.7%	0.6%	0.5%	0.7%	2.7%	0.6%	0.3%	0.9%
Avon & Somerset	0.8%	0.6%	0.5%	0.2%	2.1%	2.3%	0.8%	0.2%	0.9%
Surrey	3.5%	0.2%	0.1%	0.1%	1.8%	1.0%	0.7%	0.1%	0.9%
Cleveland	1.4%	1.8%	1.3%	0.2%	0.4%	1.1%	0.3%	0.0%	0.8%
West Yorkshire	0.9%	1.1%	0.6%	0.4%	0.5%	1.9%	0.3%	0.3%	0.7%
London, city of	0.5%	3.0%	0.6%	0.1%	0.7%	0.4%	0.2%	0.0%	0.7%
Nottinghamshire	0.3%	0.9%	0.8%	0.6%	1.5%	0.8%	0.4%	0.1%	0.7%
Metropolitan police	1.3%	0.4%	0.3%	0.1%	1.3%	1.2%	0.2%	0.1%	0.6%
Gwent	0.4%	0.4%	0.3%	0.1%	1.6%	1.0%	0.5%	0.4%	0.6%
Devon & Cornwall	1.4%	0.3%	0.3%	0.1%	0.7%	0.5%	0.2%	0.1%	0.4%
Humberside	0.2%	0.0%	0.0%	0.0%	0.4%	1.7%	0.2%	0.9%	0.4%
Bedfordshire	0.4%	0.9%	0.1%	0.1%	0.7%	0.4%	0.4%	0.2%	0.4%
Greater Manchester	0.6%	0.3%	0.1%	0.1%	1.0%	0.8%	0.2%	0.2%	0.4%
South Yorkshire	0.8%	0.1%	0.1%	0.0%	0.6%	1.4%	0.1%	0.1%	0.4%
Essex	1.1%	0.0%	0.0%	0.0%	0.7%	0.8%	0.1%	0.0%	0.3%
Thames Valley	0.7%	0.6%	0.1%	0.0%	0.5%	0.5%	0.1%	0.1%	0.3%
Sussex	0.6%	0.5%	0.4%	0.3%	0.2%	0.2%	0.2%	0.1%	0.3%
Hertfordshire	0.5%	0.5%	0.2%	0.1%	0.3%	0.5%	0.2%	0.1%	0.3%
Suffolk	0.2%	0.0%	0.0%	0.0%	0.9%	1.0%	0.2%	0.0%	0.3%
Hampshire	0.1%	0.1%	0.1%	0.0%	0.6%	0.9%	0.1%	0.1%	0.3%
Cheshire	0.4%	0.2%	0.1%	0.1%	0.3%	0.7%	0.3%	0.1%	0.3%
Lancashire	0.3%	0.3%	0.3%	0.3%	0.1%	0.4%	0.1%	0.1%	0.2%
Kent	0.3%	0.1%	0.1%	0.1%	0.5%	0.6%	0.1%	0.1%	0.2%
Northumbria	0.1%	0.0%	0.1%	0.0%	0.5%	0.6%	0.0%	0.1%	0.2%
North Wales	0.3%	0.1%	0.2%	0.0%	0.1%	0.5%	0.0%	0.0%	0.2%
Merseyside	0.3%	0.1%	0.1%	0.1%	0.2%	0.3%	0.1%	0.1%	0.2%
Norfolk	0.5%	0.0%	0.1%	0.1%	0.2%	0.2%	0.1%	0.0%	0.1%
TOTAL	3.9%	1.9%	1.6%	0.8%	1.2%	1.2%	0.5%	0.2%	1.4%

Table 1: The percentage of police officers and staff in each force who had ‘signed in’ to receive the e-learning.

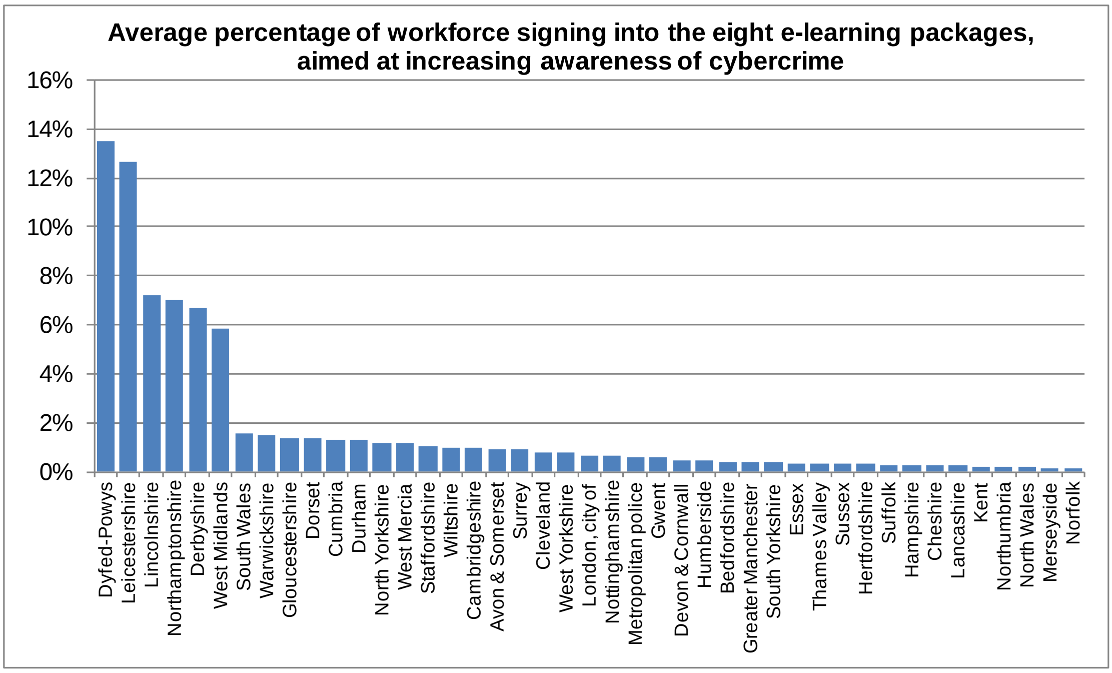

Figure 1: The average percentage of the workforce signing into the eight e-learning packages aimed at increasing awareness of cyber-crime

HMIC recognises that the four e-learning packages for police officers and staff responsible for investigating crimes will attract much lower ‘sign in’ percentages than the four designed for all police officers and staff dealing with the reporting of crime. This is because investigators constitute a much smaller percentage of a police force’s total workforce. Table 1 highlights those forces that have the very highest ‘sign in’ percentages. With the exception of the top six forces, the average ‘sign in’ percentage for all eight e-learning packages is less than two percent as shown in Figure 1. All police forces should ensure that their workforce is capable of: understanding what cyber-crime is when it is reported to them or they discover it; and taking initial steps to investigate cyber-crimes and secure evidence.

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.

A NCCP 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.

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.

The universal availability of digital technology has not only created new and varied opportunities for people to commit crimes but also provides new opportunities to catch criminals. Apart from the use of telephone traffic or other communications information to investigate murders and other serious crimes, there was little indication that police forces were considering how best to harness the opportunities presented by digital technology and the internet to prevent and detect crimes.

Using digital technology to prevent crime and protect the public

Greater Manchester Police monitors social media to identify potentially vulnerable people. They have looked at 'open social media profiles', that anyone can access, and found some young teenagers being stalked by paedophiles. This has enabled them to advise potential victims before they are harmed and provide intelligence to target offenders.

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. More than that, it is also 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.

In conclusion, police forces are not yet able to effectively identify or understand the threat, risk and harm posed by cyber-crime. 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 workforce to tackle cyber-crime.

Consistency

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."*[67]

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."*[68]

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 leadership disciplines, acknowledged by the Police Professional Body from 2013."*[69]

[67] SPR introduction to section 5
[68] SPR paragraph 5.1
[69] SPR paragraph 5.2

Police forces need to remain abreast of developments in technology. High-tech crime staff received College of Policing training packages, and all 18 forces visited independently procured specialist training from technology providers or other private contractors. They also buy a range of technology products required to find and store evidence found within the latest ICT.

Our interviews with officials responsible for police procurement and police leaders responsible for their forces' cyber responses all stated that the specifications for training and equipment were formulated on the advice of their own specialists who were performing high-tech examinations in response to crimes.

In the absence of a list of nationally accredited cyber-crime courses from private companies, forces are buying training and IT software and hardware for staff that may not be compatible. Interviews with police forces' cyber-crime staff and managers revealed that no consideration had been given to how they would work with other police forces or the NCCU.

Connectivity

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 a large-scale cyber incident (including criminal attack).

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."*[70]

[70] SPR paragraph 6.1

During our fieldwork, we found no evidence that police forces' high-tech crime investigation capabilities were connected. For example, they did not share data storage facilities nor did they collaborate to tackle particularly large volumes of data in major investigations. We discussed with police leaders responsible for forces' cyber-crime capabilities how their staff and equipment could work with those from other forces, ROCU cyber-crime units and NCCU in the event of a need to respond jointly to a large-scale cyber incident. This scenario had not been considered and there was no plan for it.

"Accessing intelligence mechanisms relevant to the threat"[71]

The Police National Database (PND) was introduced in response to the findings and recommendations of the *Bichard Inquiry*.[72] 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 information management and its wider effects on the PND separately, as part of the *Building the Picture – Information Management* inspection.

Intelligence generated by the police, NCCU of the 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.[73] These systems all contain potentially valuable items of intelligence that remain difficult for investigators to connect together.

[71] SPR paragraph 6.1

[72] 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

[73] *Mistakes were made: HMIC's review into allegations and intelligence material concerning Jimmy Savile between 1964 and 2012*, HMIC, March 2013, chapter 8

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.[74] The effect of these classifications is to control carefully the extent to which intelligence can be shared.

HMIC found that police forces are developing 'confidential units' as part of a programme to increase ROCU capabilities.[75] These units, operating to particularly high standards, provide the necessary connectivity between police force intelligence systems and the NCA systems. 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 counter-terrorism units. Our inspection found that significant levels of investment were involved in providing the encrypted IT systems and 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.

HMIC concluded that progress towards improved connectivity to share intelligence relevant to the threat of a large-scale cyber incident 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.

[74] See https://www.gov.uk/government/publications/government-security-classifications

[75] Serious and Organised Crime Strategy, Her Majesty's Government, Cmnd 8715, October 2013, paragraph 4.11

"Co-operation with tasking arrangements led by the National Crime Agency."[76]

The NCCU, as part of the NCA has a national responsibility for leading, supporting and coordinating the response to the most serious incidents of cyber-crime. We were told that, in the main, serious crimes are reported directly to the NCA and that, such crimes being reported to police forces, they would expect these to be referred to the NCA.

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. The most serious incidents of cyber-crime would be discussed within these co-ordination processes.

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).

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.

The NCA's authority to task and co-ordinate police forces in response to serious crime is provided by the Crime and Courts Act 2013. Since October 2013, the National Crime Agency Director General has had the legal authority to 'direct' chief

[76] SPR paragraph 6.3

officers to perform specified tasks such as deploying police officers to specific investigations or duties. At the time of our inspection, the Director General of the NCA had not made use of this power[77] and there was evidence that there had been constructive co-operation between the director general and chief constables about the new arrangements.

The NCCU's responsibility for leading the national response to cyber-crime has led to clarity in national leadership; the National Cyber Capabilities Programme has identified the need to improve how intelligence is collected from industry and how it uses information from CISP to assist police forces to protect their information systems from malware. The programme does not describe how the wider response to cyber threats – 'Prevent', 'Protect' and 'Prepare' – should be taken forward. Without a clear framework, which provides clarity about how an overall response to cyber threats would be coordinated, it is difficult for forces to know how they can connect to the national arrangements.

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

Conclusion

Capacity and contribution

Our findings confirm what was recognised in the SPR itself; that, "*the police response to cyber-related threats needs to develop further*". [78] This is because the rapid development of digital technology and the internet has created opportunities for communication that is beyond the majority of 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.

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.

Capability

Police forces are not yet able to effectively identify or understand the threat, risk and harm posed by cyber-crime. 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 cyber-crime.

[78] SPR paragraphs 1.5 and 3.2

It is now essential that police officers have the capability to deal confidently with the cyber-element of crimes; it is fast becoming a dominant method in the commission of crime. More than that, it is also 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 service must very soon be able to operate just as well in cyberspace as it does on the streets today.

Consistency

The NCCU and the College of Policing have started putting things in place to achieve consistency in the arrangements put in place to respond to this threat. However, there is insufficient understanding by forces of how the arrangements should work and forces have been slow to take up the training that they said were mandatory for their staff.

Connectivity

In terms of **connectivity**, HMIC found mixed evidence. Chief constables co-operated with the NCA's tasking arrangements. 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.

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

Annex B – Description of E-learning Training Courses

Digital communications, social media, cyber-crime and policing

This training helps to develop initial awareness of digital communications technology and its impact on different areas of cyber-crime, social media, law enforcement and policing. Guidance is given on the use of social media and open source information and students learn about cyber-crime. The benefits and risks in the use of social media and open source intelligence are illustrated with real examples.

Cyber-crime and digital policing – an introduction

This basic package will help to develop a general awareness of the types of emerging threats and risks from criminals exploiting modern technology. It will be related to relevant legislation. The training also covers cyber-crime prevention. This is the first of three training packages covering cyber-crime at basic levels. The next two cover the first responder and cyber-crime investigation respectively. A realistic online fraud scenario is used to illustrate key concepts. This e-learning module is designed for all police officers and special constables, and individuals within a law enforcement community.

Cyber-crime and digital policing, first responder

This package contains key information and guidance that helps with handling the first response to cyber-crime incidents. It also covers investigative considerations, including methods which can used to capture digital evidence. This is the second of three packages covering cyber-crime and builds on the training provided by Cyber-crime and digital policing – introduction.

Cyber-crime and digital policing – investigation

This cyber-crime and digital policing package covers the investigative considerations and evidence-handling issues most pertinent to cyber-crime and cyber-enabled crime. Students learn about technology concepts including the internet and World Wide Web, IP addresses and domain names, and e mail headers. The knowledge acquired in this module assists in identifying investigative opportunities when dealing with any crime involving digital devices. The same online fraud scenario is used as in the first two modules to illustrate key concepts.

Introduction to communications data and cyber-crime

This package shows the skills needed for a basic level of understanding of the uses of communications data within law enforcement including guidance on cyber-crime prevention. It also includes a Cyber bullying scenario, and useful resources. It is intended to form a base for later, more advanced, modules and training programmes.

Communications data in investigations

After the introduction, which recaps learning on communication devices and services, the course covers the identification and acquisition of communications data. A story based chapter illustrates how communications data is used in an investigation and the final chapter looks at the presentation of communications data as evidence

Communications data – introduction to the internet

This package provides an introduction to the internet and its associated devices. It is designed for investigators and those in contact with specialist staff who work in the cyber-crime and communications data arenas.

Communications data and cyber-crime – introduction to law and procedure

This packages covers legislation that:

- applies to the examination of a communications device to extract information;
- investigators must consider when communications devices are used to commit offences;
- must be considered when making an application for authority to obtain Communications Data relating to a communications device or service;
- must be considered when preparing Communications Data for evidential purposes; and
- In addition the module covers the procedures associated with implementing this legislation.