#thinkdigital

DIGITAL INVESTIGATION AND INTELLIGENCE

Policing capabilities for a digital age
April 2015

Official – not policy

Contents

Official – not policy

01 FOREWORDS

Mary Calam
Director General
Crime and Policing,
Home Office

Home Office

" Despite the fact crime is down and continues to fall, developments in technology mean that we need to understand better what drives crime and ensure that our response to crime evolves accordingly.

In order to continue to abide by the Peelian principle that the police are the public, and the public are the police, forces must ensure that they embrace technology, and keep pace with future developments.

Criminals are aware of the opportunities that technology opens up to them, whilst much of law enforcement lags behind. The reasons for this, in my view, include the rate at which technology is evolving; reducing budgets; and the impact it is having on police investment decisions.

It is really important that every police officer has the ability to tackle crime with the sort of digital elements that are now commonplace,

be that because the crime needed a computer to take place, or was made easier by technology or even that the offender tweeted about it afterwards.

We need the sort of changes we saw at the advent of forensics – not just specialist labs, but making sure every officer understands how to capture the evidence in the first place.

The opportunity to do more in this space is a major challenge for all of us. We need to work together to understand and define the capabilities required to function effectively. At a fundamental level, we need to explore whether the police operating model, established to combat traditional crime, needs to change.

Only the police can decide this model and with support from the Home Office and others, collectively, we can help to shape and develop a new national vision on these matters."

Mandate

Letter to The National Policing Leadership on the mandate of CC Stephen Kavanagh to lead Digital Investigations and Intelligence - 4th Sept 2014

We wish to inform you of the appointment of CC Stephen Kavanagh as national policing lead for digital investigation and intelligence.

Stephen's appointment recognises increasing awareness of the rapidly changing law enforcement challenges arising from the digital world among the Home Office, ACPO, College of Policing and National Crime Agency.

There is a growing consensus of the need for law enforcement to develop an integrated approach nationally, build new skills and ways of working, and support the development of new legislation where appropriate…

…This is an issue that can touch the lives of anybody, at any time, from any background. There are too many victims out there whose lives have been devastated by online abuse, fraud and cyber crime.

There is a need for better co-ordination, stronger leadership and clear communication to the public on what policing is doing and why.

Stephen will work with the Business Areas and the existing National Policing Leads including Peter Goodman building on the work done in cybercrime; National Leads for fraud and economic crime, communications data, intelligence, the CT network and digital forensics, alongside NCA and Home Office, to map existing work into a new digital investigation and intelligence programme.

Signed,
ALEX MARSHALL, CEO, College of Policing
SIR HUGH ORDE, President, ACPO

Figure 1: DII Governance
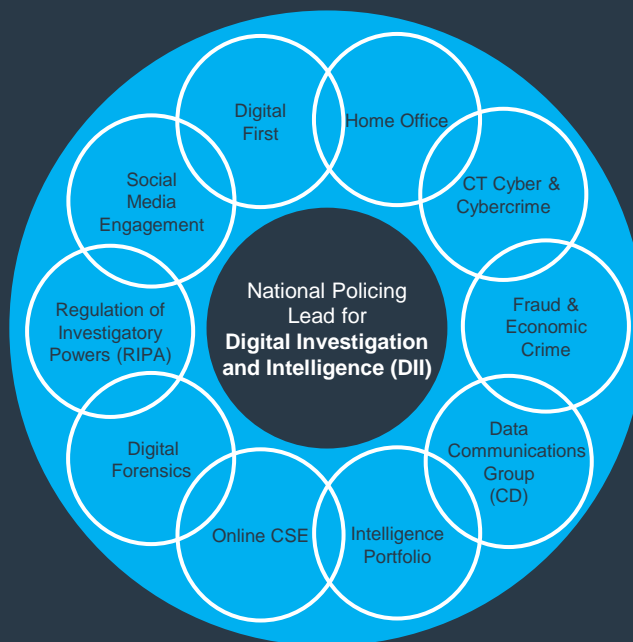
" This remains a fundamental challenge for policing, with a need for everyone from call handlers and first responders to investigators and forensic specialists to think digital."

Official – not policy

Chief Constable Stephen Kavanagh
Lead for Digital Investigation and Intelligence (DII)

" The internet has affected everyone in the UK and has changed society. It has also affected crime.

Traditional crime types, such as burglary and car crime, are on a downward trend whilst online crime has grown dramatically. Phishing, trolling, malware, online scams, revenge pornography and the proliferation of child abuse imagery go largely unrecorded, unanalysed and, as a result, not fully understood. Criminals are exploiting technology, and the tools to preserve anonymity online, more quickly than law enforcement is able to bring new techniques to bear.

The internet is also changing the way the public are using technology; the ways they want to engage with policing; and their expectations of the services they wish to receive. We need to look at the implications for the current policing model and identify what more we must do to protect the public, rather than simply reacting to what happens online

There is a huge amount of work already in train across the service responding to this changing world, but we need to co-ordinate better and recognise the scale of transformation required. We will work with a broad range of partners to make this happen, but we can't wait for government or policy makers to set out the implications for policing – we must do that ourselves.

That is why we came together on 17 February as national policing leaders to agree:

- A vision for developing digital intelligence and investigation capabilities
- Clarity over the gap between where we are now and where we need to be
- A new governance framework to plan, oversee and deliver these capabilities
- A very clear message, to our staff, the next government and above all to the public about how policing is going to be different.

This report sets out that direction of travel - an ambitious and sobering agenda. It is not a full business case or programme plan, although these will follow. It is an agenda that we must action to address the challenges and opportunities posed by technology.

My key message is a simple one – in the digital world our ability to apply technology quickly will significantly determine our capabilities. These will shape our operational effectiveness, which will in turn influence the level of relevance we have to an increasingly online public. We will be judged accordingly."

Official – not policy

02 KEY RECOMMENDATIONS

Delivering the step change in digital investigations and intelligence capability will require a coordinated national effort bringing together the expertise of each force, national policing portfolios, the College of Policing, HMIC and the Home Office as well as working in partnership with industry and academia.

These organisations will need to work with one another in three key areas to accelerate DII capabilities; develop the right governance for a digital initiative; and drive a transformation from local to national level.

1

Accelerating DII capabilities

DII needs to focus on accelerating implementation through identifying and driving key solutions that will make the most impact in forces over the next 18 months. Digital capabilities have the potential to drive a fundamental change to the operating model, services, role and responsibility of police forces , and although this wider change is not the focus for DII, proving the impact of digital capabilities will be critical in the path to further change and modernisation (p.14-16).

2

The right governance for a digital initiative

The scope of DII cuts across a variety of national policing portfolios. A DII Capability Management Group needs to be established that brings together representatives from these different portfolios as well as introducing new focus on key DII capability areas, through assigning dedicated leads to coordinate and drive the development of capability areas across portfolios and forces. This will act as an interim governance arrangement to accelerate coordination and progress, and establish future transformation programme implementation (p.17-20).

3

Driving the digital transformation

Delivering a significant national transformation will require teams to be coordinated to implement key activities that are best performed centrally. This will include stakeholder engagement to energise staff at all levels across forces and design/ portfolio management activities to keep track of capability developments and ensure coherence, as well as engagement with industry and academia. The scale of the transformation challenge requires both a different approach to capabilities management development and dedicated resources to support the programme (p.21).

03

POLICING IN A DIGITAL AGE

Prof. Michael Mulqueen
Professor of Media and Security Innovation, Director of the Centre for Applied Research in Security Innovation [CASI]

Digitalisation is creating a tsunami of data, which is threatening to envelope us. It is estimated that 90 per cent of all the information in the world since time began has been created in the last two years, and is doubling every three years.

We could be overwhelmed by all of this information. Or we could develop ourselves to sense, seize and exploit the opportunities it provides us to reduce threat, risk and harm.

The Intelligence Futures Group (IFG) believes that the way forward for policing lies in Sustainable Innovation, whereby policing is enabled to be an innovation ecosystem, a sector where the best ideas rise to the surface and collaboration with outside, diverse expertise is continuous. But innovation in digitalisation must be tied to clear ethics: Innovation + Ethics = Sustainable Innovation. Here, we set out our reasons with reference to the challenges of risk, relevance and austerity.

Risk: Big Data is presenting new risks in the operating environment for policing. We are at a point at which technological development frequently outpaces the capacities of the law and Government policy to keep pace.

Risks arise if we search too far into the information, or if we fail to yield enough information, or if we have the information but fail to deploy it correctly. Risks form over the corporate reputation of policing and the privacy of individuals, which UK policing must manage very carefully.

Some risks are being better recognised than others. For instance, online child exploitation is a welcome focus of action. But other less prominent risks are equally worrying: are we, for example, tooled up to police scientists working in private laboratories, who, using Big Data, have mutated the DNA of deadly viruses into much more dangerous forms? Numerous other examples of science fiction made real by Big Data could be cited here.

Relevance: Digitalisation is a massive growth area in the private sector and the public sector is getting left behind. Media reports suggest increasing numbers of small, agile, tech-savvy businesses taking on the role of cyber security and investigation for larger businesses and organisations. They trade on what they claim is policing's lack of expertise and capacity to cope. This perhaps shades the work police forces are undertaking against serious and organised crime, as well as terrorism, on the encrypted dark net.

Centre for Applied Research in Security Innovation [CASI]
Liverpool Hope University

Official – not policy

However, the expansion of everyday social activity into the virtual world also raises challenging questions as to the capacity to be relevant.

Social media services including WhatsApp are already providing end-to-end encryption for users. As such, the many children and young people for whom social media is their online street, their playground, and their place to gossip exist in a world designed to be difficult to observe. Policing such encrypted spaces is expensive yet social media is providing a giant, crowded space to which crime in the community is increasingly drifting. Do we have the technology, the people and the organisational agility to conduct routine patrols and investigations in these encrypted spaces? Relevance may depend on it.

Austerity: Policing is irrelevant if it costs too much and irrelevant if it cannot do enough. In this context, digitalisation can enable police to do more with less but create side effects that can stretch the intellectual bandwidth of any responsible decision maker. The internet of things can support smarter interventions of all kinds. It can lead to better monitoring of police officer health and savings on the running costs of police vehicles and buildings. But police usage of information currently gathered through PND, ANPR and other sources is patchy. A wider risk is that digitalisation will prompt further austerity. The philosopher Jaron Lanier compares Kodak, which had 14,000 good quality jobs at its peak, and Instagram, which, when floated, had 13 people on payroll. What does this kind of digitalisation imply for policing communities?

Innovation: Taken together, risk, relevance and austerity drive complexity for policing. Innovation is essential to overcoming complexity and staying ahead of the threat. IFG advocates a radical approach to innovation in policing. A key challenge for policing is to move beyond a traditionally sealed in environment. In our view this requires openness to unfamiliar networks with unfamiliar partners leading, perhaps, to unprecedented outcomes. Such partners may include academe and, notably the creative industry and third sector, whose best people may see threats and solutions in very different ways. Debates about force capacity may be less about officer numbers and more about their capacity to collaborate. The transformation of policing into a flourishing innovation ecosystem is a great management challenge: command in an ecosystem requires enabling policing personnel at all levels to develop new ideas to success (or, en route, failure), either by their own initiative or in collaboration with outsiders. Education is a key support: education sparks innovation by the many.

Ethics: Innovation without ethics is a risk to consent-based policing. For policing the challenge is to empower personnel to be ethical actors as well as lawful ones. This is why we are developing frameworks of digital ethics useable in multiple decision making scenarios.

IFG: We advocate bringing police, academe and the creative industry together in the national interest to promote transformation of policing in a digital age. We believe this partnership will generate smart ideas on efficiency; produce radical horizon scanning of threat; and engage the public mind in the dilemmas of digital policing as well as the policing mind in the ethical question of 'how far can we go' in the use of data. It can also shape a more informed media narrative about data in policing. Facing complexity, we are better together.

Official – not policy

04

DII FRAMEWORK

Digital Investigation and Intelligence (DII) is the response to the following crime and CT challenges.

Understanding the digital footprint i.e. the trail of data that is left behind by all users of digital services. In an investigative context, this typically relates to mobile and online communications, travel and financial transactions by offenders and victims.

Countering Internet-facilitated crime where the internet and smart phones are used in planning or committing traditional criminal or terrorist activity, ranging from online abuse as part of a neighbourhood dispute through to communications between terrorists planning attacks.

Countering Cyber Enabled Crimes (such as fraud, the purchasing of illegal drugs and firearms and child sexual exploitation) which can be conducted on or offline, but online may take place at unprecedented scale and speed. This might include terrorism, e.g. where cyber-enabled fraud is used to fund terrorist activities.

Countering Cyber-dependent crimes which can only be committed using computers, computer networks or other forms of information communication technology (ICT). They include the creation and spread of malware for financial gain, hacking to steal important personal or industry data and denial of service attacks to cause reputational damage for criminal purposes or terrorism.

Figure 2: The core focus of different crime types is different at national, regional and local levels

Official – not policy
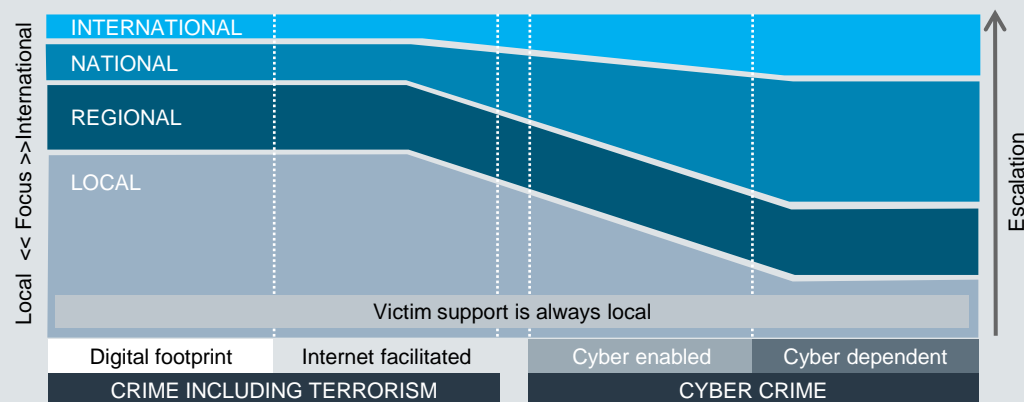
National policing leads and policymakers came together to agree a framework of key capabilities at the College of Policing.

Participants were asked to vote on the state of current capabilities and how they might change over time in the face of the changing threat.

Digital Exploitation was the clear concern amongst the delegates – it was voted as both the most inadequate and a deteriorating capability. Ways of working and people were also felt to be inadequate whilst digital sources was felt to be a good capability perhaps reflecting the level of national investment in access.

The capability framework model provides a checklist for the types of operational capabilities required through four categories:

1. People: skills, knowledge and expertise of the police when working with digital investigation and intelligence, and their ability to integrate digital within mainstream operations.
2. Ways of working: the structures, processes and governance in place for working with digital intelligence and digital investigations.
3. Digital exploitation: fusion, analysis and visualisation of digital data.
4. Digital sources: the ability of the police to get digital data both overtly and covertly.
5. Collaboration and Partnership: ensuring that the right internal and external partnerships are in place.

Figure 3: View of where core DII capabilities are now and over time

Figure 4: The DII Capability framework

Official – not policy
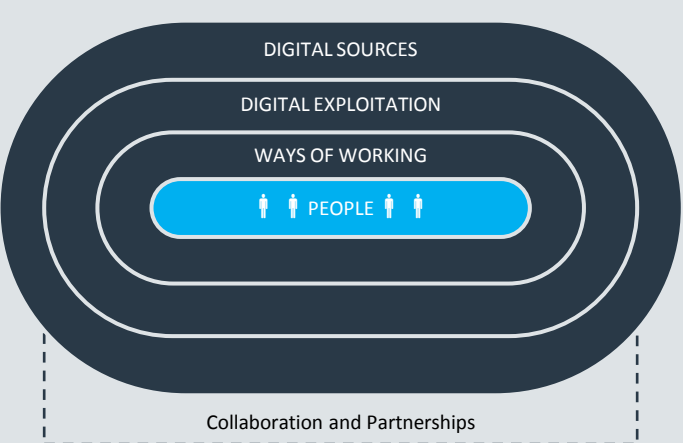
05 DIGITAL INVESTIGATIONS AND INTELLIGENCE CAPABILITIES

DII strategy builds on detailed capability framework developed with the College of Policing.

This sets out what UK Policing will need to be able to do deliver digital investigations and intelligence.
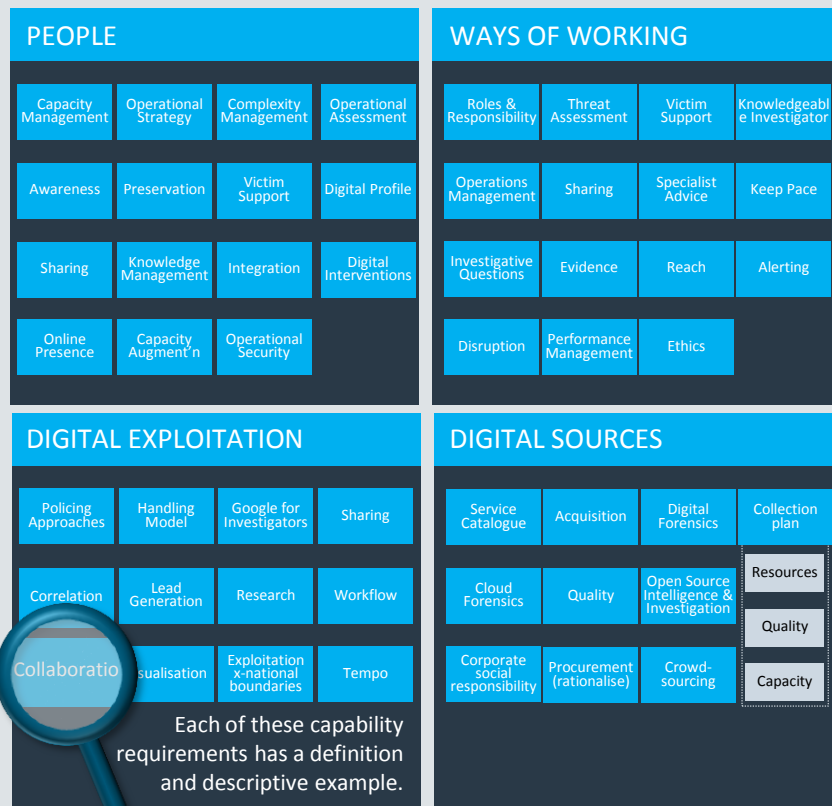
These capabilities need to be tailored to national, regional and local levels in line with their responsibilities. Over the last few years there has been significant progress in building some of these capabilities at the national level (NCCU) and Regional (ROCUs), although at both of these levels there remains issues around operational capacity.

Capabilities are strongly influenced by the supporting infrastructure of police ICT. The absence of national requirements and standards across the service will have a significant impact on operational capabilities locally. As DII capabilities are developed and articulated they will need to feed into the Operational Requirements Board that sets national police ICT requirements and there is a key role for the Home Office and Police ICT company in translating these into practice.

Figure 5: The DII Capability map

PEOPLE

Capacity Management	Operational Strategy	Complexity Management	Operational Assessment
Awareness	Preservation	Victim Support	Digital Profile
Sharing	Knowledge Management	Integration	Digital Interventions
Online Presence	Capacity Augment'n	Operational Security	

WAYS OF WORKING

Roles & Responsibility	Threat Assessment	Victim Support	Knowledgeable Investigator
Operations Management	Sharing	Specialist Advice	Keep Pace
Investigative Questions	Evidence	Reach	Alerting
Disruption	Performance Management	Ethics	

DIGITAL EXPLOITATION

Policing Approaches	Handling Model	Google for Investigators	Sharing
Correlation	Lead Generation	Research	Workflow
Collaboratio / sualisation	Exploitation x-national boundaries	Tempo	

Each of these capability requirements has a definition and descriptive example.

DIGITAL SOURCES

Service Catalogue	Acquisition	Digital Forensics	Collection plan
Cloud Forensics	Quality	Open Source Intelligence & Investigation	Resources
Corporate social responsibility	Procurement (rationalise)	Crowd-sourcing	Quality
			Capacity

i.e. **Collaboration***:* As an investigator, I can employ collaboration tools to share new digital tradecraft, knowledge and experience.
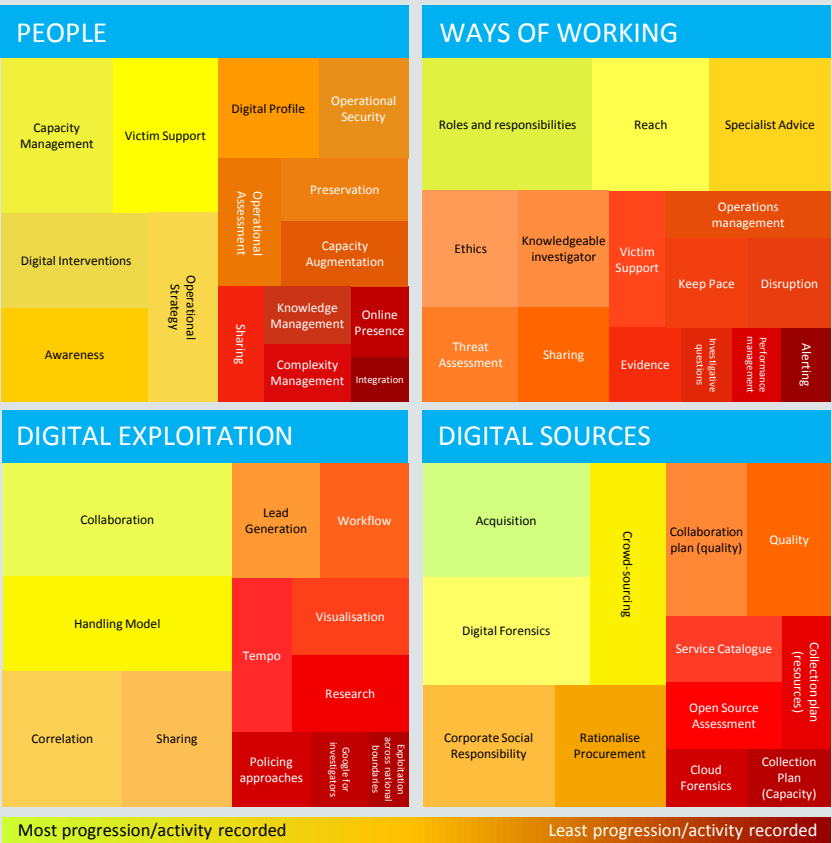
For example: Local investigative teams share operational experience and questions using on-line tools to support learning from experience and provide a layered knowledge base

Official – not policy

We have an initial view of where there are gaps in capability development

Forces have already started to build DII capabilities. During 2014, a comprehensive survey of existing activity highlighted progress to develop capabilities at national, regional and local levels, and identified areas that need focus.

This initial snapshot gives a sense of where there are gaps in focus within capability development. Feedback on this high level view has confirmed that the 'reds' feel like the right priority areas.

Figure 6: The DII Capability heat map

PEOPLE

- Capacity Management
- Victim Support
- Digital Profile
- Operational Security
- Operational Assessment
- Preservation
- Capacity Augmentation
- Digital Interventions
- Operational Strategy
- Awareness
- Sharing
- Knowledge Management
- Online Presence
- Complexity Management
- Integration

WAYS OF WORKING

- Roles and responsibilities
- Reach
- Specialist Advice
- Ethics
- Knowledgeable investigator
- Victim Support
- Operations management
- Keep Pace
- Disruption
- Threat Assessment
- Sharing
- Evidence
- Investigative questions
- Performance management
- Alerting

DIGITAL EXPLOITATION

- Collaboration
- Lead Generation
- Workflow
- Handling Model
- Tempo
- Visualisation
- Research
- Correlation
- Sharing
- Policing approaches
- Google for investigators
- Exploitation across national boundaries

DIGITAL SOURCES

- Acquisition
- Crowd-sourcing
- Collaboration plan (quality)
- Quality
- Digital Forensics
- Service Catalogue
- Collection plan (resources)
- Corporate Social Responsibility
- Rationalise Procurement
- Open Source Assessment
- Cloud Forensics
- Collection Plan (Capacity)

Most progression/activity recorded — Least progression/activity recorded

06

ACCELERATING
CAPABILITY
DEVELOPMENT
FOR FORCES

Official – not policy

Findings and conclusions from the workshop: illustrative requirements for digital capability within a typical police force

Figure 8: Illustrative DII capability requirements at force level

The DII workshop identified what the capability framework might mean for a typical police force, and what good might look like for DII capability development at force level. This provides the foundation for understanding what forces need to implement, and work will be done to validate these findings with forces.

Leadership

Performance framework for cybercrime and digital capabilities	**Prioritisation and tasking** for cybercrime incidents	**Strategic lead for DII**	**Digital ethics**	**Communications to public** on digital capabilities and ethics

Neighbourhood	Response	Investigations	Specialist support	Intelligence

Neighbourhood / Response

Officers have **general awareness of DII sources** so they can make an initial response to preserve digital crime scene

Officers can carry out **open source research securely**

Online presence and can **'patrol' the internet**

Standard level of **digital crime prevention advice** with specialist support as an online service

Officers can provide a standard level of cybercrime **victim identification and support**

Online service to provide engagement with the public for crime reporting and intelligence

Investigations

Advanced understanding of DII sources to support investigations

Digital disclosure

Channels to **crowd source investigations**

Officers able to conduct and request **online disruptive operations** to protect victims

Major crime/ SOC
- Task **investigations on dark web**
- Knowledge of **criminal comms tradecraft**
- Knowledge of **international processes**
- Build **digital evidence case file**

Specialist support

Hi tech/ E-forensics
- Lead force on **expert digital collection skills**
- Ability to exploit data in the cloud
- **Partnerships with** specialist industry suppliers

Public protection
- Online suspicious **behavior alerts**

CSI
- **Initial response to** preserve and collect digital

Search/firearms/traffic etc..
- General digital awareness to preserve scenes

Intelligence

Data exploitation- standards for fusion, analysis and visualization systems

Assessments of **cybercrime threats and digital opportunities**

Data sharing with other organisations

Analysts/ data scientists to exploit big data

Proactive digital operations/ online UC/CHIS

Enablers

Data exploitation **infrastructure and apps**	**Cyber security**	Digital specialist **career pathways**, recruitment and retention and specials	**Agile procurement** for digital capability

Changes to the digital environment present the need for a fundamental rethink of the responsibilities, role, services and operating model of forces in England and Wales.

Accelerating DII capabilities

DII needs to focus on accelerating implementation through identifying and driving key solutions that will make the most impact in forces over the next 18 months. Digital capabilities have the potential to drive a fundamental change to the operating model, services, role and responsibility of police forces , and although this wider change is not the focus for DII, proving the impact of digital capabilities will be critical in the path to further change and modernisation.

We will need to work with forces to validate requirements for DII capabilities at a local level.

Capability Recommendations

1. **The DII governance board should conduct a more systematic review** of Force level capabilities to validate prioritisation.

2. **The appointment of a Chief Officer Lead for each Force** who can drive and monitor the DII capability development within that Force

3. **The DII Lead in each Force should focus on developing** priority capability development areas once these are validated:

- **Development of a new performance framework** that looks at cybercrime and operational DII capabilities rather than just number of officers and more traditional crime statistics

- **Provision of victim support for cybercrimes** delivered at the neighbourhood level where officers can give out a standard level of advice and support materials.

- **Using partnerships to enhance capability** for example working with industry, volunteers or specials who have specialist skills or knowledge.

- **General digital awareness** for all officers built into probationer training so that they can respond to a digital crime scene and know what specialist capabilities are available.

- **Digital training for investigators** so they can develop collection plans and purse digital leads

- **Digital crime prevention at local level able to provide victims of crime** (e.g. domestic abuse, fraud, ASB with standard advice backed up by specialist officers).

- **Joined up approach to data exploitation/ big data** capabilities, drawing on current innovation activities/ bids to develop common standards and services across forces

- **Development of career paths for digital specialists** recognising the need to move between organisations, pool resource and work closely with industry

- **Communicating with their local public** so they understand DII capabilities and continue to support policing online and the police maintain public consent.

- **Enabling online reporting** making it easy for the public to report crime and intelligence to the police through easily accessible online tools.

Official – not policy

07

ESTABLISHING THE RIGHT DII GOVERNANCE

The right governance for a digital initiative

The scope of DII cuts across a variety of national policing portfolios. A DII Capability Management Group (CMG) needs to be established that brings together representatives from these different portfolios and the College of Policing. It will also introduce new focus on key DII capability areas, through assigning dedicated leads to coordinate and drive capability development across portfolios and forces.

This governance will act as an interim arrangement to accelerate coordination and progress to a formal programme structure.

DII needs a new style of governance, fit for digital-age challenges

In the policing context there are challenges to move away from traditional, hierarchical structures towards a more innovative and creative solution that moves faster, trials approaches and adapts to the changing environment.

Delegates highlighted the proliferation of mirror-image 'sub-groups' (e.g. training, evidence) within each area, and the opportunities to rationalise these existing governance structures (figure 9).

These existing structures have achieved a lot of progress for their areas of focus, and provide strong foundations through which to build DII governance.

Critical success factors for DII governance are to:

1. **Provide management oversight** to ensure that the DII portfolio is responsive to a rapidly evolving threat; embraces agile delivery; and has an affordable total operating cost.

2. **Provide end-to-end accountability** to ensure that the DII portfolio is integrated, and that delivery is sequenced to achieve the best, and earliest, operational outcomes.

3. **Achieve these outcomes with the leanest possible governance team** - using technology and virtual structures to avoid adding new layers of management controls and effort.

Figure 9: Current portfolio governance arrangements – illustrative

Official – not policy

Governance recommendations

1. **DII should be led through a 'Capability Management Group' (CMG)** to drive consistent and coordinated development of digital capabilities at operational level

2. **The scope of DII governance should include portfolio and capability leads**
- DII will be steered by the nine areas of work identified in the DII mandate letter (pg.3)
- It should be extended to include the 'Digital First' portfolio to ensure that operational capability development is clearly linked to the criminal justice system
- The existing Cybercrime portfolio should be part of the DII steering group in order to ensure alignment of capability development nationally, regionally and locally
- DII will also work closely with the College of Policing, and with Police ICT co.

3. **CC Stephen Kavanagh should be appointed 'Single Point of Accountability' for DII delivery** to achieve appropriate and effective governance and leadership

4. **DII governance should be allocated full-time portfolio management resource, underpinned by a core delivery programme**
The Home Office Communications Capabilities Development (CCD) Programme was cited as an example of a programme that could be re-scoped to support a wider DII delivery portfolio, whilst providing valuable capability integration, technology expertise, training and business change. It is a programme that already has well-established links with the policing, counter-terrorism and serious & organised crime agencies.

5. **Each of the 15 CMG members should be responsible for chairing a Capability Working Group (CWG)** for their respective portfolios/ capability areas, and for reporting by exception on progress, risks and issues which impact on national plans (Figure 10).

6. **The CMG should drive coordination and monitor performance of the following four strategic roles** undertaken by national policing (Figure 11):
- Setting the Strategic Vision for Digital Investigations and Intelligence
- Establishing an integrated approach to DII capability development
- Maintaining oversight of DII capability delivery
- Setting standards for, and monitoring, operational delivery of DII capability.

### Proposed interim CMG Terms of Reference:
- CMG will meet quarterly (alternating the agenda and participation between portfolio leads and capability area leads).
- It will operate as the 'engine room' driving progress and monitoring performance.
- It will include leads from the ten cyber / digital portfolios
- It will include new national leads for each of the five capability areas, as a single accountable owner each area to ensure coherence and effective integration.
- The Group will be chaired by the DII lead.

Figure 10: DII capability management group
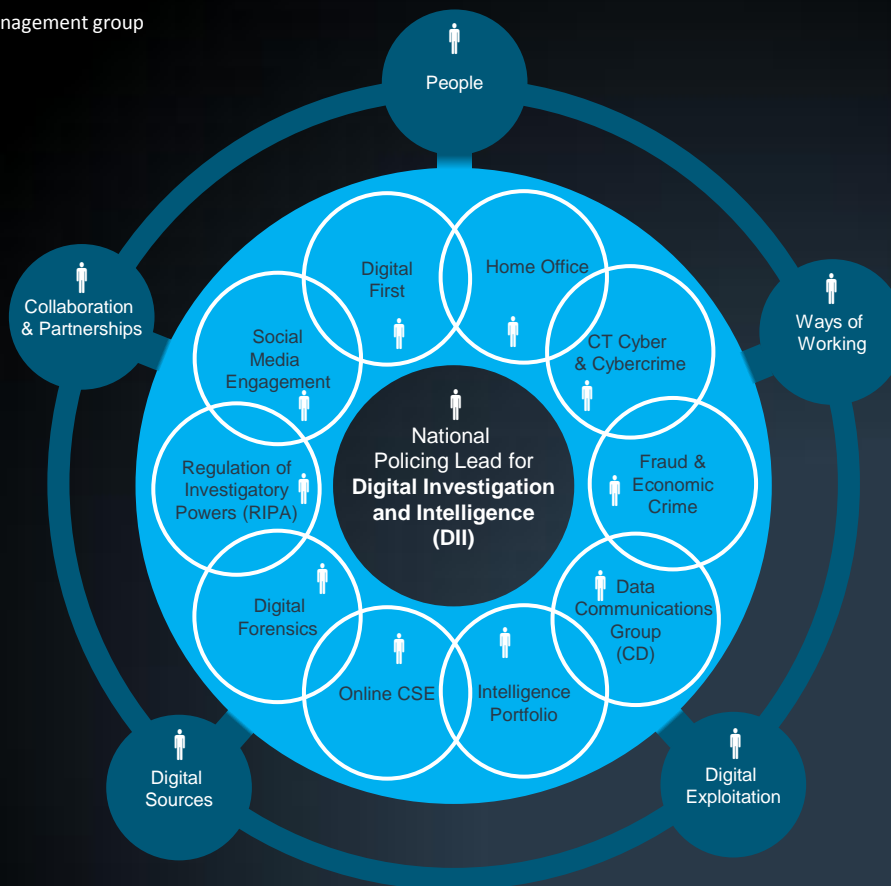
The CMG will need to work with a range of partners to deliver the transformation in policing. This will affect all aspects of policing and include the involvement of the Home Office, College of Policing, Police ICT Company, National Crime Agency, Police and Crime Commissioners, staff associations and Chief Constables as well as representatives from beyond policing. The CMG represents an interim position towards setting up the necessary governance arrangements focused on the core digital investigation and intelligence capabilities that need to be aligned without delay.

Figure 11: DII governance and implementation model
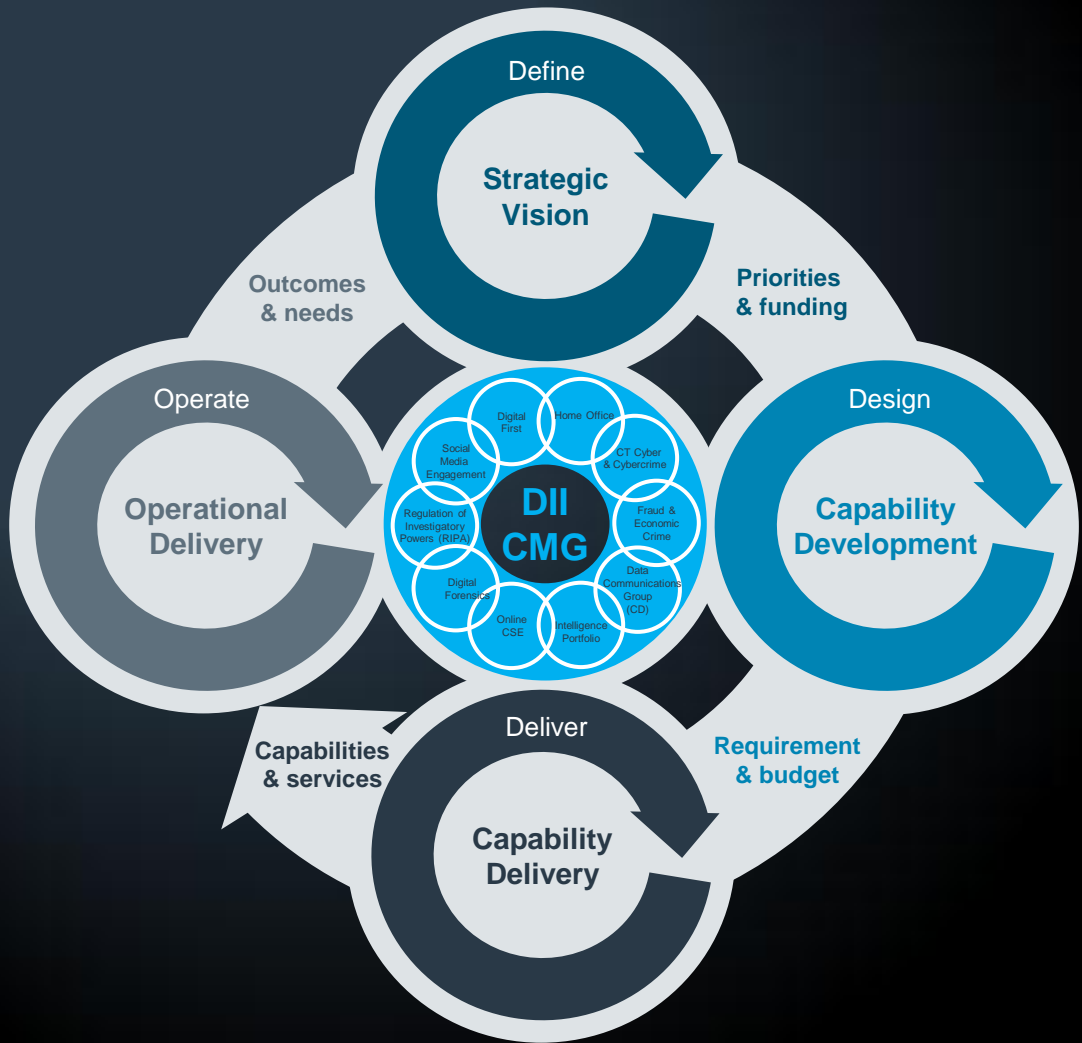
The election and post-election spending review process provides an opportunity to rationalise and co-ordinate capability development and programme delivery across DII.

Seven priority actions for driving digital transformation through DII

1. **Define the national vision for DII** to describe what success looks like for local forces and the victims of cyber and internet-facilitated crimes

2. **Establish measurement and assessment of cyber/digital crimes** - to establish a baseline and help communicate successes and issues

3. **Develop national standards for digital policing**

4. **Identify and work to remove duplication** of activities, resources and funding

5. **Set investment priorities**, highlighting both gaps and opportunities

6. **Identify and communicate best practice** to enable forces to access and benefit from emerging tradecraft

7. **Harness external assistance** (e.g. academia and industry) in a coherent and thoughtful way; ensuring that we avoid conflicting local initiatives and that each CC/PCC can identify and access 'best of breed' support.
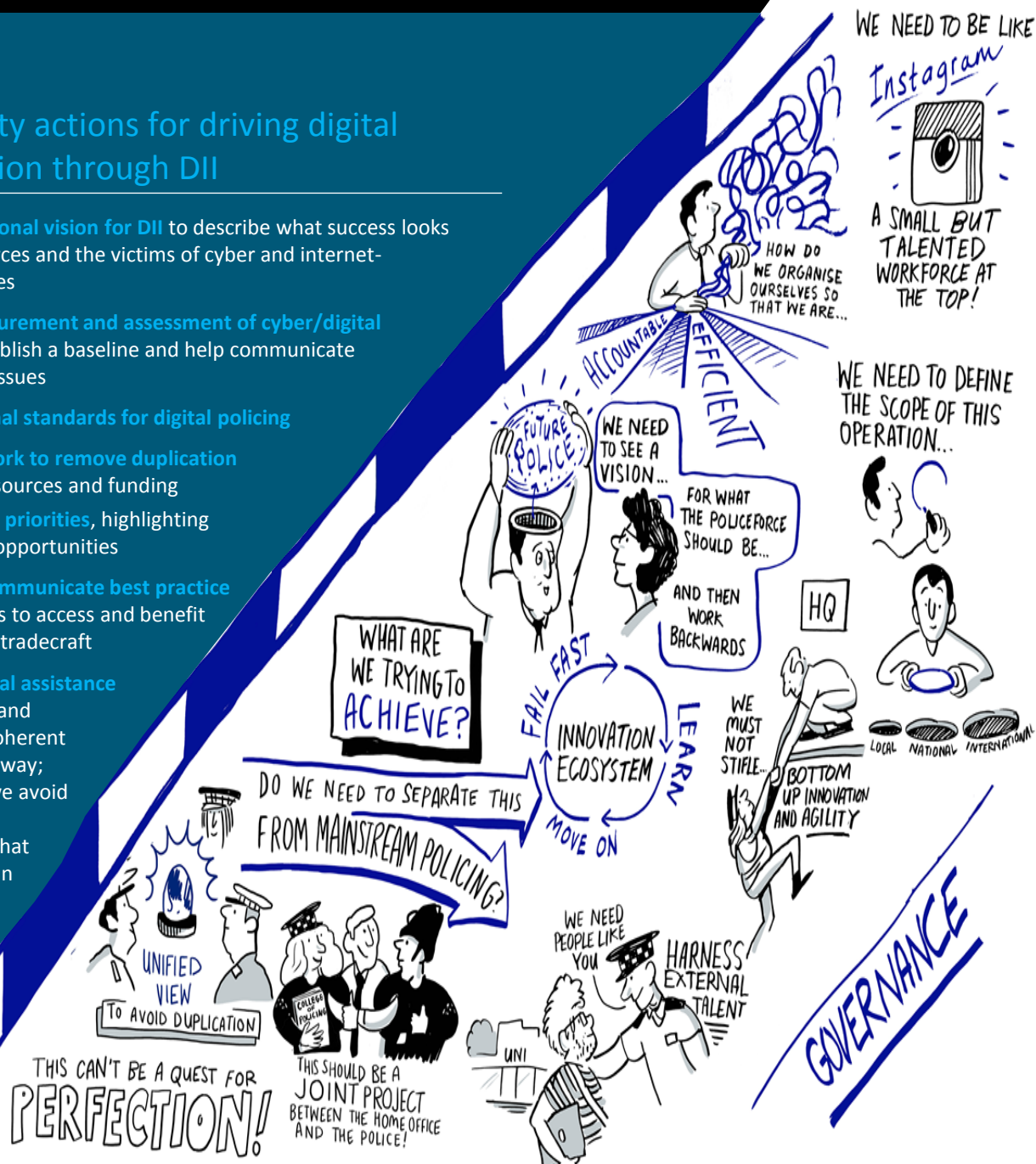
08

WE ARE MAKING PROGRESS NATIONALLY, REGIONALLY AND LOCALLY.

Training of **4000+** officers across the country through the CoP's **MCCT programme**

Strategic working group development ensuring all agencies on the same level across one framework – *Intelligence Professionalisation Programme (Durham Police)*

National contracts for 2 **social media monitoring** tools – *ACPO open source and intelligence*

60 staff **OSI trained** – *North West Regional Cyber Crime and Open Source*

OCG/USG group mapping generating tactical advice and guidance in exploring the full range of RIPA telecoms applications – *Merseyside Cyber Interventions*

Enthusiasm from business and industry **partners** to develop a North Wales **Trust Group** – *North Wales Cyber Crime*

Daily Cyber crime and **incident scanning** – *Greater Manchester Police*

55 cyber trained officers and secure **covert internet platform** implementation – *Cheshire Police*

"**Detective skill-set** enhancement" – *Powys Digital Communications and Cyber Crime*

"Very strong **business links**" with the national cyber skills centre and Malvern cyber cluster – *West Mercia and Warwickshire Police*

National Cyber Crime Unit established within NCA to **coordinate response nationally and internationally**

Met Falcon Unit established to respond to cyber enabled fraud

National

Regional

Local

Official – not policy

UK CERT and **Estonian Government collaboration** to develop an incident operating model for CERT and LE – *National Cyber Training and Development*

9 regional cyber crime units established - *ACPO*

Alignment of **Force Strategy** with Regional/National plans – *West Yorkshire Cyber Crime*

National Surveillance conference: strategic and user associated presentations delivered to **150 delegates** from all UK forces and law enforcement – *National Surveillance*

Investment in Digital Forensics and Communications Data capabilities – *South Yorkshire Digital Forensics*

The provision of **un-attributable laptops** to officers – *Norfolk and Suffolk Cyber Crime*

'Cyber' briefings given to all senior managers – *Thames Valley Cyber Investigations SG*

Design, approval, implementation of **Cybercrime strategy** – *South East CRUG*

New easily **adoptable** processes that support **interoperability** and **data consistency** in Digital Witness statement creation – *Surrey and Sussex Digital Evidence SG*

First **national OS conference** (2014) and first EU conference planned (2015)– *ACPO Open Source*

LOOKING FORWARD, WE COMMIT TO:

- Gaining the National Police Chief's Council endorsement in April

- The establishment of an interim capability management group by April, with its first meeting in May

- Engagement with forces on capability development and validation from May continuing throughout 2015

- Engagement with Government on programme design and resourcing

- Engagement with Police ICT company over support to the programme.

#thinkdigital

The Digital Investigations and Intelligence workshop was
facilitated by PA Consulting Group

PA

CONSULTING
TECHNOLOGY
INNOVATION