The Shape of Things to Come. The potential impact of fraud and cybercrime on the organisational profile of police services in England and Wales

Barry Loveday

University of Portsmouth

Policing: A Journal of Policy and Practice (to appear)

Abstract

Recent official statistics have highlighted for the first time in the UK the nature and extent of computer fraud and cybercrime against individuals and households. This has in turn posed questions about the adequacy and the speed of the police response to these newly highlighted crimes. At the same time the Public Accounts Committee has pressed for more co-ordination of efforts to counter cybercrime against government departments [PAC, 2017]. Although a number of useful initiatives have already been put in place, by the Home Office and police forces, into understanding and responding to these threats the paper claims that much more needs to done, particularly in changing policing structures, in recruitment, in training and in co-ordination of work across agencies. The paper considers the current police response, the potential problems confronting change management arising from police organisational culture. It does however identify successful police modernisation programmes that have enabled police services, outside Europe, to both restructure and recruit appropriate personnel in response to a changing criminal environment which now confronts them. It argues that in a similar way new demands on the police service will require it to significantly review its capabilities which may impact on traditional commitments to capacity.

Introduction

Recent statistics from the Office of National Statistics have clearly highlighted the nature and extent of computer fraud and cybercrime [ONS 2016a]. As a consequence this has raised concern about the response of the police to these newly highlighted crimes. The estimate is based on a single year and thus it cannot be established statistically whether such crimes are on the increase. Yet it is also clear that the fall in the crime rate for traditional offences against households for which the police had been claiming a success has now been replaced by a significant change in the nature of offending. This also appears to be reflected in the changing backgrounds of victims of crime.

ONS Data demonstrates that residents in England and Wales are 20 times more likely to be a victim of fraud than robbery and 10 times more likely to experience fraud than theft from the person [ONS 2016a]. This was based on crime survey estimates that there were around 3.8 million fraud cases and 2 million computer misuse offences annually. As stated by ONS:

'*The estimate of 5.8 million fraud and computer misuse offences is similar in magnitude to the current headline estimate covering all other CSEW offences and provides an indication of the scale of threat from such offences*' [ONS CSEW Section 6:2016a].

Examples are online shopping scams, computer virus attacks, ticket frauds computer hacking and theft of bank details along with credit and bank card fraud. [ONS:2016b]. When added to

other crime cyber fraud and cybercrime pushes up the total crime experienced annually by households to more than 12 million offences [Ford 2016].

This suggests that volume 'fraud/cyber' crime is now of the same order of magnitude as volume 'acquisitive' crime and probably greater if crimes where the victim is a public body or a commercial company- not counted by the survey – were to be included. This represents a new and significant challenge to police services. Victimisation patterns also appear to be different from what was understood previously. The chance of being a victim of fraud transcended established boundaries as the likelihood of victimisation was the same regardless of class, region, age group or whether a person lived in a rural or urban area [ONS 2016].

Despite the significant amount of effort already put in by police forces and the Home Office into understanding and responding to cybercrime a simple example demonstrates that a good deal work is still necessary. If an individual reports that £10,000 has been stolen from his house in a burglary, he is likely to get an immediate response from his local force: if the same householder reports £10,000 has been stolen from his bank account, the local police are likely to refer the victim to his bank or to Action Fraud and the crime is much less likely to be investigated individually.

Trends in Crime

The changing nature of crime reflects a relentless increase in the public use of computers and new technology. The exponential growth of sales of computers and ICT has provided new opportunities for offenders able to reap the benefits of fraudulent activities from places of comparative safety. It is also the case that the major banks have actively contributed to this by encouraging users to move to online banking. Banks have agreed to underwrite losses and if customers can prove they have been defrauded, banks usually reimburse their loss.

The current threat represented by fraud and cybercrime have been identified by the National Fraud Intelligence Bureau for April –March 2016 [City of London Police 2016]. It identifies the total volume of reports of cyber enabled fraud as standing at 104,547 reports. It identifies the 'top 10 Types' by volume of reports. Major types of fraud are identified as 'online shopping and auctions': 30,249; computer software service fraud: 11,625; cheque, plastic card and online- banking: 4945; Ticket fraud: 4028 [NFIB City of London Police 2016].

The majority of reports were made by individuals. The victim impact by volume of reports showed that of the total some 4,481 were to be classified as 'severe'; 25,464 were identified as 'significant' and 23,403 were classified as 'concerned' [NFIB 2016]. The median loss per victim for cyber-enabled crime was estimated to be just £400.00. This figure does not take into account the differing economic situations of victims and the impact of financial loss on individual victims. Interestingly the new Crime Harm Index recently developed by the Home Office, to weigh the impact of crimes on victims, entirely overlooks computer crime and financial fraud [Foreman 2016].

As noted, the shift away from traditional volume offenses and acquisitive crime to cyber - crime fraud or money laundering reflect a new reality. This now is seen as being both safer to commit and also much more lucrative 'than its real world counterpart' [Naughton 2015]. As has been argued:

'*The rewards are much greater and the risk of being caught and convicted are astonishingly small. If you are a rational criminal why would you bother mugging people, breaking into*

houses, stealing cars and all the other crimes that 'old style' criminals commit and that 'old style' cops are good at catching them doing? '[Naughton 2015].

It is estimated that forty percent of online fraud cases resulted in no monetary loss. Yet the very frequency of victimisation found by the CSEW in the past year indicated that one in ten adults had been a victim of fraud or cybercrime and that:

'*The chance of being a victim is the same regardless of social class or whether someone lives in a deprived or affluent urban or rural area*' [ONS 2016].

The most common type of fraud identified was either bank and credit account fraud at 2,472,000 cases or non-investment fraud where the victim was persuaded to invest in a non-existent scheme which stands at 1,420,00 cases [Allen 2016].

Individuals and households are not the only victims. The Public Accounts Committee [PAC, 2017] in addressing the need to protect information across government departments, found that '*the processes for recording personal data breaches are inconsistent and dysfunctional*' and concluded that:

'The use of the internet for cybercrime is evolving fast and the government faces a real struggle to find enough public employees with the skills to match the pace of change.'

The Police Response

One interesting feature of the dramatic rise in fraud and cybercrime has been the slow reaction by the police service to this development. Recent analysis of police establishment directed to respond to the problem show that total numbers have actually fallen over recent years. In 2014 it was estimated that a total of 416 officers were then investigating fraud. This represented just 0.27% of all police personnel [Button et al 2014]. More recently it has been estimated that more police officers are now investigating complaints against the police than are investigating fraud [Button and Cross 2016].

Elsewhere it has been argued that the police response to this problem was to raise concern 'not least among police officers'. They believed that cyber- crime 'had been at alarming levels for some time and none of whom appeared to be confident that the law enforcement system could deal with it' [Naughton 2015]. This was perhaps a reflection of what had been perceived by police traditionally as 'white collar' crime viewed as a second level priority and which could make big demands on police resources when police budgets were being cut and sustaining visible policing had become a political priority [Button et al 2014; Collinson 2016].

In the police service there has been a relative indifference to the problem of 'online crime'. This has been highlighted in a 2015 report by HMIC. In this the failure of police forces to fully appreciate the changing pattern of victimisation was identified. Noting that modern technology was now an integral part of people's lives HMIC was to question police perceptions of online victimisation [HMIC 2015:Para1.13]. It was found that the police were often dismissive of online crime and failed to act in response to victim's complaints. HMIC drew attention to online financial crime. One victim of financial crime who lost £60,000 in a 'boiler room' shares fraud stated that he had no contact 'whatsoever from his local police force after reporting the crime' [Barrett 2015].

A similar problem was experienced elsewhere. It was argued that negative views about the police in response to online crime was corroborated '*by the experiences of 5% of UK internet*

users who had been victims of various kinds of cybercrime –identity theft , phishing scams, card fraud and malware attacks. They report that a variety of responses-almost none of them helpful- from the local police to whom they had turned for help' [Naughton 2015].

The need to re-orientate policing to confront the changing nature of crime is apparent. It should also address the issue of capability identified by HMIC in its 2015 PEEL Efficiency Report. In the Report police forces had it was found a very accurate knowledge of police force capacity – police numbers, ranks, costs and police staff. In terms of capability however this knowledge rarely extended beyond senior investigative, firearms or public order officer numbers.

More damaging still many forces, in seeking to protect capacity in response to recent budget cuts, did so at the expense of capability. HMIC added that most forces were, unable to describe accurately what the current strengths or weaknesses were in their skills either across the whole workforce or by rank or grade [HMIC 2015:33].

This lacuna within police policy could extend to the problem of fraud and cybercrime. Here capability will also need to be developed. Some evidence of a response by police has already been demonstrated.

If the Metropolitan Commissioner was to be criticised for what appeared to be an attack on victims of bank fraud [Travis 2016] the MPS was also, in 2015, to establish under Operation Falcon, the Metropolitan Police Cyber Crime Unit [MPCCU]. This Unit targets serious incidents of cybercrime and works closely with the National Crime Agency in proactively targeting cybercrime criminals [MPS Operation Falcon website 2016].

However the work of the MPCCU extends to only the most serious cases. It will therefore exclude the great majority of offences. A similar reservation might extend to the City of London Police's most recent initiative. This is to employ private law firms to pursue criminal suspects to target cybercriminals and fraudsters. This initiative is seen by the police as one way of more effectively tackling fraud now estimated to cost £193 billion a year and which is, it is argued, 'overwhelming police and the criminal justice system'. The use of the civil courts and a lower level of proof, based on the balance of probabilities, are expected to aid the recovery of money to victims of fraud [Dodd 2016].

These developments must be viewed against a background where within the MPS a decision was made to recruit 800 additional armed officers in 2016 while an extra 1,500 armed officers are now planned nationwide. This initiative represents a huge resource investment and extends far beyond any similar response to changing patterns of crime in either London or outside of the capital [Grierson 2016].

The shape of things to come

In reaction to the new ONS figures on cybercrime, an identification of possible responses has been made. These could, and probably should, have implications for police organisational structures and recruitment policies. Some indication of the new dimensions required of future police personnel recruitment has in fact already been identified. In oral evidence to the Home Affairs Committee the then Director General of the National Crime Agency was to respond to questions about high staff turnover within the NCA by stating that:

'*The reason we have needed people to leave –is that we had too many senior people who were probably of my generation in law enforcement –and law enforcement has changed. We need more crime fighters who are digitally hugely competent , more people who can write*

code and more people who are expert in how banks operate –so we need different skills' HAC Oral Evidence 2015 Q39p9].

While releasing many police officers the NCA has, however, been engaged in directly recruiting '*hundreds of people who have joined as trainee investigators and trainee intelligence officers*' in order to shift the workforce '*to be the contemporary workforce that was needed*' [HAC Oral Evidence 2015 Q40p10].

For the NCA recruiting direct entry '*highly qualified code writers and engineers*' was not viewed as problematic. Retaining them in face of competition from the private sector was however. The Director General commented '*it was increasingly important to establish careers based on the intellectual challenge of tackling the most difficult cyber criminals*' while also '*keeping the public safe*' [HAC Oral Evidence 2015 Q66p16].

Elsewhere the current Director General of the NCA has commented on the way the criminal environment has undergone a sea change and the need for the police to respond to that. Arguing that:

'*The chances of being a victim of a burglary, a vehicle crime or a street robbery are all much lower than they have ever been before. All those were crimes that effectively happened in the streets so they could be dealt with by the visible police officer responding. There is now a much greater likelihood of you becoming a victim within your own home through your computer. The great developments in technology have enabled offenders to behave in different ways and there has been a fundamental change*' [Sylvester and Thomson 2016].

This insight into current and future criminal engagement has also been noted by the current CHMIC. He has argued that 'bobbies on the beat' were increasingly 'old fashioned' in an internet age and that:

'*The probabilities of a police officer walking past a burglary in progress are pretty low. A great deal of crime is not taking place on our streets. The perpetrator feels safer, because he or she is sitting in front of a computer, rather than breaking in somewhere*' [Sylvester and Thomson 2016].

Changing Police Perceptions

Dealing with the avalanche of fraud and cybercrime offences has been recognised most recently by the Police Superintendents Association which has argued for a rethink of police recruitment policy to establish new capability in this expanding crime area. Primary recommendations for change involve greater flexibility in terms of recruitment [Thomas 2016:1]. The technical nature of the problem the police will face means a need to consider the skills mix of its recruits to enable it to deal with the threat. The President of the PSAEW has argued that:

'*The traditional skills that have served policing well through successive generations are not the only ones that will be required in the future [and]future recruitment might target people in their late teens or early 20s as a means of tackling fraud investigation*' [Thomas 2016].

This could mean recruiting cybercrime and financial experts outside of policing whose skills can be immediately utilised rather than relying on the traditional model of training a police officer first and '*then going on to train them to be an expert in cybercrime , money laundering or fraud*' [Thomas 2016:2].

This proposal would appear to provide a much more attractive option than the recruitment of local 'volunteers', a proposal supported by the then Home Secretary Theresa May. Local 'volunteers' would be able 'to exercise intrusive powers over neighbours and others in the community' without any measurable degree of accountability [Weinfass: 2016]. This initiative could create potentially dangerous hostages to fortune but could be viewed as further evidence of the belated nature of official recognition of the threat that fraud and cybercrime now represents.

The problem has been recognised at least within the National Police Chief's Council [NPCC]. This has established a Digital Investigation and Intelligence Programme which will begin to address the problem in a more professional manner and with a greater prospect of success than that espoused earlier by the Home Secretary. It is also evident that the size of the problem has been identified. This has been recognised most recently within the 2015/6 report of the Independent Surveillance Review within which the growing challenges making citizens potential targets for fraud criminals and terrorists is highlighted [RUSI 2015:12] As is also noted, however, the 'task for the police' has become more demanding as they try to stay abreast of rapid technological innovation that emanates across the globe' [RUSI 2015:12]

Yet currently a rather limited horizon has characterised the official response to the problem. The then Home Secretary Theresa May was to create a Joint Fraud Taskforce along with a Police Reform and Transformation Board. Yet how much impact either can be expected to make on what remains a fast developing and increasingly global crime threat remains difficult to ascertain [Button and Cross: forthcoming].

More recently the UK government has passed into law the Investigatory Powers Act 2016, which could eventually assist security services and the police in their work to counter cybercrime. This new surveillance law requires web and phone companies to store all web and browsing histories for 12 months and give police, security services and official agencies unprecedented access to the data. It also provides police and security services with powers to hack into computers and collect communications data in bulk. [UK Legislation [2016]]

Important safeguards are included in the act, but it has none the less come in for a great deal of criticism and the details of its implementation are unclear. The European Court of Justice - whose rulings are still valid while Brexit is being negotiated - has ruled, since the act was passed, that '*only targeted interception of traffic and location data in order to combat serious crime – including terrorism – is justified*.' At very least this is likely to cause some delay in implementation, as the government will need to produce guidelines under which police and security services are required to work when applying the provisions of this Act.

Further problems confronting the police relate to resources. Police forces have recently experienced significant cuts in spending. One major casualty of this process has been, for example, the effective burial of workforce modernisation programmes initiated a decade ago [Loveday 2007].

One former chief officer has argued that the impact of resource decisions made within most forces has been to throw the modernisation process into reverse. Increasingly he concludes the common experience has been the 'officerisation' of the police service as civilian staff have been released to sustain police capacity [Loveday 2015]. Major reductions in civilian support staff [including PCSOs] have been one consequence of the inflexibility of current employment arrangements for sworn officers. The result has been to undermine local

neighbourhood policing while removing police officers from operational roles to fulfil functions once the responsibility of support staff [Unison 2013; 2016].

Yet the workforce modernisation programme showed the value of employing more not less civilian support staff. These benefits do not just pertain to reduced cost. They extended to increasing police effectiveness most immediately by the introduction of Mixed Economy Investigation Teams [Loveday 2008]. This feature of workforce modernisation may have a ready application to the future investigation by the police of fraud and cybercrime.

Current policing of fraud and the use of Investigative Support Officers [ISOs] has provides a useful precedent upon which to build. Outside of the police service there has been an expansion in of non-sworn fraud investigators entitled Counter Fraud Specialists [Button et al 2008]. It is computed that by 2007 the DWP, local authorities, NHS and HMRC together employed over 8,000 Counter Fraud Specialists. This entirely overshadowed police investment in fraud investigation [Button et al 2008]. This imbalance in investigation capability between police forces and CFS personnel continues to pertain. Capability planning by police forces should explore the employment of civilian investigators to bring with them both appropriate professional and technical skills.

Future estimates of police capability in fraud investigation was to conclude that any credible response would be based on increasing investigative capacity with non-sworn police staff. This could be based on the success of non-sworn investigators. Such expansion would be the most cost effective option [Button et al 2008]. If fraud and cybercrime are to be subject to police response then expanding rather than reducing their numbers should be paramount.

Two examples of police force re-engineering

Australian Federal Police

A number of Police forces have undertaken dramatic internal re-engineering and they could provide the basis of significant internal re-engineering within the police service of England and Wales. Reforms implemented in Australia and New Zealand may also offer insights into the benefits of change. These involved the Australian Federal Police and the New Zealand Police Service. For the AFP reform began with a reduction in the number of police ranks; the alignment of police support staff with police ranks to create a unified force and granting the commissioner chief executive status [Loveday and McClory 2007:28].

By simplifying payment structures the AFP was able to make more cost- effective use of personnel. This was based on a recognition within the AFP that 'flexible investigation teams' consisting of police officers and civilian staff were the key to effective investigations [Loveday and McClory 2007:29]. The need for high quality investigation reflected a changing pattern of crime to which the AFP responded and which included. The threat of international terrorism, the drugs trade, people trafficking, money laundering and the rise of organised crime across South East Asia. Each called on specific areas of expertise. As was to be argued:

'Bringing a workforce of police technicians, administrative officers and a range of specialist personnel employed under the same terms and conditions was a major step in creating a cohesive and flexible workforce' [AFP 1997:16].

On this basis a Team Based Model within the AFP was to be established. Within the model the composition and size of each Team would depend on the nature and complexity of the task undertaken. A 'Team' approach has encouraged the identification of Team Leaders and

Team Co-ordinators. Selection is based on the capability and competence of individuals not on rank or seniority.

The identification of new challenges confronting the AFP led to a range of technical specialists and not just sworn officers being recruited to the AFP. Specialists could be non – sworn officers who would be integrated into the AFP. Examples included forensic science staff, forensic accountants and information technology specialists. Where appropriate specialist non-sworn staff would also be identified as Team leaders or co-ordinators.

A unified approach was supported by the AFP Association representing the interests of both sworn staff and non-sworn staff. The creation of common pay rates for all staff and the extension of police powers exercised by non-sworn personnel served to sustain a unified workforce.

New Zealand Police

In New Zealand the Police Act review of 2006-2008 led to the introduction of reforms to enhance internal flexibility within the workforce and direct recruitment of specialist staff who had expertise the police service lacked. As was argued:

'*The need to confer specific police powers on police staff reflects the difficulty in training sworn staff to deal with every aspect of contemporary crime. Examples are technology based crimes requiring specialist understanding or technical skills, international organised crime groups including cyber- crime , complex fraud offences and terrorist threats*' [Loveday and McClory 2007:31].

For New Zealand Police as with the AFP the internal review encouraged the creation of a unified service and to create a greater mix of appropriately empowered staff. It was recommended that trained specialists on joining the police would be granted specific police powers which allowed them to contribute to policing immediately [Loveday and McClory 2007:31; McCardle et al Police Act Review: New Zealand Police 2008] and reflected the limitations of established police employment structures. More flexibility was needed along with more specialisation and when to this was added to a move toward a Team based policing changes to employment arrangements were viewed as crucial. As a result the proposed employment structure was the centre piece of New Zealand's reform programme designed to enable the police service:

'*To establish a greater mix of appropriately empowered staff to contribute to individual and community safety covering the full range of policing duties from minor incidents to major emergencies'* [Loveday and McClory 2007:31].

The review was to also highlight the need to for much greater flexibility enabling staff to move between constabulary and non-constabulary roles and to take up and relinquish certain police powers when required. A significant recommendation concerned civilian staff on whom police powers could be conferred where appropriate [Loveday and McClory 2007:33]. The move to greater flexibility in employment was reinforced by the New Zealand Police Federation decision to extend membership to civilian personnel which cemented a unified approach.

The AFP and New Zealand Police demonstrate that internal re-engineering can be accomplished. In both cases this was to be also driven by a changing criminal environment and desire to maximise the use of all operational staff. The restructuring undertaken a decade ago has achieved the set objectives. This suggests that significant change management can be

undertaken by police forces even where this challenges long established procedures, structures and culture.

Police Organisational Culture

Yet the potential influence of police organisational culture as a barrier to reform cannot be ignored. Recent evidence of this within England Wales arose in relation to relatively limited reform undertaken there. The introduction within the 2002 Police Reform Act of Police Community Support Officers as a uniformed supplement to operational police generated great opposition across the police service and was led very largely by the Police Federation.

If the public were ready to accept PCSOs as an element of visible policing it was apparent that in London the decision to introduce them was highly political. Ian Blair as Metropolitan Commissioner noted that the London Boroughs had discovered '*an interesting gap in legislation which was that there was nothing to stop anyone setting up a police force if they want one*'. He added that:

'Kensington and Chelsea proposed to create its own constabulary to police not just parks but streets not just city centre shopping areas or its own council estates but the whole borough. This threatened the balkanisation of the policing of London, and I was determined to prevent that if possible' Blair [2009:125].

The initiative led the Police Federation to attack the PCSO programme and to denigrate PCSOs as 'plastic policemen' who provided 'policing on the cheap'. This argument was to be amplified by media coverage. Yet in reality he PCSO role was to form the bedrock of neighbourhood policing strategy adopted nationally by the police service after 2002. For the Commissioner it was a hard fought battle. As he observed, prior to their introduction:

'*On two successive days I had to go first to the ACPO conference and make a direct intervention to disagree openly in public with the ACPO President [who was 'unconvinced' about the value of PCSOs] and then to the Federation Conference to face a hostile and silent hall*' [Blair 2009:126].

Ultimately the PCSO initiative was to be undermined through the austerity programme of the Conservative led Coalition government which required a 20% cut in police spending. It was noticeable that most of the cuts were to be directed at police staff employees and PCSOs [Loveday 2015; Unison 2013].

In a further planned cutback by government in late 2015, several police forces –including the MPS- planned to close down the PCSO role in its entirety [Loveday2015]. This also provided a ready demonstration of police commitment to capacity over capability as PCSOs were, by 2015, acting as the primary local intelligence stream to operational police officers across London [Loveday and Smith 2014].

Police response to the Direct Entry Initiative

The impact of police organisational culture has been again highlighted with the introduction of direct entry into the police service. Following a recruitment drive for potential candidates over 600 applications were to be made [Smith 2016]. Yet of these just eight candidates were to take up operational roles. The attrition rate proved to be remarkably high [Smith 2016 forthcoming]. Recent research provides an explanation for this. It ranges from highly exaggerated standards required of direct entrants through to open professional hostility from both police trainers and chief officers [Smith 2016 forthcoming].

Research suggested there was vocal opposition from the Superintendents Association to direct entry, which represented the very rank to which the new entrants aspired [Smith 2016:13]. Elsewhere successive chief officers proved to be equally vocal in their opposition to direct entry [Hickey 2016]. Direct entry officers were to record that they had been initially interviewed by senior officers in a manner which suggested 'they did not support the scheme' [Smith 2016]. One candidate was to discover that he had failed a final interview panel because he did not appear 'to exhibit the intangible presence' that superintendents were expected to have [Smith 2016]. Elsewhere direct entrants were to reflect on a 'Meet the ACCs Event' which provided an opportunity for chief officers to inform them of their opposition to the programme [Smith 2016 forthcoming].

This most recent response to limited change in the police service, suggests that cultural impediments to reform and modernisation can also be held at the top of the organisation. It has also been found that the initial sifting process was guided by the extent to which candidates knew and empathised with the police service [Stubbs 2016]. Feedback from direct entry officers indicated that they had, however, found abundant evidence of poor management and leadership in the short time they had served as trainee superintendents - enough indeed to entirely justify the original experiment [Smith 2016].

The experience of direct entrants may confirm a more general cultural trait most recently identified by the Chair of the National Police Chief's Council [NPCC]. This officer has argued that policing in Britain is blighted by a 'defensive and closed culture' which, unlike other public services, appears unable to learn from failure not least because of the rampant blame culture which also thrives with in the police service [Dodd 2016].

Despite the problems identified above police forces have been further encouraged to adopt new approaches to recruitment. Recently a number of forces have signed up to the proposed direct entry for inspector rank. Over 900 people were to apply for direct entry at forces outside London in mid- 2016. Of these just 16 were deemed eligible by the police national assessment centre to go through to the next stage consisting of an interview with their respective forces [Weinfass 2016b].

As with direct entry to superintendent rank the attrition rate among applicants has again proved to be remarkably high. Within MPS, a participating force, the Metropolitan Federation chairman has recently condemned direct entry by reference to professional police exceptionalism and the need for prior operational experience [Weinfass 2016c].

Conclusion

In conclusion it would be irresponsible not to highlight the competing challenges with which the police service must wrestle. These would include inter alia the threat of domestic and foreign terrorist attack, a public reassurance role along with the growing challenge of community mental health issues which currently engages much police time.

Nor can recent initiatives undertaken in response to fraud and cybercrime be overlooked. Thus the MPS has recently established within Operation Falcon the Metropolitan Police Cyber Crime Unit [MPCCU] to tackle the most serious incidents of cybercrime and fraud and works in partnership with the NCA. In the City of London the police will engage private law firms to target cybercriminals and fraudsters [Dodd 2016].

It is also evident that at a higher police level the size and nature of the problem has been recognised. This is reflected in the response of the National Police Chief's Council to this

threat, the creation of the Independent Digital Ethics Panel for Policing and the formation of the new Centre for Digital Research and Industrial Collaboration.

In late 2016 the new National Security Centre [NCSC] led by former directors from GCHQ, was also established in London and is expected to '*transform how the UK tackles cyber security issues*' [Mason 2016]. Additionally the introduction of the NPCC Digital Investigation and Intelligence Programme [D11] has also served to enhanced mainstream capabilities for digital crime. To this needs to be added the increasing operational role of the Regional Organised Crime Units within this sphere. The expansion of these units begins, in fact, to respond to recommendations made earlier by academic commentators, that fraud investigations should be 'reorganised along the lines of serious crime with national or regional fraud squads to overcome perceived limitations on police resources' [Doig et al 2011].

Yet it is also evident that the size of the case-loads of these new units is likely to extend only to major cases. Within the NCA attention is directed to 'elite cyber criminals' and the NCCU to date has, in fact, dealt with just 16 investigations against organised crime groups [Mason 2016]. Below the elite and middle rank of criminality remains 'volume cybercrime' currently estimated to involve 2.5 million cases per year and which is also subject to significant under reporting. This is unlikely to be dealt with by any specialist unit. As a result '*cybercrime is currently seen as a high reward, low risk activity for a growing number of criminal groups*' [Mason 2016].

Moreover as cybercrime ceases to be the reserve of wealthy criminals with resources 'it becomes available to everyone' and, as the Head of the NCCU has argued recently '*from a law enforcement perspective that changes what we need as a response and it also changes the type of officer we need*' [Hulett quoted in Mason 2016].

Given the size and nature of the threat posed by fraud and cybercrime it has been argued that one solution would be to create a National Fraud Authority to deal with fraud offences [Button et al 2014].Yet this solution might marginalise the police service from what is predicted to be a major element of future criminal offending. Yet to begin to engage with the new crime profile the police may have to accept a modernisation programme that on current evidence could prove difficult implement.

This has to a degree been recognised within the police hierarchy. This has been reflected in the decision within the National Police Chief's Council to create new portfolios on fraud and cybercrime. Moreover on an individual basis some police forces are now using volunteers to form specialist organisations and at least one force now actively responding to the threat with the creation of specialist units to counter this challenge. In one force a former hacker has, in fact, been employed as a police staff manager. The greater employment and use of unwarranted staff may also become more frequent in response to this challenging crime type.

However piece- meal change is unlikely to prove to be a substitute for the kind of modernisation which is now required. This in turn must be expected, inevitably, to engage with the police organisational culture which remains a potential impediment to change. Yet it is argued here, only by way of significant change in recruitment along with organisational re-engineering, will the police service ever prove likely to exhibit a level of capability that the rise in fraud and cybercrime now demands.

END

Bibliography

Allen C [2016] CSEW: Fraud most common crime, Police Professional: News, retrieved at http://www.policeprofessional.cpm/news.aspx?id=26705;

Barrett D [2015] Police 'dismissive' of online crime victims, Daily Telegraph December 23rd;

Blair I[2009] Policing Controversy, Profile Books, London;

Button M Blackbourn D and Tunley M [2014] The Not so thin Blue Line Afterall? Investigative Resources dedicated to Fighting Fraud/Economic Crime in the UK, Policing: A Journal of Policy and Practice, OUP;

Button M and Cross C [2016 Forthcoming] Technology and Fraud: The Fraudogenic Consequences of the Internet Revolution;
Button M,, Johnston L and Frimpong K [2008] The Fraud Review and the Policing of Fraud: Laying the foundations of a Centralised Fraud Police or Counter Fraud Executive? Policing 2: 241-250;

Collinson P [2016] Cybercrime much of it from Russia and Ukraine is flooding Britain says UKs top anti-fraud commissioner, The Guardian 27th August;

Dodd V [2016] Police hire law firms to seize fraudsters assets-for profit, The Guardian 17th August;

Dodd V[2016] Police Chief's leader attacks 'culture of defensiveness', The Guardian July;

Doig, Johnson S and Levi M [2001] New Public management, old populism and the policing of fraud, Public Policy and Administration;

Ford R [2016] Fraud doubles the number of crimes, The Times;

Foreman J [2016] Forget lists, just put police back on the streets, Comment , Mail on Sunday 21st August;

Grierson J[2016] Plans for London to have 600 extra armed officers to combat threat from terrorists, The Guardian August 4th;

Hickey H [2016] No evidence direct entry of any major benefit- New Merseyside boss says the right people to lead the force are already in it, Police Oracle 3rd July;

Hill A [2016] Child abuse work 'may hit police effectiveness', The Guardian July;

HMIC [2015] Real lives, real crimes: A study of digital crime and policing, HMIC Globe House, London;

HMIC [2015] PEEL: Police Efficiency 2015, HMIC Globe House, London;
Home Affairs Committee [2015] Oral Evidence: The work of the National Crime Agency HC475 Tuesday 8th December, retrieved at http://data.parlaiment.uk/written evidence/committeeevidence.svc/evidencedocument 14/12/2015;

Loveday B [2008] Workforce Modernisation in the Police service, International Journal of Police Science and Management, 10[2]:136-144;

Loveday B[2015] Plodding Along: police personnel configuration needs urgent reform, Policinginsight November 20th;

LovedayB and McClory J [2007] Footing the bill, Reforming the police service, Policy Exchange, London;

Loveday B and Smith R [2014] A critical evaluation of current and future roles of PCSOs and Neigbourhood Wardens within the MPS and London Boroughs, International Journal of Police Science and Management,

Mason G[2016] Hacked off: Cyber security in the UK, Police Oracle August, retrieved at http://www.policeoracle.com/news/police;

National Fraud Intelligence Bureau [2016] Cyber Dependent Fraud April 2015-March 2016; Cyber Enabled Fraud April 2015-March 2016, City of London Police;
ONS [2016a]: 'Crime in England and Wales-Year ending March 2016; retrieved 1 February 2017 https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2016

ONS[2016b]: Overview of Fraud Statistics: year to March 2016: retrieved 23 January 2017 from https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudstatistics/yearendingmarch2016

McCardle H , Webb M and Harvey P [2008] Police Act Review: Discussion Documents and Policy Papers for the Development of a new Policing Bill, Wellington, New Zealand;

Naughton J [2015] These days crime doesn't pay-unless it is done online, The Observer March;

Police Act Review [2008] Discussion Documents and Policy Papers for the Development of a new Policing Bill,

PAC[2017] Protecting Information across government: downloaded on 3 February 2017 from https://www.publications.parliamnent.uk/pa/cm201617/cmselect/cmpubac/769/76902.htm

RUSI [2015] Democratic License to operate, RUISI, London.

Smith R[2016] 'Don't call me Ma'am: Direct entry into leadership roles in British policing, The Police Journal,1-16;

Smith R [2016] New Insights on police culture: A critical evaluation of direct entry into senior leadership roles in the police service, Doctoral Thesis Portsmouth University forthcoming;

Stubbs G [2016] Changing Culture Presentation to Evidence Based Policing Christ Church University Canterbury, 23rd June;

Sylvester R and Thomson A [2016] New Age of criminality leaves police struggling to catch gangs, The Times March 24th;

Thomas G[2016] New figures, new thinking: How to deal with the cyber- crime problem, Policing Insight July 21st;

Travis A[2016] Police urge campaign against cybercrime, The Guardian July 22nd;

UK Legislation [2016] Investigatory Powers Act, 2016 downloaded on 3 February 2017 from www.legislation.gov.uk/ukpga/2016/25/contents/enacted/data,htm

Unison [2016] Out of Sight, Out of Mind, Survey of PCSOs, Unison, London;

Unison [2013] Trouble in the Neighbourhood, Government cuts to neighbourhood policing take their toll, Unison London;

Weinfass I [2016a] Accountability of new volunteers with police powers called into question, Superintendent Association president elect raises concerns, Police Oracle January 26th retrieved at http// www.police oracle.com/news/uniformed-operations/2016/jan/25/accountability;

Weinfass I [2016b] Hundreds apply to become direct entry inspectors, Met Police belatedly comes on board in a boost to the inaugural round of recruitment , Police Oracle, August 8th, retrieved from http://www.policeoracle.com/news/police_staff/2016/Aug/05/;

Weinfass I [2016c] Met fed chairman slams direct entry inspector recruitment plan, Police Oracle August 16th, retrieved at http://www.police oracle.com/news/Met-Fed-chairman-slams direct entry inspector- report.