Policing Cybercrime[1]

Author:

Esther Snell, MSc (Royal Holloway, 2015).

Abstract: Cybercrime has added a new dynamic to the nature and rate of criminality that has created new challenges for policing agencies around the world. This article considers the duties of the police in the UK and asks whether these roles remain realistic and achievable in the cyber space. Ultimately the discussion considers whether it is time for policing to embrace change and seek out a new approach to meeting the challenges of cyber offending.

In 1973 the financial world was rocked by a crime that would become known as one of America's biggest ever computer frauds. The scandal occurred at Equity Funding Corporation of America and involved a conspiracy of 100 employees, including some of its top executives, who sold fake policies of mutual funds and life insurances to fictitious customers. The scam, which ran from 1964 to 1973, netted the schemers $2 billion, with a further $25 million in counterfeit bonds and $100 million in unaccounted for assets. Central to the running and success of the scam was the use of a dedicated computer that created and maintained 64,000 phony policies. This ambitious and long-running fraud was ultimately exposed by a whistleblower. Whilst 19 employees and 2 auditors were imprisoned for their offences, the sentences were rather light: executive Stanley Goldblum who came up with the scheme, served only 3 years. In audacity and novelty however the crime contains all the elements of a Hollywood blockbuster and indeed it has grasped the imagination of film makers, writers and audiences around the world. But could those responsible for the crime, or those tasked to investigate it, have realised that it signalled a sea-change in both the nature and rate of offending?

The impact of cybercrime

Since 1973, as computers have become increasingly more accessible, affordable, diverse and pervasive, the nature and rate of offending via technology has evolved and grown to enormous proportions. Today technology is used to commit, not just fraud, but also theft, harassment, espionage, paedophilia, smuggling, piracy and trafficking. And on top of this a whole new genre of crimes have emerged aimed just at computer devices themselves. And the number of such crimes is large. In October 2015 the Crime Survey of England and Wales revealed that 5.1 million frauds and 2.5 million acts of computer misuse (such as the

[1] This article is to be published online by Computer Weekly as part of the 2016 Royal Holloway information security thesis series. It is based on an MSc dissertation written under the supervision of John Austen, a consultant lecturer in the ISG, Royal Holloway, University of London.

distribution of viruses and the hacking of social media and email accounts) had occurred in the 12 months before May 2015 and these were only those offences the survey uncovered. Distinction is drawn between cyber-dependent and cyber-enabled crime. Cyber-dependent crimes involve acts, such as hacking and the distribution of malware, that only take place in the cyber space. Cyber-enabled crimes, however, are traditional offences that now have a cyber-element such as a mobile phone or the internet. Both types of offending pose problems, with malware, extortion, and vulnerability through social media being particular current concerns. One vendor reported that 317 million new pieces of malware were created in 2014, almost a third of which were 'virtual machine aware'. While Mandiant found that some attacks went undetected in networks for an average of 356 days. The impact of such crimes can be far reaching as technology provides 'force amplification'. The 2015 Android bug was said to have infected 950 million devices. Such offending poses a problem to organisations, individuals and nation-states. One study of 664 UK businesses estimated that 90% of large, and 74% of small and medium enterprises, suffered a security breach in 2014. While a survey of 24 countries concluded that 431 million people had fallen victim to cybercrime in a twelve month period. Whilst the cost to individual victims lies on average between 50 and 850 US dollars annually, the brunt of the cost appears to fall on the private sector. The recent TalkTalk breach, which saw the loss of financial data belonging to 157,000 customers, will cost the company between £30 and £35 million.

Not unsurprisingly such risks put people off using the internet and means that cybercrime stands directly in the way of the benefits the internet offers. The Mckinsey Global Institute found that between 1994 and 2011 mature countries who utilised the internet saw their Gross Domestic Product increase by over $500 per capital. The Industrial Revolution took 50 years to achieve such growth. The UK is the largest digital economy in the G20, with the internet contributing 10% of its GDP. In 2015 the internet was expected to contribute £180 billion to the UK economy and it is estimated that the Internet of Things could increase by £303 billion between now and 2030.

The internet is a resource that must be protected, but just how this is achieved presents something of a challenge. US Assistant Attorney General Leslie R. Caldwell encourages us that 'for all its scope and complexity, cybercrime is not an unsolvable species of crime'. However, it remains doubtful whether we are winning the war on cybercrime.

Police objectives in the physical space

When thinking about crime control the first port of call for most people are the police. Modern constabularies have a wide remit of duties, but their primary goals are to prevent and detect crime, to maintain public order, and to provide assistance to those in need. Although a large number of crimes are never reported or investigated, or if they are investigated are not solved, these goals are realistic for tackling crime that occurs in the physical off-line world. However, a large proportion of crime today occurs online or involves technology and these crimes present significant challenges to policing agencies in meeting their objectives.

Crime prevention is a core duty of the modern police and indeed has been for the past 187 years. Prevention was the primary duty of the Metropolitan Police when they were introduced in 1829 and so policing agencies have significant experience in preventing physical crimes. In that time the police have learnt to regulate criminal behaviour within and with the help of local communities, set up education programmes, encouraged the use of technology to protect our property and ourselves, and we have also learnt how to design buildings and outdoor spaces that discourage offending. Similarly the detection and investigation of crime has benefitted from advances in science and technology; from the relatively speedy communication of the telegraph, to the discovery of fingerprinting and later DNA profiling.

Maintaining public order is also is achievable within the context of the physical world. Although budget cuts have hindered the number of officers on the streets, the presence of a bobby on the beat on a Friday night or at a football match can still work somewhat (if not perhaps completely) to maintain public order through the visibility of an officer. A physical reminder of the law can act as a deterrent. This is supported by legislation that enables the police to arrest and detain those behaving illegally and ultimately the threat of being discovered and punished for a crime acts to deter many from offending.

The police, as one of the emergency services, are often the first to respond to criminality and to provide assistance to the victims. Many (although not all) crimes leave visible signs of having occurred that are often recognisable to ordinary people. Anyone, therefore, who sees these signs can call the police and the police have a physical crime scene to examine. Ultimately, in fulfilling their duties to prevent and detect crime the police are providing assistance to victims in helping them gain justice for their mistreatment.

Police objectives in the cyber space

However the world is changing. Criminality is moving online, its volume is increasing, evolves constantly and rapidly, often leaves no clear sign of its occurrence, and leaves no easily accessible physical crime scene to be examined. Achieving the policing goals, therefore, presents specific challenges within the context of online crime.

The detection of online crime presents increased challenges for policing agencies. One media investigation from 2015 claimed that cybercrime in the UK was being ignored, with only 1 per cent of reported crimes investigated and only a small fraction of cases prosecuted. The UK police are not alone in facing such criticisms. It has been argued that in America low level online offending (measured by financial impact) is often not investigated, leaving offenders to act with impunity. One approach to crime argues that crime thrives where there is a motivated offender, suitable targets, and the absence of capable guardians. Cybercrime ticks all these boxes and because of this it has become a low-risk and high-reward activity.

Part of the problem is that there are not enough officers in the UK with the appropriate skills to investigate cybercrime. The introduction of the Mainstream Cybercrime Training in 2014 formed part of the government's pledge to 'create a hostile environment' for cyber criminals by increasing the number of security professionals and strengthening law

enforcement. The programme is made up of 4 tiers of training with all staff expected to participate in the large number of available tier 1 e-learning packages and also the tier 2 open source research training. The training aimed to increase the skills, tools and knowledge of 6,000 police officers and civilian staff in its first year. Whilst this seems a lot when placed in the context of 207,140 police workers in England and Wales, it would take many years to get through all police personnel. However in recent months effort has been made to attract skilled recruits into this arena, and even this month it was announced that volunteers with IT skills would be used to investigate cyber offending.

Another challenge of investigating cybercrime is that the internet has increased the reach of criminals so they can now strike from thousands of miles away. Cybercrime is often transnational with the offenders operating in a different country to that in which the victim lives and the police are working. The use of proxy servers, physical distance, international politics, and lack of legislation and national agreement to give up suspects for trial in another country, all make it difficult to investigate cybercrimes and often impossible to bring the offenders to justice. A police force might spend months and significant resources investigating a case committed in another country, only to have the investigation dropped when the evidence is passed to another jurisdiction.

Trying to prevent cybercrime also poses challenges. The police have devised and encouraged the use of education programmes, and used social media to raise awareness of and send warnings about cybercrime. However budget cuts have meant community engagement has perhaps not been as extensive as some would have liked. Calls for 'better housekeeping' places greater responsibility on the public to take measures to protect themselves. But people cannot be forced to patch, install firewalls, and remember to reconfigure software, or avoid dodgy sites. How would this be monitored? Also some people will always be more computer savvy than others and better able to protect themselves. But those with less knowledge are left unprotected. Many modern scams are sophisticated and victims, being unprepared for how convincing they are, find themselves conned. All the while, the crimes themselves are constantly evolving to take advantage of vulnerabilities, new technologies and social trends, and it is difficult and time consuming to keep on top of this. Guidance and support then is needed by many people, but do the police have the skills and resources to provide that to the extent needed?

Maintaining public order online is also problematic. The police cannot have a presence in all chatrooms, monitoring conversations and checking activity. Even if they could, would the presence of officers online have the same visibility and impact as they do in real life and the same deterrent effect on would-be offenders? The difficulties of maintaining public order online is increased through many users' use of routers that provide anonymity. Approximately 2 million people use TOR daily, and for many it provides a valuable and important service. Also the online world exceeds national legal borders and a problematic user might not reside in the same country as the police officer present. Ultimately, as discussed earlier, the majority of crimes are not investigated let alone prosecuted and punished. Criminals, then, do have a good chance of getting away with their offences and this message does not help the maintenance of order online.

The Mainstream Cybercrime training mentioned above was designed to enable all police officers and staff to be able to respond to digital crime. The capability of first responders is crucial in building the public's trust and confidence in the police's ability to tackle cybercrime. This is important if victims are to be encouraged to report these crimes. The government's own research suggests that not all police officers and support staff are sufficiently confident in dealing with electronic offending. The training, however, did appear to be successful in introducing participants to online crime and increasing their confidence in using technology to investigate it.

Reassessing police objectives

The police, then, are facing a new dimension of criminality and it is one where modern policing goals meet particular challenges when placed in the cyber space. However this is not new. Social and economic changes have challenged existing methods of social control and policing objectives before and new approaches were developed to meet those changing circumstances. Notably this refers to the transformation in policing style that occurred in 1829 with the establishment of the Metropolitan Police Service.

Before 1829 social control was maintained through a community system of Justices of the Peace, watchmen and constables, with entrepreneurial thief takers operating in some places. All men were required to contribute to the Watch to maintain social control in their communities. Crime prevention was achieved partly by the fact that people lived in relatively small communities where offenders were likely to be recognised and have to face the formal or informal consequences of their actions. This was supported by a system of public punishment that showed to others the penalty of crime. Underpinning all this were religious beliefs that God was always watching and offenders would be punished, if not on earth then certainly when arriving at the pearly gates. When crime did happen, as of course it did, the victim was responsible for bringing the felon to justice. However they were, ideally, supported by the community through the Hue and Cry, which was used to chase suspects and bring them to justice. This was not a fail proof system however and, despite the message of certain justice, many felons got away with their crimes.

The introduction of a formal system of 3000 uniformed police officers, accountable to a minister of state, was a departure from the traditional methods of social control. They only operated at first within a 10 mile radius in London, but the new force was the start of what we would recognise as our modern police. Its introduction occurred because of the great economic and social changes brought about by the Industrial Revolution. As large numbers of people flocked to the industrial centres in search of a better life traditional functions that regulated social control could not cope. Traditional community methods of policing collapsed as the large urban cities broke social bonds and brought anonymity. Alongside the increasing reassessment of religion that questioned the direct involvement of God in human affairs, earlier fears that crime was growing out of control only got worse. This led to a reassessment of how crime was to be managed; and the result was the new police.

More nuanced interpretations now recognise the continuities between the traditional and new policing systems. Also of course it would be wrong to give the impression that policing

strategies have not changed since 1829. However there is no doubt that the developments that happened in this year were significant. This was not, however, an easy or uncontested occurrence; resistance took decades to overcome. The late 1700s and early 1800s saw society change from village- to urban-based communities. Two hundred years later we are experiencing a similar change as our individual lives and societies have moved from urban to global existences. Crime takes advantage of our changing lifestyles, and creates opportunities from our evolving interactions and circumstances. Most people want to live in a world where they are safe and where social justice can thrive. This might mean, however, that we need to rethink our policing goals and approaches to criminality.

What is the future of cybercrime policing?

What might that change look like for the police? There are different pathways this could take. One option would be to enhance police services' abilities to achieve their current objectives in the cyber domain. This would see policing agencies receiving a much greater amount and wider range of resources to be able to detect and prosecute crime. This would include a significant increase of officers skilled in IT, as well as a considerable expansion in the training agenda. Both these elements would be expensive and require a large injection of capital. They would also require the passing of extensive new powers of surveillance, where messages can be unencrypted, automated checking occurs, and full recordings of chatrooms and forums made available in order to detect and investigate offending. All this would mean a surrender of privacy and civil liberties: a potential post-modern '1984' existence that would be abhorrent to many.

A second direction would be to take parts of the policing objectives away from police services and reassess what can realistically be accomplished and by whom. While the police concentrate on public hardening and support, in an effort to prevent the occurrence of cybercrime, the investigation of online offending would be undertaken by private companies. In this scenario individuals take greater ownership for their own online protection. They could take out 'roadside assistance' style subscriptions, with premiums based on assessments of risk, which would provide help in the event of them becoming a victim of cybercrime. Perhaps ultimately it is accepted that, at least for now, investigation and prosecution in this space is difficult and resources are aimed at the big cases where there is a clear and visible impact that can be used to deter future offending.

Or maybe the direction of policing will take an altogether different route. Much like the transformation led by Sir Robert Peel in the 1800s, something new will emerge with fresh goals and new ways of operating that better address the new dynamic of criminality.

Biography: Esther Snell is a senior lecturer in criminology and Head of Law and Criminology at Southampton Solent University. Specialising in the history of crime and punishment in the early modern period, Esther's research is particularly interested in perceptions and representations of offending and justice. She has published and presented in this area both nationally and abroad. More recently Esther's attention has turned to information security

and electronic crime. This present article is influenced by her current research on the Mainstream Cybercrime Training which was conducted in 2015.