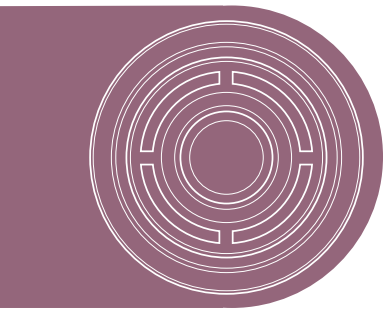
CYBER CRIME:

An inspection of how the Criminal Justice System deals with Cyber Crime in Northern Ireland

June 2017

Criminal Justice Inspection
Northern Ireland
a better justice system for all



CYBER CRIME:
An inspection of how the Criminal Justice System deals with Cyber Crime in Northern Ireland

Laid before the Northern Ireland Assembly under Section 49(2) of the Justice (Northern Ireland) Act 2002 (as amended by paragraph 7(2) of Schedule 13 to The Northern Ireland Act 1998 (Devolution of Policing and Justice Functions) Order 2010) by the Department of Justice.

June 2017

Criminal Justice Inspection
Northern Ireland
a better justice system for all

Contents

List of abbreviations

ACPO	Association of Chief Police Officers
ATM	Automatic Teller Machine
C1	PSNI Reactive and Organised Crime Branch
C2	PSNI Serious Crime Branch
CCC	PSNI Cyber Crime Centre
CCTV	Closed Circuit Television
CERT-UK	UK National Computer Emergency Response Team
CiSP	Cyber-security Information Sharing Partnership
CJI	Criminal Justice Inspection Northern Ireland
DDoS	Distributed Denial of Service
DESU	PSNI District E-Crime Support Unit
DOJ	Department of Justice
DPC	District Policing Command
ECU	Economic Crime Unit (within PSNI)
FBI	Federal Bureau of Investigation
GB	Great Britain
HMIC	Her Majesty's Inspectorate of Constabulary
ICIDP	Initial Crime Investigators Development Programme
ICT	Information Communication Technology
IT	Information Technology
IP	Internet Protocol
ISP	Internet Service Provider
LPT	Local Policing Team
LSD	Lysergic acid diethylamide
MDMA	Methylenedioxymethamphetamine
MoRiLE	Management of Risk in Law Enforcement Risk Prioritisation
NCA	National Crime Agency
NCCU	National Cyber Crime Unit
NCSC	National Cyber Security Centre
NCALT	National Centre for Applied Learning Technologies

NCSP	National Cyber Security Programme
NFIB	National Fraud Intelligence Bureau
NICS	Northern Ireland Crime Survey
Niche	PSNI electronic case management system
NIPB	Northern Ireland Policing Board
NPCC	National Police Chiefs' Council
NUIX	An IT company software platform for indexing, searching, analysing and extracting digital information.
OCTF	Organised Crime Task Force
ONS	Office for National Statistics
PCSP	Policing and Community Safety Partnership
PoliceNet	The PSNI intranet
PPS	Public Prosecution Service
PSNI	Police Service of Northern Ireland
ROCU(s)	Regional Organised Crime Unit(s)
ROSIE	Research, Open-source, Internet and E-mail training course
SBNI	Safeguarding Board for Northern Ireland
SOCA	Serious and Organised Crime Agency
SOTP	Student Officer Training Programme
SPR	Strategic Policing Requirement
SQL	Structured Query Language
TNA	Training Needs Analysis
UK	United Kingdom
US	United States of America
4-MEC	4-Methylethcathinone

Chief Inspector's Foreword

Our dependence on digital technology is increasing, but for many citizens the risks associated with this technology is neither fully appreciated nor understood. It is only when someone becomes a victim of fraud; their intimate details are shared or exploited without their knowledge or consent; or their children are groomed by unscrupulous, insensitive and evil perpetrators who are seeking to exploit their human frailties, that the full understanding of our vulnerability becomes apparent.

Perpetrators are often based in different countries and their identity and the full range of their activities are often unknown. It is clear that the state has a responsibility to protect its citizens and the range of threats and risks extend well beyond the competence and capacity of our traditional protectors the police. The internet providers - the industries and businesses who encourage our use of digital technologies - are making considerable profits from their services and should be leading the way in making the available technology safer for us to use.

Equally there is an onus on individuals and businesses to take steps to increase their own awareness of cyber crime and online security and to protect themselves from this threat.

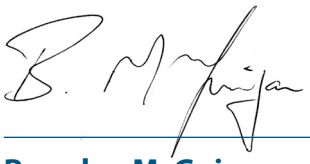
This report highlights the differences between cyber-enabled and cyber-dependant crime and outlines the response we should receive from the criminal justice agencies. Frontline police officers do need to know how to investigate cyber-enabled crime, such as where stolen goods are sold on-line or emails are used to support criminal activity, and be able to access the technical support that is required to support them in bringing offenders to justice. Specialists are also required to provide advice and guidance and to conduct more complex and serious crime investigations and to interface with the agencies and organisations at the leading edge of this science.

Getting the balance right for both now and the future is critical. This report identifies the need for a comprehensive analysis of cyber

crime as it affects Northern Ireland including the under-reporting and recording of the cyber crime types, and the implications for policing of emerging criminal developments in the misuse of technology. This will help the Northern Ireland Policing Board (NIPB) and the police to make the necessary decisions about demarcation of responsibilities and resourcing. Partnership working is critical to assist the Police Service of Northern Ireland (PSNI) in preventing and reducing crime in this area.

This report also makes six further operational recommendations for the PSNI to help improve service delivery and public safety. The last recommendation requires a joint response from the Department of Justice (DoJ) and the PSNI to increase public and business community awareness of the current threats and actions needed to improve internet security.

This inspection was led by Dr Ian Cameron and supported by Rachel Lindsay. My sincere thanks to all who contributed to this inspection.



Brendan McGuigan
Chief Inspector of Criminal Justice in Northern Ireland

June 2017

Executive Summary

Cyber crime is a relatively recent phenomenon and its prevalence has increased exponentially in recent years at the same time as rates for the traditional crime types have fallen. More crime is committed online than offline and the cost of cyber crime to the economy is substantial.

It is high reward and relatively low risk, anonymous and borderless, and cyber crimes can be perpetrated on a scale that is of a different magnitude than other crime types.

The general lack of understanding of cyber crime and the ways in which it affects individuals and businesses means that it is significantly under-reported to police.

The nature of cyber crime requires a multi-agency, cross-jurisdictional and cross-national approach and the Police Service of Northern Ireland (PSNI) was fully incorporated into national policing arrangements for major incidents and for sharing specialist capability across the United Kingdom (UK).

The PSNI had formed a Cyber Crime Centre (CCC) with expertise to investigate cyber-dependent crime, and which provided forensic and technical examination of mobile phone and computer devices on behalf of the PSNI. The officers had built up excellent relationships with a number of partners from law enforcement, business and academia to investigate cyber crime and share information, and had prosecuted complex cases.

Cyber crime was a fast-developing area and a comprehensive assessment of the scale and extent of cyber crime was necessary for the PSNI to provide an effective response to the current threat, to allocate resources and to meet investigative and victim needs. There was a recognised under-reporting of cyber crime. Police recording did not capture the full extent of reported cyber crime and cyber fraud; this created a gap between the true scale and impact of cyber crime and that which was reported in crime statistics.

Almost all crime now had a technological aspect; as people had moved their communications and shopping online; criminals had done the same with their offending. The scale of demand for digital forensic examinations, coupled with the increasing capacity of devices had created examination backlogs. Whilst the PSNI had taken

a number of steps to address this issue, delays impacted on victims of crime, the effectiveness of criminal investigations and the speed of justice through the courts, and the PSNI needed to take action to reduce the number of examinations awaiting completion.

The digital forensic capacity of the CCC was supported in the Police Districts by local E-Crime Support Units which performed a valuable role. The demand for device examination had exceeded the Units' capacity, and recognition of this had led to an internal review which Inspectors welcomed as an opportunity to re-examine the effectiveness of the provision of digital forensics for District policing, and online access for investigative purposes.

From April 2015 fraud and related cyber crimes were no longer reported to the PSNI but to the 'Action Fraud' national reporting centre. The transition had encountered some initial difficulties and Inspectors found a mixed level of understanding about the reporting arrangements among front-line police and the business community. Work was taking place to improve IT information transfer, and the PSNI had taken positive steps to improve fraud investigation management and monitoring to improve outcomes. Inspectors considered it an opportune time to review the effectiveness of this approach to tackle fraud.

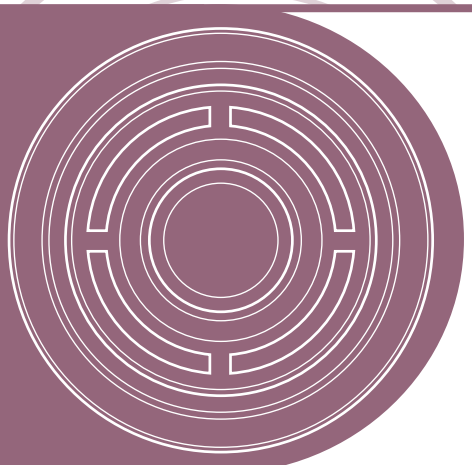
Training is vital for officers to effectively investigate cyber crime, to provide advice about preventative measures and to support the needs of victims. Training for the PSNI officers had been provided at various levels, including new staff joining the Service, however Inspectors identified gaps, and the current provision should be assessed against a comprehensive analysis of need.

It was evident during this inspection that a limited understanding of the threat from cyber crime was widespread. The PSNI was fully involved in the national initiatives operating here; it was a key player in the local groups involving academia and the business community, and police had established excellent links with stakeholders across Northern Ireland. There were extensive resources provided on the PSNI website and active media promotion and advice about cyber crime and internet security. Despite all of this, cyber crime was the cause of considerable concern amongst the public, and Inspectors identified the need for a more strategic approach to increase awareness and education about cyber crime and internet security amongst the business and wider community in Northern Ireland.

Strategic recommendation

1 The PSNI should undertake a comprehensive strategic analysis of cyber crime as it affects Northern Ireland. This should include the issues identified in this report about under-reporting and recording of the cyber crime types. It should also consider the potential future demand on police, together with the investigative implications for policing developing areas, for example, crypto currencies, 'cloud' use and the dark net. This analysis should be prioritised and completed within six months of the publication of this report (paragraph 3.15).

A further six operational recommendations are contained within the report.



Inspection Report

1 Introduction

Introduction

1.1 Cyber crime is a relatively recent phenomenon and its prevalence has increased exponentially in recent years at the same time as rates for the traditional crime types have fallen. There are reports of cyber crime in the media on an almost daily basis, and it is now a firmly established threat to businesses and individuals. Cyber crime is not an emerging threat; it is the reality of crime now, and police forces need to adapt quickly to meet the threat.[1]

1.2 Cyber crime is high reward and relatively low risk,[2] it is anonymous and borderless. What is illegal offline is illegal online and the assessment of the PSNI is that more crime is committed online than offline.[3] Cyber crimes can be perpetrated on a scale that is of a different magnitude from traditional crime types, and while some cyber-dependant crime requires IT expertise, cyber-enabled crime can be perpetrated on a massive scale by an individual using relatively unsophisticated IT equipment (see Case Study 1).

1.3 Many victims are broadly unaware of the digital threat, of the prevalence of such crimes and the specific offences which have been committed. This uncertainty means that in many instances victims are not able to take steps to prevent the crime or its repetition.[4] Whilst cyber awareness is improving in the UK, there remains a general lack of understanding of cyber crime.[5] The nature of cyber crime, and its affects on individuals and businesses, means that it is significantly under-reported to police.

1.4 Cyber criminals can differ from criminals in the more traditional fields in that their motivation may not always be for financial gain, some are motivated by the technical challenge of 'hacking', others may have a grievance against a company or employer.

1.5 A recent Her Majesty's Inspectorate of Constabulary (HMIC) report emphasised the very real impact that cyber crime had on victims and this is referred to in more detail in Chapter 2.

---

1 State of Policing. The Annual Assessment of Policing in England and Wales 2013/2014. Her Majesty's Chief Inspector of Constabulary. 27 November 2014. http://www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/state-of-policing-13-14.pdf

2 Cyber Resilience: How to Protect Small Firms in the Digital Economy. Federation of Small Businesses. June 2016. http://www.fsb.org.uk/docs/default-source/fsb-org-uk/fsb-cyber-resilience-report-2016.pdf?sfvrsn=0

3 Northern Ireland Assembly. Committee for Justice. Official report (Hansard). Business Crime: Stakeholder Event. 14 May 2015.

4 Real lives, real crimes. A study of digital crime and policing. Her Majesty's Inspector of Constabulary. July 2015. https://www.justiceinspectorates.gov.uk/hmic/our-work/digital-crime-and-policing/real-lives-real-crimes-a-study-of-digital-crime-and-policing/

5 NCA Strategic Cyber Industry Group. Cyber Crime Assessment 2016. Need for a stronger law enforcement and business partnership to fight cyber crime. 7 July 2016. http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file

Definition of Cyber Crime

1.6 Cyber crime is an over-arching term to describe two distinct, but closely related criminal activities: cyber-dependent and cyber-enabled crime. It is also referred to in some quarters as digital crime or e-crime. In this report the use of the term 'cyber crime' refers to both types of crimes unless otherwise indicated. Appendix I provides an indication of the scope of activities and offences that can be classed under the umbrella term 'cyber crime'.

- **Cyber-dependent crime** – where a criminal act can only be committed through the use of computers, computer networks or other Information Communication Technology (ICT) devices. In these cases the devices are both the tool for committing the crime and the target of the crime, e.g. harvesting of online bank account details using malware,[6] the spread of viruses and other malicious software, hacking, and distributed denial of service (DDoS) attacks, i.e. the flooding of internet servers to take down network infrastructure or websites. Cyber-dependent crimes are primarily acts directed against computers or network resources, although there may be secondary outcomes from the attacks, such as fraud.

- **Cyber-enabled crime** – involves traditional crimes that are increased in their scale or reach by the use of computers, computer networks or other ICT. Unlike cyber-dependent crimes, they can still be committed without the use of ICT. These include:

  - Fraud (including mass-marketing frauds, 'phishing' emails and other scams; online banking and e-commerce frauds);
  - Theft (including the theft of personal information and identification-related data);
  - Sexual offending against children (including grooming, and the possession, creation and/or distribution of sexual imagery), prostitution and human trafficking;
  - Criminal commodity supply including firearms and drugs; and
  - Internet-facilitated crime – is a subset of cyber-enabled crime and for example, includes widespread use of communications and social media platforms to harass, stalk, groom, incite hatred and threaten using social media or other cyber platforms. It can also involve the disposal of stolen property or counterfeit goods on auction sites.[7]

Inspection Scope

1.7 This is an inspection of how the Northern Ireland criminal justice system deals with cyber crime. The PSNI had the primary responsibility for recording and investigating cyber crime in Northern Ireland, as well as a significant role to play in crime prevention, education and awareness-raising amongst members of the public and business community, and so this was the primary focus of this inspection. It is not however an inspection of the quality of police crime investigations, as this was addressed by other recent CJI inspection work.[8]

6 Annual report and threat assessment 2015. Organised Crime Task Force. www.octf.gov.uk
7 PSNI Corporate Control Strategy. PSNI internal document.
8 For a more detailed inspection of this aspect see CJI Report: An Inspection of the Quality and Timeliness of Police Files (Incorporating Disclosure) Submitted to the Public Prosecution Service for Northern Ireland. CJI. November 2015. http://www.cjini.org/CJNI/files/9f/9faaa7ad-b1a9-4d66-bd35-79ff20848c7c.pdf

1.8 The UK Cyber Security Strategy identified cyber threats as emanating from criminals, foreign intelligence services, terrorists and politically motivated groups and individuals or 'hactivists'.[9] Cyber crime also incorporates on-line child sexual exploitation, indecent images of children and elements of serious and organised crime, and the inspection does not seek to repeat issues which were examined in separate inspection work, for example in Serious and Organised Crime,[10] or in the Independent Inquiry into Child Sexual Exploitation in Northern Ireland.[11] Likewise cyber terrorism, the threats from other States and political activists were outside the scope of this inspection.

1.9 There had been much media attention about the prevalence of cyber-bullying in Northern Ireland, and whilst this was a significant issue, cyber-bullying was not classed as a crime *per se;*[12] it was a cyber-enabled offence, and was not examined as a separate issue in this inspection.

1.10 Businesses, as well as individual members of the public were victims of cyber crime and this report should be read in conjunction with the forthcoming CJI report on Business Crime as the two areas are closely connected.

Use of Technology

1.11 Computer and internet use is now a fundamental and indispensable component of businesses and the everyday lives of individuals. The increasing capacity and functionality of devices has happened at the same time as their relative cost has plummeted. Use has increased dramatically with:

- the internet was accessed every day, or almost every day, by 82% of adults (41.8 million) in Great Britain (GB) in 2015, compared to 35% (16.2 million) in 2006;
- 70% of people accessed the internet using a mobile device;
- 77% of adults bought goods or services online; and
- 89% of households in GB had internet access.[13]

1.12 We are critically dependent on the internet, yet it is inherently insecure.[14] As computer use has grown, so have the opportunities for technology to be exploited by criminals. Cyber crime is now an unfortunate reality and criminal groups and individuals have been quick to diversify. Organised crime groups were availing of new technology to assist in their criminality.

9 UK Cyber security strategy. Cabinet Office. November 2011. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

10 Serious and Organised Crime: an Inspection on how the Criminal Justice System deals with Serious and Organised Crime in Northern Ireland. November 2014. CJINI. http://www.cjini.org/CJNI/files/4e/4e668867-6095-4687-9bf5-61fb05973478.pdf

11 Child Sexual Exploitation in Northern Ireland. A Report of the Independent Inquiry. 19 November 2014. http://www.cjini.org/CJNI/files/f0/f094f421-6ae0-4ebd-9cd7-aec04a2cbafa.pdf. Also see Online and on the Edge: Real Risks in a Virtual World. An Inspection into how Forces deal with the Online Sexual Exploitation of Children. Her Majesty's Inspectorate of Constabulary. July 2015.

12 Unless it incorporates other elements, e.g. sexting which can be a criminal offence. Cyber crime: a review of the evidence. Research Report 75. Summary of key findings and implications. Home Office. October 2013

13 Internet Access – Households and individuals 2016. Statistical Bulletin. Office for National Statistics. 4 August 2016.

14 National Cyber Security Strategy 2016-2012. HM Government. 2 November 2016. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/564268/national_cyber_security_strategy.pdf

Key areas included the use of encrypted communications, the dark net, privacy-based browsers, and virtual currencies.[15]

1.13 The inter-networking of physical devices (the so-called 'internet of things') is another developing area with potential implications for perpetrating crime and creating victims.

1.14 The National Crime Agency (NCA) assessed the accelerating pace of technology and criminal cyber capability development as outpacing the UK's collective responses to cyber crime. This 'cyber arms race' was likely to be an enduring challenge and an effective response required collaborative action from government, law enforcement, industry regulators and critically, business leaders.[16]

Cost of Cyber Crime

1.15 A 2016 Global Economic Crime Survey found the incidence of cyber crime was increasing. It reported that:

- over a quarter of respondents had been affected by cyber crime, with another 18% not knowing if they had been affected. The insidious nature of the threat was such that of the 56% who said they were not victims, many are likely to have been compromised without knowing it;
- reputational damage was considered to be the most damaging impact of a cyber breach; and
- cyber crime is a powerful countervailing force limiting potential[17] and a threat to growth.[18]

1.16 Anti-virus providers conclude that security attacks globally were in the billions and levels were increasing.[19]

1.17 The NCA estimated the cost of cyber crime to the UK economy was billions of pounds per year and growing, with potentially millions of individual victims and many thousands of corporate victims.[20] Get Safe Online and the National Fraud Intelligence Bureau assessed the cost of fraud and cyber crime to the UK in the 12 months to October 2016 as £10.9 billion.[21]

15 Annual report and threat assessment 2015. Organised Crime Task Force. www.octf.gov.uk
16 NCA Strategic Cyber Industry Group. Cyber Crime Assessment 2016. Need for a stronger law enforcement and business partnership to fight cyber crime. 7 July 2016. http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file
17 See also Cyber security and fraud: The impact on small businesses. Federation of Small Business. http://www.fsb.org.uk/LegacySitePath/frontpage/assets/fsb_cyber_security_and%20_fraud_paper_2013.pdf
18 Adjusting the Lens on Economic Crime. Preparation brings opportunity back into focus. PWC Global Economic Crime Survey 2016. www.pwc.com/crimesurvey.
19 Cyber crime: a review of the evidence. Research Report 75. Summary of key findings and implications. Home Office. October 2013
20 NCA Strategic Cyber Industry Group. Cyber Crime Assessment 2016. Need for a stronger law enforcement and business partnership to fight cyber crime. 7 July 2016. http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file and http://www.nationalcrimeagency.gov.uk/publications/207-nca-strategic-assessment-of-serious-and-organised-crime/file
21 https://www.getsafeonline.org/news/fraud-cybercrime-cost-uk-nearly-11bn-in-past-year/

1.18 Other estimates put the cost to UK businesses in the region of £34 billion per year: £18 billion in lost revenue and £16 billion on increased IT spending as a result of breaches.[22] Losses to the banking sector alone in 2013-14 peaked at £60.4 million.[23]

1.19 Almost one third of Federation of Small Business members were a victim of online crime in 2012,[24] this increased significantly to 66% in 2014-15. On average small business were a victim on four occasions, with a total loss to UK small businesses in the region of £5.2 billion.[25] Fraud and online crime costs the average small business £4,000 per annum. [26]

1.20 The Office for National Statistics (ONS) estimated that adults experienced around 5.8 million fraud and computer misuse incidents in 2015-16, and of the frauds, just over half (51%) were cyber-related.[27]

1.21 In Northern Ireland estimates put the costs of cyber crime to the economy in the region of £100 million per annum.[28]

1.22 A recent PSNI press release to launch ScamwiseNI estimated that 17% of people across Northern Ireland had been the victims of scams in the last three years which equated to 314,840 people.[29] However it is extremely difficult to quantify the scale of loss to individual members of the public.

Under-reporting of Cyber Crime

1.23 Under-reporting of both cyber-dependent and cyber-enabled crime[30] was widespread amongst the general public and businesses. It obscured the full impact of cyber crime in the UK;[31] a HMIC report assessed the scale of under-reporting as considerable.[32]

22 Centre for Economics and Business Research. http://www.cebr.com/reports/60-of-british-ctos-say-uk-government-is-performing-poorly-in-protecting-firms-from-cyberattacks/
23 The Implications of Economic Cybercrime for Policing. Research Report. City of London Corporation and City of London Police. October 2015.
24 Cyber Security and Fraud: The Impact on Small Businesses. Federation of Small Businesses. http://www.fsb.org.uk/LegacySitePath/frontpage/assets/fsb_cyber_security_and%20_fraud_paper_2013.pdf
25 Cyber Resilience: How to Protect Small Firms in the Digital Economy. Federation of Small Businesses. June 2016. http://www.fsb.org.uk/docs/default-source/fsb-org-uk/fsb-cyber-resilience-report-2016.pdf?sfvrsn=0
26 Cyber security and fraud: The impact on small businesses. Federation of Small Business. http://www.fsb.org.uk/LegacySitePath/frontpage/assets/fsb_cyber_security_and%20_fraud_paper_2013.pdf
27 Office for National Statistics. Statistical Bulletin. Crime in England and Wales: year ending March 2016. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmar2016.
28 Northern Ireland Assembly Official Report (Hansard). Monday 7 December 2015. Volume 110, Number 2.
29 https://www.psni.police.uk/news/Latest-News/101116-scamwiseni-initiative-launched/
30 See also Organised Crime Task Force. Annual Report and Threat Assessment 2015. www.octf.gov.uk
31 NCA Strategic Cyber Industry Group. Cyber Crime Assessment 2016. Need for a stronger law enforcement and business partnership to fight cyber crime. 7 July 2016. http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file
32 State of Policing. The Annual Assessment of Policing in England and Wales 2013/2014. Her Majesty's Chief Inspector of Constabulary. 27 November 2014. http://www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/state-of-policing-13-14.pdf

1.24 Some estimates suggested that as few as 1% of adult internet users who experienced hacking or unauthorised access, reported it to the police.[33] More recent data showed that 39% of people who said they had been the victim of an online crime had not reported the incident.[34]

1.25 The ONS estimated that there were 2.46 million cyber incidents and 2.11million victims in the UK in 2015, but only 16,349 cyber-dependent and 700,000 cyber-enabled incidents reported to Action Fraud in the same period.[35] This was less than 30%. This data excluded a significant volume of card and bank account fraud, as data was not collected on some types of plastic card fraud including 'remote purchase frauds', frauds from lost or stolen cards or ATM fraud.[36] The National Cyber Security Centre (NCSC) reported that banks were under-reporting cyber incidents.[37]

1.26 Explanations for the level of under-reporting included the potential effectiveness of security filters, and that many people deleted phishing e-mails as a nuisance rather than as an attempt to victimise.[38] Many cyber frauds relied on the users' ignorance, naïveté or willingness to accept offers that were 'too good to be true', and the reluctance by individuals to report these types of crimes could be for a variety of reasons, including embarrassment.

1.27 The PSNI recognised that the vast majority of cyber crime was not reported and that there was a need for an accurate picture of the scale and nature of cyber crime to enable a more effective response.[39]

1.28 The Federation of Small Business' research into business crime generally, which included cyber crime, found that 24% of small businesses did not report any crime against their businesses or staff; 33% reported only the most serious of crimes; and only around 20% reported all the crimes their businesses or employees experienced. Reasons for this reluctance to report crime included: a feeling that reporting crime would not achieve anything (46%); a perception that police would not be able to find or prosecute the perpetrator (38%); reporting a crime would be too time consuming (26%); and a negative experience of previously reporting a crime to police (21%).[40]

1.29 Other research found that businesses reported just two per cent of online crimes and concerns about commercial damage[41] and reputational damage contributed to the under-reporting.[42] Other factors in corporate under-reporting included:

33 Cyber crime: a review of the evidence. Research Report 75. Summary of key findings and implications. Home Office. October 2013
34 https://www.getsafeonline.org/news/fraud-cybercrime-cost-uk-nearly-11bn-in-past-year/
35 NCA Strategic Cyber Industry Group. Cyber Crime Assessment 2016. Need for a stronger law enforcement and business partnership to fight cyber crime. 7 July 2016. http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file
36 Office for National Statistics. Statistical Bulletin. Crime in England and Wales: year ending March 2016. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmar2016.
37 https://www.ncsc.gov.uk/report/weekly-threat-report-24-october-2016.
38 Office for National Statistics. Discussion Paper on the coverage of Crime Statistics. ONS. 23 January 2014.
39 Northern Ireland Assembly. Committee for Justice. Official Report Hansard Business Crime Stakeholder Event. 14 May 2015.
40 Tackling Business Crime: FSB Manifesto. Federation of Small Businesses 2016. http://www.fsb.org.uk/docs/default-source/fsb-org-uk/fsb-tackling-business-crime-manifesto-v01.pdf?sfvrsn=0.
41 Office for National Statistics. Discussion Paper on the coverage of Crime Statistics. ONS. 23 January 2014.
42 See also Northern Ireland Assembly Official Report (Hansard). Monday 7 December 2015 Volume 110, No 2 which made reference to a Justice Committee stakeholder event which found that some of the larger companies were fearful of reporting cyber crime in case consumers would lose confidence in their ability to keep information safe and operate in the online world.

- many businesses were unaware of breaches;
- IT teams were reluctant to inform senior management for fear of criticism;
- senior management believed it was better to settle customer losses and fix problems quietly; and
- some lawyers advised companies it was not in their legal interests to report.[43]

1.30 The reluctance to report and concern about reputational damage to businesses were likely to be even more acute when the crimes were as a result of an 'insider threat'.[44]

Recording of Cyber Crime

1.31 Traditional police crime recording and Crime Survey estimates were victim-focussed with the underlying principle of counting crime on the basis of one crime record for each victim.[45]

1.32 The recording of cyber crime presented additional challenges in terms of identifying, locating and counting victims, for example, for cyber-enabled credit card fraud the bank may suffer the direct financial loss but the card-holder suffered the inconvenience of dealing with the aftermath.[46]

1.33 The scale of cyber crime also presented a problem for victim-focussed recording, and a single act of uploading a virus or malicious e-mail could impact on tens of thousands of people. There was a question of the appropriateness of comparing these directly, even if it were possible to accurately count the number of direct and indirect victims, with the more traditional acquisitive crimes such as burglary or car theft. Cyber crime recording was also more complex than traditional crime in terms of jurisdiction.

1.34 Information on conviction rates was not readily available and the Minister of Justice advised the Northern Ireland Assembly that it was not possible to detail the number of convictions for cyber crime without manually trawling court records, as the offences were usually prosecuted under a more generic offence such as theft or fraud.[47]

1.35 It was however, in the public interest that the true magnitude and extent of cyber crime was established. An accurate picture of the scale of cyber crime was also required to enable effective police response and for informed decisions to be made about police resource allocation.[48]

43 NCA Strategic Cyber Industry Group. Cyber Crime Assessment 2016. Need for a stronger law enforcement and business partnership to fight cyber crime. 7 July 2016. http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file

44 Where a member of staff has joined a company for the express purpose of stealing data or disrupting systems, or where an employee has been approached or threatened by criminals due to his/her position within the company.

45 In the case of the Crime Survey for England and Wales victims are households or members thereof.

46 Office for National Statistics. Discussion Paper on the coverage of Crime Statistics. ONS. 23 January 2014.

47 Northern Ireland Assembly. Written Answer. AQW 3304/16-21. Answered 3 October 2016.

48 See also Northern Ireland Assembly. Committee for Justice. Official Report Hansard Business Crime Stakeholder Event. 14 May 2015, and Real lives, real crimes. A study of digital crime and policing. Her Majesty's Inspector of Constabulary. July 2015. https://www.justiceinspectorates.gov.uk/hmic/our-work/digital-crime-and-policing/real-lives-real-crimes-a-study-of-digital-crime-and-policing/

2 Strategy and governance

The National Strategy

2.1 The potential impact of cyber crime and the need for improved cyber security were recognised by Government. From 2011 to 2016 the UK Government funded the first National Cyber Security Programme (NCSP) with £860 million to deliver the strategic objectives[49] with work programmes, *inter alia*,

- to ensure law enforcement had the skills and capabilities needed to tackle cyber crime and maintain the confidence needed to do business on the Internet;
- improve cyber awareness and risk management amongst UK business; and
- ensure members of the public knew what they could do to protect themselves, and were demanding good cyber security in the products and services they consumed.[50]

2.2 In these latter areas measures to help businesses and individuals included:

CERT-UK: the UK National Computer Emergency Response Team, formed in March 2014. It had four main responsibilities which were:

- national cyber-security incident management;
- support to critical national infrastructure companies to handle cyber security incidents;
- promotion of cyber-security situational awareness across industry, academia, and the public sector; and
- the single international point of contact for co-ordination and collaboration between national CERTs.[51]

49 Those objectives are:
- to make the UK one of the most secure places in the world to do business in cyberspace;
- to make the UK more resilient to cyber attack and better able to protect our interests in cyberspace;
- to help shape an open, vibrant and stable cyberspace that supports open societies;
- to build the UK's cyber security knowledge, skills and capability.

50 The UK Cyber Security Strategy. Report on Progress and Forward Plans. December 2014.https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf

51 https://www.cert.gov.uk/what-we-do/

- ***CiSP***: the Cyber-security Information Sharing Partnership was a joint industry-Government initiative to share cyber threat and vulnerability information, and to increase overall awareness of the cyber threat and reduce the impact on UK business. It allowed members from across sectors and organisations to securely exchange cyber threat information in real time. Members received network monitoring reports from CERT-UK covering any malicious activity detected on their networks.[52]

Get Safe Online: a public/private sector partnership supported by Government and leading organisations in banking, retail, and internet security. The website provided practical advice on protection for computers and mobile devices, businesses, identity theft, viruses and other problems encountered online.[53]

Cyber Streetwise: a cross-Government campaign delivered in partnership with the private and voluntary sectors, aimed at improving the online safety behaviour and confidence of consumers and small businesses.[54]

Cyber Essentials: developed in consultation with industry. It provided businesses with clarity on good basic cyber security practice, by focusing on basic cyber hygiene to better protect companies from the most common cyber threats. It was for organisations of all sizes, and in all sectors and had been mandatory for central government IT contracts advertised after October 2014.[55]

2.3 The 2011-16 Strategy was superseded in November 2016 by the launch of the National Cyber Security Strategy 2016-21 to address the growing number of cyber attacks which were increasingly more frequent, sophisticated and damaging when they succeeded.

2.4 This was accompanied by a five-year investment of £1.9 billion to transform the UK's cyber security. The strategy committed the UK Government in partnership with the devolved administrations in Northern Ireland, Wales and Scotland, to work with the private and public sectors to ensure that individuals, businesses and organisations stayed safe on the internet.[56] At the time of writing Inspectors had not been made aware of the detail of how this would be implemented in Northern Ireland. However, cyber security was not solely a justice issue; it required action across the Northern Ireland Executive Departments.

52 https://www.cert.gov.uk/cisp/
53 https://www.getsafeonline.org/about-us/
54 https://www.cyberstreetwise.com/
55 https://www.cyberstreetwise.com/cyberessentials/
56 National Cyber Security Strategy 2016-2012. HM Government. 2 November 2016. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/564268/national_cyber_security_strategy.pdf

2.5 As part of the National Cyber Security Strategy, in October 2016 the NCSC became operational as the UK authority on cyber security,[57] and brought together a number of organisations[58] to simplify the UK cyber security landscape.[59] At the time of writing, the NCSC had just been launched and as a new organisation with a national co-ordinating role, its interrelationship with UK policing would be a process which developed over time.

2.6 In Scotland the 2014 Programme for Government signalled the intention to produce a strategy for building Scotland's cyber resilience which built on the UK Strategy. Recognising that cyber resilience was a shared responsibility the Strategy included a wide representation of public sector partners (including education, health, enterprise, policing and local authorities), business and industry representative bodies, private sector organisations and the third sector.[60]

The National Crime Agency (NCA)

2.7 The cyber crime aspects of serious and organised crime and the threat of a national cyber crime incident were identified in the Strategic Policing Requirement (SPR)[61] as Tier One risks. Whilst the SPR applies to England and Wales, many of the national risks affected the wider UK, and there was collaborative working and the provision of mutual aid between the NCA and UK police forces, which included the PSNI.

2.8 In the UK the NCA led in the investigation of serious and organised crime. The NCA became operational in the UK in October 2013 and had been operational in Northern Ireland since May 2015. Its role extended to cyber crime insofar as it related to serious and organised crime, and incorporated the National Cyber Crime Unit (NCCU) which led operations on serious cyber crime whether they originated in the UK or internationally, and which worked closely with the Regional Organised Crime Units (ROCUs) in England and Wales and with the PSNI.

57 The NCSC is part of the National Cyber Security Strategy and will focus on:
- Understanding the cyber security environment, sharing knowledge and using that expertise to identify and address systematic vulnerabilities;
- Reducing risks to the UK by working with public and private sector organisations to improve their cyber security;
- Responding to cyber security incidents to reduce the harm they cause to the UK; and
- Growing the UK national cyber security capability, and provide leadership on critical national cyber security issues. https://www.ncsc.gov.uk/news/national-cyber-security-centre-becomes-operational.

58 These include the Communications-Electronics Security Group (CESG), the information Security arm of GCHQ; the Centre for the Protection of National Infrastructure (CPNI); CERT-UK; CiSP and the Centre for Cyber Assessment.

59 https://www.ncsc.gov.uk/news/national-cyber-security-centre-becomes-operational.

60 Safe, Secure and Prosperous: A Cyber Resilience Strategy for Scotland 2015. www.gov.scot/cyberresilience.

61 The SPR is issued in accordance with the Home Secretary's statutory duty to set out national threats and the appropriate national policing capabilities required to counter those threats.

Policing

2.9 All other aspects of cyber crime were dealt with by local police forces. Whilst cyber crime was increasing, limited data was available on the police resources required to respond, although it was recognised that there were potential resourcing implications as cyber crimes were generally more complex to investigate.[62]

2.10 HMIC's '*Digital Crime and Policing*' report examined the strategic approach taken by police forces to address cyber crime. It emphasised that those who committed digital crime created victims who demanded and deserved the support and help of police as much as any other victim of crime: digital crime was not a lesser crime type, it was as pernicious and disruptive as any other and merited an equal response.

2.11 The report stressed that it was no longer appropriate for the police service to consider the investigation of digital crime to be the preserve of those with specialist knowledge, and the public had a right to demand swift action and good quality advice from every officer with whom they come into contact – from the first point of contact to the experienced detective. The report concluded that police work needed to:

- show that the police service took digital crime and its impact seriously;
- better tailor support and advice to victims of digital crime;
- increase awareness of how to investigate digital crime and the evidence required to support such an investigation; and
- keep the victims of digital crime better informed of progress in the investigation.[63]

2.12 There was also an identified need for the police service at strategic level to establish the scale and impact of cyber crime and how to respond to it.

2.13 HMIC also stressed the need for forces to have the capacity to examine digital devices in the most appropriate, effective and speedy manner and to provide sufficient local capability to deal effectively with cyber crime.[64]

2.14 The HMIC report concluded that there were times when police needed to make a major leap forward in capability to keep pace with the crime threat, and this was particularly true of cyber crime, where the gap between the threat and police capability was widening.[65]

62 College of Policing analysis: Estimating the demand on police services. College of Policing 2015.
63 Real lives, real crimes. A study of digital crime and policing. Her Majesty's Inspector of Constabulary. July 2015. https://www.justiceinspectorates.gov.uk/hmic/our-work/digital-crime-and-policing/real-lives-real-crimes-a-study-of-digital-crime-and-policing/
64 Ibid.
65 State of Policing. The Annual Assessment of Policing in England and Wales 2013/2014. Her Majesty's Chief Inspector of Constabulary. 27 November 2014. http://www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/state-of-policing-13-14.pdf

2.15 One initiative to increase capability was a recruitment initiative for volunteer 'Cyber Specials' across English and Welsh police forces to harness expertise from the private sector to increase further police capacity to investigate cyber crime.[66]

2.16 The way cyber crime was recorded by police had not helped forces understand the growing nature and full extent of the volume of cyber crimes committed. A Freedom of Information request to police forces revealed that of the 25 forces which received the requests, around 50% could not supply accurate figures of cyber crime without a manual analysis of their recording systems.[67] Since April 2015 the Home Office had sought to rectify this problem by requiring police forces to 'flag' cyber crimes.

2.17 The National Cyber Security Strategy also raised the need for improved measurement of outcomes and referred to the effective use of metrics as essential to delivery of the Strategy and to identify the resourcing requirements.[68]

Fraud

2.18 Fraud, including digital fraud was one of the principal offences which did not respect police or international boundaries; as a result the National Fraud Reporting Centre was set up in 2006 to provide a co-ordinated and nationally consistent response.[69]

2.19 In 2009 it was renamed Action Fraud, and was the UK's national reporting centre where members of the public reported fraud if they had been scammed, defrauded or been the victim of cyber crime. Action Fraud was run by the City of London Police[70] and the National Fraud Intelligence Bureau (NFIB) and provided a central point of contact for information about fraud and financially motivated internet crime.

2.20 The NFIB used reports of fraud and cyber crime to identify serial offenders, organised crime gangs and emerging crime types, and obtained data through:

- reports from individuals and small businesses made to Action Fraud;
- fraud data from industry and the public sector which included banking, insurance, telecommunications and government departments; and
- a variety of intelligence sources including, national and international police crime/ intelligence systems.

66 Specials to be in place by March 2018. The UK Cyber Security Strategy 2011-2016. Annual report. April 2016. Cabinet Office. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf

67 Partners against crime. How can industry help the police to fight cyber crime? Tech UK. October 2015. http://www.techuk.org/insights/reports/item/6102-techuk-calls-on-police-and-industry-to-work-together-to-tackle-cyber-crime

68 National Cyber Security Strategy 2016-2012. HM Government. 2 November 2016. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/564268/national_cyber_security_strategy.pdf

69 Real lives, real crimes. A study of digital crime and policing. Her Majesty's Inspector of Constabulary. July 2015. https://www.justiceinspectorates.gov.uk/hmic/our-work/digital-crime-and-policing/real-lives-real-crimes-a-study-of-digital-crime-and-policing/

70 The City of London Police is the national police lead for economic crime

2.21 The NFIB also sought to disrupt the fraud enablers that were causing harm by working with service providers to close down IT services abused by fraudsters.

2.22 Outputs from the NFIB included:

- individual crime packages, following the reporting of crime from members of the public/ businesses, reviewed and disseminated to local police forces for investigation;
- victim profiles with details of victim and crime types provided to police forces; and
- fraud alerts disseminated to law enforcement agencies, industry partners and members of the public to highlight emerging trends.[71]

2.23 Action Fraud was not responsible for the investigation of fraud offences: this remained the responsibility of the local police force. In cases where solvability factors were indentified, and if there was a realistic prospect of identifying the offender, the case was passed to the relevant police service to pursue. Otherwise cases remained on the Action Fraud database for further analysis.[72]

2.24 HMIC identified a lack of knowledge amongst police officers at all ranks of the functions of Action Fraud, consequently advice and support to victims of such crime was poor.[73]

Northern Ireland

2.25 The draft Programme for Government 2016-21 had an outcome of having 'a safe community where we respect the law, and each other' with indicators to reduce crime; reduce offending and increase the effectiveness of the justice system.[74]

2.26 The Northern Ireland Executive recognised the concerns around the safety of children and young people online and funded the Safeguarding Board for Northern Ireland (SBNI) to develop an E-Safety Strategy for Northern Ireland. The work was being overseen by the Department of Health with the Department of Justice (DOJ) and PSNI was represented on the Project Board. The draft strategy was to be disseminated for public consultation in late 2016.[75] It would be the view of CJI that the E-Safety Strategy should be an integral element of a wider Cyber Strategy for Northern Ireland (see Chapter 4).

71 Action Fraud. http://www.actionfraud.police.uk
72 Real lives, real crimes. A study of digital crime and policing. Her Majesty's Inspector of Constabulary. July 2015. https://www.justiceinspectorates.gov.uk/hmic/our-work/digital-crime-and-policing/real-lives-real-crimes-a-study-of-digital-crime-and-policing/
73 Ibid.
74 Draft Programme for Government Framework 2016-21. Northern Ireland Executive. 27 May 2016. https://www.northernireland.gov.uk/sites/default/files/consultations/newnigov/draft-pfg-framework-2016-21.pdf
75 Northern Ireland Assembly. Written Answer. AQW 143/16-21. Answered 26 May 2016

Organised Crime Task Force (OCTF)

2.27 The OCTF was established in 2000 to confront organised crime through multi-agency partnership involving Government Departments, the criminal justice agencies, the Northern Ireland Policing Board (NIPB), the business community and the community at large.[76] The OCTF had no role in operational law enforcement delivery: it performed a purely coordinating role for joint working, operations and information-sharing. It operated as a three-tiered structure with Stakeholder and Strategy Groups and underpinning sub-groups. There was a Cyber Sub-Group and a Cyber Crime Industry Group to engage and share intelligence with business and academia.[77]

2.28 The Northern Ireland Organised Crime Strategy was first published in 2010 and highlighted an increasing profile for cyber crime. In June 2014 it assessed organised crime groups as increasingly using advances in technology and communications to commit crime:[78] the 2016 assessment described cyber crime as a key growth area in all sectors in Northern Ireland.[79]

2.29 The OCTF Control Strategy had various objectives for Prevention, Protection and Enforcement aspects, which included outcomes to:

- raise the external understanding of the threat posed by cyber crime to industry, the public sector and individuals; and
- develop a Cyber Strategy for Northern Ireland.[80]

2.30 The OCTF Control Strategy for Cyber Crime contained a number of activities to progress the strategic objectives. It would be CJI's view that the Control Strategy contained a comprehensive set of objectives to address the wider aspects of cyber crime, however it was primarily process-driven. For effective governance and performance improvement the measures needed to be outcome, and not activity-based, with actions allocated to individuals/organisations, and time-bound measures to allow assessment of performance over time.[81]

76 Organised Crime Task Force Annual Report and Threat Assessment 2015. www.octf.gov.uk

77 Other sub-groups include: Armed Robbery, Criminal Finance, Cross-Border Fuel Fraud, Drugs, Immigration and Human Trafficking; Intellectual Property Crime, Legal and Publicity.

78 Organised Crime Task Force. The Northern Ireland Organised Crime Strategy. June 2014. www. octf.gov.uk

79 Organised Crime Task Force. Annual Report and Threat Assessment 2016. https://www.justice-ni.gov.uk/sites/default/files/publications/justice/doj-octf-report-june-2016.pdf

80 Organised Crime Task Force. The Northern Ireland Organised Crime Strategy. April 2016. http://www.octf.gov.uk/OCTF/media/OCTF/documents/publications/N.I.%20Organised%20Crime%20Strategy/The-NI-Organised-Crime-Strategy-April-2016.pdf?ext=.pdf

81 See also the Draft Programme for Government Framework 2016-2021 which advocates a different approach for Government departments to focus on outcomes with indicators to show change and measures to assess success. https://www.northernireland.gov.uk/sites/default/files/consultations/newnigov/draft-pfg-framework-2016-21.pdf

Business Crime Action Plan 2016-17

2.31 The DOJ, the PSNI and the NIPB's jointly released Business Crime Action Plan[82] also recognised the threat from cyber crime. In the Prevention and Protection strands the strategic aim was to improve the uptake of protective security and prevention advice with a specific area to promote the awareness of cyber crime and cyber threat to individuals and business. Actions/ targets to achieve this included:

- to scope the need for a Northern Ireland-wide cyber strategy; and
- to encourage cyber resilience in businesses, through the promotion of the Cyber Essentials Scheme.

2.32 Inspectors would comment that, like the OCTF Control Strategy, the Business Crime Action Plan should be more outcome-based with a strengthened governance mechanism and clear lines of responsibility to allocated individuals, with timelines for achievement and milestones to measure progress.[83]

PSNI

2.33 The Northern Ireland Policing Plan had a strategic outcome for the PSNI to work in partnership to address serious and organised crime. This recognised that criminal methodology had changed with crimes increasingly facilitated and enabled by technology. To achieve this the PSNI must demonstrate to the NIPB how it identified the risk and threat from serious and organised crime and cyber-related crime and thereafter how it dealt with these issues,[84] and the Annual Policing Plan for Northern Ireland contained a requirement for the PSNI to report to the NIPB on the initiatives, interventions and outcomes in relation to cyber-dependent, enabled and facilitated crime.[85] It would be the view of CJI that this requirement should be reviewed for future Policing Plans to be more specifically related to the scale and impact of cyber crime in Northern Ireland, and which provided the NIPB with a mechanism to hold the PSNI to account for performance in this area.

2.34 The police response to cyber crime was driven by the OCTF Strategy, the PSNI assessment of the threat (problem profile),[86] and the PSNI Control Strategy developed under the National Intelligence Model. Cyber crime had been identified as a service strategic priority and the Control Strategy provided the direction across the PSNI to tackle cyber crime. It took account

82 Business Crime Action Plan 2016-2017. DOJ, PSNI, NIPB. https://www.justice-ni.gov.uk/sites/default/files/publications/justice/business-crime-action-plan-10-may.pdf

83 See also the Draft Programme for Government Framework 2016-2021 which advocates a different approach for Government departments to focus on outcomes with indicators to show change and measures to assess success.

84 Northern Ireland Policing Board Strategic Outcomes for Policing in Northern Ireland 2016-2020. https://www.nipolicingboard.org.uk/sites/nipb/files/media-files/Strategic-outcomes-for-policing-2016-2020.pdf

85 Annual Policing Plan for Northern Ireland 2016-2017.March 2016. http://www.nipolicingboard.org.uk/final_pdf_-_policing_plan_2016-17.pdf

86 A problem profile is intended to provide the force greater understanding of established and emerging crime or incident series, priority locations or other identified high risk issues. It should be based on the research and analysis of a wide range of information sources, including information from partner organisations. It should contain recommendations for making decisions and options for action. HMIC definition.

of the national and Northern Ireland-wide strategy and governance issues referred to in this report and provided a forward plan in the areas of Prevention, Reassurance, and Enforcement, together with outcomes and activity measures. The Control Strategy was subject to monthly review through the Service Executive Team. Inspectors would have views (similar to those expressed above about the OCTF Control Strategy and the Business Crime Action Plan) about the process-driven nature of the strategy and the governance for accountability and performance outcomes. However at the time of writing Inspectors understand that the Control Strategy was under review, to examine the governance aspect and to include an increased focus on vulnerability.

2.35 HMIC found that the PSNI strategic threat assessment, based on the MoRiLE[87] model, demonstrated understanding of the high threat areas such as organised crime, child sexual exploitation, and cyber crime.[88] Although as referred to in Chapter 3, the undercount of cyber crime would lower the overall assessed risk for this crime type.

2.36 The PSNI Cyber Crime Centre (CCC) was created in April 2015 as part of C2 Serious Crime Branch, and amalgamated the Serious Crime Branch E-Crime Unit and the Organised Crime Branch Cyber Unit. It brought together existing technical and investigative expertise to investigate cyber-dependent crime, and to provide forensic and technical examination of devices on behalf of the PSNI. The PSNI assessed this model as most appropriate for the strategic and operational needs of the service, in the context of overall resourcing constraints and a crime problem that was acknowledged to be growing and with potential to extend far beyond current levels.

2.37 The PSNI CCC aimed to keep people safe through a strategy based on prevention, protection and enforcement underpinned by industry engagement. It led criminal investigations into cyber-dependent crime, supported investigations into cyber-enabled crime, and provided technical and forensic support to digital examinations for serious and organised crime.

2.38 The CCC performed the functions provided in GB policing by the:

- NCA National Cyber Crime Unit;
- Regional Organised Crime Units;
- Police Service High-tech Crime Units; and
- Counter-terrorist Cyber Units.

87 Management of risk in law enforcement - a College of Policing model of risk assessment which considers the likelihood and extent of harm in a given area against the capability and capacity of the law enforcement agency to manage the threat.

88 PEEL: Police Efficiency. An Inspection of the Police Service of Northern Ireland 1-5 February 2016. HMIC August 2016. https://www.justice-ni.gov.uk/sites/default/files/publications/justice/psni-peel-efficiency.PDF

2.39 There was a network of District E-Crime Support Units (DESUs), which were a District Policing Command (DPC) resource, to support District digital forensic and technical examination capability. The DESUs were supported in policy, equipment and training by the CCC.

2.40 The CCC digital forensic provision, supported by the DESUs function at District level, incorporated the full scope of crime investigations undertaken by the PSNI, ranging from the straightforward response-orientated volume crime incidents, to complex major investigative work into terrorism, murder, child sexual exploitation, indecent images of children, and other forms of serious and organised crime.

2.41 At national level the PSNI was represented on the NCCU Strategic Governance Group which allowed it to ensure that its strategy and operational activity reflected the wider UK approach. The PSNI CCC operated under the national ROCU Cyber Unit structure to national standards, and there was capability-building through both joint-training events and the national tasking process in respect of capacity or specialist capability.

2.42 The nature and extent of cyber crime required a multi-agency, cross-jurisdictional and cross-national approach and the PSNI successfully worked with a number of partners from law enforcement, business and academia to investigate cyber crime, share information and educate on the preventative action needed to increase protection. Recent PSNI investigations involved engagement with the NCA, Interpol and US Department of Homeland Security.

2.43 The scale of cyber crime that could be perpetrated by an individual using commercially-available IT equipment was referred to earlier and is illustrated in Case Study One.

Case Study One

As part of a PSNI human trafficking operation a laptop was seized attempting to breach UK Government websites. Further examination uncovered a sophisticated phishing operation using criminal material purchased from the dark net. The phishing replicated email templates from well-known multi-national companies which were personalised with embedded links and directed the victims to a cloned website. The data given by victims was used for identity theft, fraud, theft and sale to other criminal groupings.

This was an automated process using relatively unsophisticated IT equipment which targeted 20 million email addresses in the UK, the Republic of Ireland and Spain, with over 1,000 victims identified, some in Northern Ireland, and this one seizure presents a significant challenge to police in terms of identification of victims, the scale of the investigation and the complicating nature of cross-national jurisdictional issues.

3 Delivery

3.1 Almost all crime now had a technological aspect, whether as the means by which the crime was committed, as evidence to trace the offender, or a source of intelligence to better understand the threat. As people have moved their communications and shopping online, they have done the same with their offending, insults, threats and abuse, often using social media. Police officers needed to understand this digital environment and to discriminate between cases which required police attention and those which did not.[89]

3.2 The statutory basis of policing included a general duty for police officers to prevent and investigate crime,[90] and this included cyber crime.

3.3 Cyber crime was no longer the preserve of the specialist officer and every police officer needed an understanding of how to deal with the cyber crimes, and assist the victims they encountered as part of day-to-day policing (see also HMIC report referred to earlier).

The Extent of Cyber Crime

3.4 The broader issues around the recording and reporting of cyber crime were outlined earlier, as was the need to establish its true scale and impact.

3.5 HMIC had highlighted the need for police to have an understanding of current and future demand in criminal use of technology and the way cyber crime was committed to allow identification of those most vulnerable. Data should be used to develop strategies, risk assessments, tactical implementation plans and local profiles.[91]

89 State of Policing. The Annual Assessment of Policing in England and Wales 2013/2014. Her Majesty's Chief Inspector of Constabulary. 27 November 2014. http://www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/state-of-policing-13-14.pdf

90 General functions of the police. It shall be the general duty of police officers—
(a) to protect life and property;
(b) to preserve order;
(c) to prevent the commission of offences;
(d) where an offence has been committed, to take measures to bring the offender to justice.
Police officers shall, so far as practicable, carry out their functions in co-operation with, and with the aim of securing the support of, the local community. Section 32 Police (Northern Ireland) Act 2000.

91 Real lives, real crimes. A study of digital crime and policing. Her Majesty's Inspector of Constabulary. July 2015. https://www.justiceinspectorates.gov.uk/hmic/our-work/digital-crime-and-policing/real-lives-real-crimes-a-study-of-digital-crime-and-policing/

3.6 The PSNI acknowledged that the vast majority of cyber crime was not reported, that current recording methods were not effective for capturing cyber crime, and recognised the need for an accurate picture of the scale and nature of cyber crime to enable a more effective response.[92]

3.7 Online crime was identified through the use of a 'flag' on the PSNI recording system: an offence should be flagged as a cyber crime where the reporting officer believed that, on balance of probability, the offence was committed in full or in part through a computer, computer network or other computer enabled device. There were exclusion criteria and offences should not be flagged where:

- The crime only involved a mobile phone network to make phone calls or send/receive text messages rather than an internet network. Some use of a computer network or internet technology is required. Messages sent via platforms that serve the same purpose as text messages should also be excluded, this includes BlackBerry messenger and iMessage.
- The computer was used to make or design fraudulent items such as fake gift or shopping vouchers.[93]

3.8 This was a very broad definition which did not distinguish between cyber-dependent and cyber-enabled crimes.

3.9 The first complete year in which online crime data was available was 2014-15 in which 634 offences were recorded and this increased to 828 in 2015-16, which accounted for 0.8% of all crimes recorded by the PSNI. The main types of offences recorded were harassment, sexual offences, obscene publications and blackmail.[94]

3.10 The PSNI acknowledged that there was a recognised undercount on the PSNI Saturn[95] system of recorded cyber crimes.

3.11 Reports to Action Fraud were not included in the PSNI crime statistics. From 1 April 2015, Action Fraud assumed responsibility for recording fraud offences (which includes financially motivated cyber crime) and these were no longer recorded by the PSNI.[96] The number of crimes reported to Action Fraud in the year to March 2016 was 2,634, which represented approximately 2.5% of overall PSNI recorded crime.

92 Northern Ireland Assembly. Committee for Justice. Official Report Hansard Business Crime Stakeholder Event. 14 May 2015.
93 Annual report and threat assessment 2015. Organised Crime Task Force. www.octf.gov.uk
94 PSNI. Trends in Recorded Crime in Northern Ireland 1998/99 to 2015/16. https://www.psni.police.uk/globalassets/inside-the-psni/our-statistics/police-recorded-crime-statistics/documents/police_recorded_crime_in_northern_ireland_1998-99_to_2015-16.pdf
95 Saturn is an PSNI internal Management Information System.
96 Police Recorded Crime in Northern Ireland: Monthly update to 30 September 2016. Published 27 October 2016. https://www.psni.police.uk/globalassets/inside-the-psni/our-statistics/police-recorded-crime-statistics/2016/september/monthly-crime-bulletin-period-ending-sep-16.pdf

3.12 The technical data provided by Action Fraud to the PSNI showed a high number of cyber attacks[97] against computers in Northern Ireland; in the single month of September 2015 there were over 14,500 malware installations detected in Northern Ireland against over 4,000 unique IP addresses[98] (14,500 potential offences represented approximately 14% of annual PSNI recorded crime). When this was compared to the full-year recorded online crime total of 828 offences for 2015-16, it was evident that there was a significant discrepancy.

3.13 The Justice Minister told the Northern Ireland Assembly that current reporting mechanisms did not allow the provision of figures for frauds, blackmails and other financially motivated crimes which utilised the cyber environment.[99] Similarly it was not possible to identify convictions resulting from financial cyber crime without a manual trawl of court records.[100]

3.14 A comprehensive assessment of cyber crime was necessary for the PSNI to provide an effective response to the current threat, to allocate resources to this fast developing crime area (both for criminal methodologies and IT technological advances), and to ensure the level of training for officers at all levels met investigative and victim needs. When the recognised issues of under-reporting of cyber crime were taken alongside those of recording of cyber crimes and fraud figures, this created a gap between the true scale and impact of cyber crime, and that which was reported in the Northern Ireland Crime Statistics.

3.15 Inspectors acknowledge and welcome the fact that the PSNI Cyber Crime Control Strategy had a workstream to determine the extent of cyber crime in Northern Ireland which should address a number of these areas. However it was the view of Inspectors that a more fundamental analysis of cyber crime was needed, to include reporting, recording and developing criminal methodologies. Accurate analysis was also critical to the development of an effective Cyber Strategy for Northern Ireland.

Strategic Recommendation 1

The PSNI should undertake a comprehensive strategic analysis of cyber crime as it affects Northern Ireland. This should include the issues identified in this report about under-reporting and recording of the cyber crime types. It should also consider the potential future demand on police, together with the investigative implications for policing developing areas, for example, crypto currencies, 'cloud' use and the dark net. This analysis should be prioritised and completed within six months of the publication of this report.

97 Action Fraud reports refer to cyber crimes and cyber attacks. A cyber crime is a single act involving a computer which is prohibited by law. A cyber attack is a collection of activities undertaken via computers and computer networks towards a specific purpose such as stealing money, information or damaging property. PSNI internal document.

98 Every instance of a malware installation is potentially a crime under the Computer Misuse Act.

99 Northern Ireland Assembly. Written Answer. AQW 3305/16-21 Answered 16 September 2016.

100 Northern Ireland Assembly. Written Answer. AQW 3304/16-21 Answered 16 September 2016.

Funding

3.16 Police resourcing to address cyber crime came from the Service Budget, and the PSNI viewed its ability to financially plan in this area to have been hampered by the funding arrangement for Northern Ireland. As referred to in Chapter 2, additional money was allocated to the National Cyber Security Programme which transferred to the Northern Ireland Assembly through the NI Block Grant. Funding decisions about cyber security were then taken by the Northern Ireland Executive, and the PSNI was required to bid for specific projects, supported by business cases.[101]

3.17 The PSNI had submitted applications for funding in a number of areas and these included:

- vehicles for digital forensic scene attendance (as referred to below) to provide increased capability for live-time examination of crime scenes and data analysis;
- six additional staff for the CCC, one of whom would be a Protect Officer[102] (see below); and
- a community SME (Small and Medium-sized Enterprise) project for web application firewall to provide cyber security.

3.18 The National Cyber Security Strategy committed £1.9 billion over five years, and at the time of writing this had just been announced, so it was not clear how this would be distributed. It would be the view of CJI that this budget should be ring-fenced for cyber security and the DOJ should make the case for this to be used to further the Cyber Strategy for Northern Ireland.

PSNI Cyber Crime Investigation

3.19 In terms of delivery, the type of cyber crime dictated how it was investigated by PSNI:

- Cyber-dependent crime: led by CCC.
- Cyber-enabled crime:
  - Serious cyber-enabled crime led by CCC;
  - Volume and less serious cyber-enabled crime led by district police/Reactive and Organised Crime with support and assistance where required by the DESU/CCC; and
  - Fraud-related cyber-enabled crime led by C1 Economic Crime Unit (ECU).
- Cyber-facilitated crime: led by district police with support and assistance where required by the DESU/CCC.

Figure 1 (see Appendix 4) outlines the investigation pathways for cyber crime.

101 Northern Ireland Assembly. Written Question AQW 51013/11-16. Answered 27 November 2015. http://aims.niassembly.gov.uk/questions/printquestionsummary.aspx?docid=249863

102 'Protect' is one of the four strands of the UK counter-terrorism strategy known as the 4 Ps. The others are Pursue, Prevent and Prepare.

Cyber-dependent Crime

The Cyber Crime Centre

3.20 At national level the CCC had good links with the NCA, its NCCU and the ROCUs. It was fully embedded in the UK national tasking arrangements for major cyber incidents. The CCC performed the role of a ROCU in Northern Ireland and as such, it was a member of the national meeting structure to discuss and to co-ordinate activity in response to major incidents. This involvement at national level would continue as the NCSC coordinating role became established. Inspectors understand that the PSNI was considering seeking funding through the national programme to second an officer in the NCSC to further improve operational effectiveness and coordination.

3.21 There was a responsibility on Internet Service Providers (ISPs) to regulate and police users of their services. This was a global issue and at national level, the NCA Strategic Cyber Industry Group provided the forum for law enforcement to work in partnership with private sector organisations to address these issues. The PSNI CCC was represented on this group and Inspectors understand that work had taken place with the IT industry in general, and ISPs in particular, to develop this area.

3.22 The former PSNI Serious Crime Branch (C2) E-Crime Unit had a staffing level of two D/Sergeants and 22 D/Constables in 2009. The overall staffing reductions in the PSNI together with the constricting economic climate meant that by early 2015, the staffing level had been halved. Following the creation of the CCC resourcing was increased to bring the CCC to its current establishment of two D/Sergeants and 18 D/Constables.

3.23 The CCC provided the PSNI operational capacity to tackle cyber crime in the following areas:

Investigations

3.24 The CCC was the lead department for investigating cyber-dependent and serious cyber-enabled crime, and provided support and assistance to the ECU, Districts and Reactive Crime for cyber-enabled and facilitated crimes. Investigating officers were trained to nationally agreed standards and involved in highly specialised investigations. Regional and national collaboration provided mutual assistance, assurance and cooperation.

3.25 Advances in technology, anonymity servers and the use of the dark net (such as outlined in Case Study Two) were making it increasingly difficult for law enforcement agencies, including the PSNI, to trace offenders and collect evidence in cyber crime investigations.

Case Study Two

A man was charged with possession of a firearm, ammunition and a silencer in suspicious circumstances, with intent to endanger life, and with possession and intent to supply Class A drugs.

The weapon and silencer were purchased on the dark net and a lengthy and detailed police operation, including covert activity, led to the subsequent arrest and searches in Belfast and North Down. The illegal drugs had also been purchased on the dark net.[103]

3.26 Emerging online or 'cloud' storage of data made it more difficult for law enforcement agencies to retrieve evidence during searches. Traditional methods of seizing ICT paraphernalia were becoming increasingly ineffective with officers having to download data at the scene from ICT devices, which was only possible if these were online. Criminals were alert to this and obtaining the necessary data by other means was much more resource intensive, and the location of the online hosting companies in most cases were outside the jurisdiction,[104] or in hard-to-reach jurisdictions which further complicated the process.

3.27 At the time of the inspection the CCC had a small number of investigating officers (one D/Sergeant and three D/Constables). These officers were investigating highly complex and wide-reaching cases (see for example Case Studies 1, 2, and 3) and their capacity was limited. In addition, these officers had commitments to provide internal PSNI training, and to support outside organisations and events as part of the Protect and Prevent work, including to Get Safe Online events throughout Northern Ireland.

3.28 Whilst Inspectors are aware of the balance that needed to be struck between visible and specialist policing, it would be the view of Inspectors that there was insufficient resilience in the investigative element of the CCC to deal with the current and potential future levels of cyber-dependent crime. The CCC had a regional function as part of the national tasking process for significant cyber crimes, and if required, there was capacity within the wider CCC and C2 to augment major investigations. The PSNI should keep this under review in the light of the current and projected future demand, based on the outcome of the analysis at Strategic Recommendation 1. Inspectors understand that a case was being made for an additional six officers (five of whom would be investigative) as part of the national cyber security funding, but at the time of writing, the result of this case was not known.

103 http://www.belfasttelegraph.co.uk/news/northern-ireland/serving-psni-officer-allen-kennedy-involved-in-drug-dealing-court-hears-35163794.html

104 See also Real lives, real crimes. A study of digital crime and policing. Her Majesty's Inspector of Constabulary. July 2015. https://www.justiceinspectorates.gov.uk/hmic/our-work/digital-crime-and-policing/real-lives-real-crimes-a-study-of-digital-crime-and-policing/

Case Study Three

Two drug traffickers from Northern Ireland used the 'Silk Road', a dark net website to buy and sell drugs, and to move cocaine, MDMA, herbal cannabis and mephedrone into and out of the UK.

When investigators arrested the men they seized orders, containing different Class A and B drugs, awaiting dispatch to customers in the US, UK, Russia, Sweden, Ireland, Greece and Israel.

Investigation by SOCA, the PSNI and the FBI showed that orders for drugs were made through digital communication such as emails, website forums and instant messaging services, using suppliers in the Netherlands, China and North America. Payment was by virtual currencies such as Bitcoin or money transfer services.

In follow-up property searches, police seized phones, computers, iPads, passports and banking details, printers, packaging and large quantities of controlled drugs including cannabis, ecstasy, 4-MEC, amphetamine and LSD substitute. The men were jailed for 14 years.[105]

Digital Forensic Examinations

3.29 Forensic examination and interrogation of digital media seized as part of criminal investigations, both as devices and the emerging area of 'cloud' storage examination and data seizure, were a significant proportion of the CCC workload. There was an emerging requirement to access live systems and on-line storage with a consequent need for the latest technology to examine and recover evidential material.

3.30 The CCC processed all digital forensic examinations for the PSNI, including indecent images of children, with the exception of the less technical mobile phone and CCTV work undertaken by the DESUs. There were eight officers fully trained for the role and nine new officers who were part-way through a two-year training programme.

3.31 The digital forensic officers were also required to attend the scenes of pre-planned search operations where it was suspected that there were complex IT or technical issues.

3.32 The demand for digital forensic examinations of devices was high and increasing over time. As device capacity and complexity had increased so had the length of time required for investigations. The PSNI estimated that the number of devices requiring examination had not increased significantly in the past five years; however the digital data held on devices had increased by 800%.

105 National Crime Agency. http://www.nationalcrimeagency.gov.uk/news/608-international-dark-web-drug-dealers-specialised-in-party-packs See also Organised Crime Task Force. Annual Report and Threat Assessment 2015. www.octf.gov.uk

3.33 At the end of 2015 there was a backlog of investigation requests of around one year for computers and two months for mobile phone devices.[106] By late 2016 computer examination time had lengthened to 18 months. There was a prioritisation system to ensure those cases with significant risk or harm were not unduly delayed. When the new digital forensic officers were fully trained there would be the potential to reduce the backlog, dependent on future demand and prioritisation.

3.34 Delays in digital forensic examinations had significant implications for victims, for investigations and for delaying criminal cases. The PSNI had taken measures to try and limit submissions, and this had included involvement with search teams and investigating officers to encourage a focus on the seizure of items with most evidential value. However the increasing capacity of phones and computer equipment meant increasingly lengthy examinations.

3.35 The CCC was moving towards an IT solution (NUIX) where the content of a device could be made available to investigating officers remotely. This was more effective from an investigative perspective and transferred examination of device content from the CCC to the Investigating Officer, and whilst this would potentially increase capacity at the CCC, it had a potential knock-on resource impact for Districts and Departments. Inspectors understand that the roll-out of the system hardware and software had cost implications which would have to compete with other PSNI internal priorities. It would be the view of Inspectors that any decision should include consideration of the potential of NUIX to increase investigative effectiveness and reduce the digital forensic backlogs.

3.36 This was an area of risk which the PSNI was acutely aware of, and as referred to earlier, HMIC had highlighted the need for forces to have capacity to examine devices in an effective and speedy manner.

3.37 Inspectors were aware of the measures the PSNI had taken in an attempt to address the backlogs, and the combination of the additional digital forensic staff when their training has been completed, the work to limit supply, and the technology to transfer device content to remote Investigating Officers all had the potential to reduce the backlog over time, assuming demand remained static.

3.38 Other options had been considered including scope for civilianisation. Inspectors understand the risk to the PSNI of providing an intensive and expensive two-year training programme to develop a level of expertise which was highly desirable to outside industry, and experience from England and Wales had taught that police remuneration cannot compete with the private sector. Consequently when trained staff leave the police service they cannot be replaced in the short-term.

106 Internal Audit Report 2015/2016. Internal Audit Review of PSNI E-crime. PWR Report. Internal PSNI document.

3.39 It would be the view of Inspectors that technological progress and its adoption to commit and facilitate crime are such that increasing demand for digital forensics over time is inevitable. Significant delays in forensic examinations impact on the effectiveness of criminal investigations, the service provided to victims and the speed of justice through the courts.

Operational recommendation 1

The PSNI should reduce the backlog of digital forensic examinations to an acceptable level. This should be based on an assessment of potential future demand and consideration of all options including:

- **the resourcing requirements to meet demand;**
- **the potential for outsourcing;**
- **the roll-out of NUIX;**
- **the potential for use of automated technology;**
- **the scope for civilianisation; and**
- **the training and awareness provided to officers about seizure and examination of technological devices.**

Technical Capability

3.40 There was good specialist capability in the PSNI which was being developed to support investigations into criminal use of IT networks, malware analysis and other technical methods.

3.41 This would be a continual process as technology develops, and it was important for the CCC to maintain and develop investigative, digital forensic capacity and expertise to deal with new technology. This included increasing IT capacities, digital encryption (which is part of a wider national programme to move away from 'dead box'[107] forensics to mirror the trend of criminals, who are increasingly moving to online and 'cloud' storage), the development of digital currencies and the increasing use of the dark net. The PSNI had submitted a business case for two specialist vehicles to allow for the necessary technology to be used at the scene of a 'live' cyber incident, and at the time of writing, Inspectors understand that this funding had been approved.

3.42 A new Cyber Crime Centre was being built in Belfast due for completion in 2017. The centre would house the CCC forensic, technical and investigative resources and would contain the IT infrastructure and capability to lead the PSNI's response to cyber crime.

3.43 The CCC also had a key role in providing awareness and education about the wider aspects of cyber crime is and this is referred to later in this chapter.

107 Digital forensic examination of a seized piece of computer hardware.

The Public Prosecution Service (PPS)

3.44 Prosecution for cyber-dependent crimes was considered by a small number of prosecutors who had undertaken cyber-specific training, some of which was through the CCC. The volume of files was not high but cases could be complicated by the need for requests to other jurisdictions for evidential material, the volume and complexity of the digital forensic evidence, and the delays in examination backlogs referred to above.

3.45 There were good working relationships between the CCC and the PPS Prosecutors who gave prosecutorial advice where appropriate, and where required, there was liaison with the PSNI at the early stages of serious or complex investigations.

3.46 The PPS Prosecutors were alert to the issues of money transfer, crypto currencies and use of the dark net, and liaised with police Investigating Officers about the gathering and presentation of evidential material. The cross-jurisdictional nature of cyber crime could require international letters of request for evidential material from other countries which could delay investigations.

Cyber-enabled Crime

3.47 Cyber-enabled crime covered the broad swathe of 'traditional' offences which were increased in their scale or reach by the use of technology. The first part of this section covers fraud which has different reporting arrangements; the remainder refers to other cyber-enabled crime which was a District policing/Reactive Crime responsibility.

Fraud

3.48 On 1 April 2015 Action Fraud assumed responsibility for the central recording of fraud offences previously recorded by the PSNI, (for police Forces in England and Wales this happened on 1 April 2014). From this date all incidents of fraud and related cyber crime in Northern Ireland were reported directly to Action Fraud, unless a 'call for service' was required.[108] The process was relatively new and Inspectors were told that it was still 'bedding-in'.

3.49 HMIC found misunderstanding of the role of Action Fraud was widespread amongst police in England and Wales with a lack of knowledge at all ranks.[109] They highlighted the importance of an effective and immediate fast response to cyber fraud where money could be transferred from victims' bank accounts to other accounts often within 24 hours of the original fraud.[110] It was important therefore that appropriate cases were identified as 'calls for service' as there could be increased chances of success if immediate action was taken, for example, if the victim contacted their bank.

108 A 'call for service' is defined as: when a fraud is being committed, or recently occurred (within 24 hours); or, where police know the suspect and they reside in Northern Ireland; or, where the victim is perceived to be vulnerable (this may be through age, or by way of mental, or physical impairment, or in need of care and support); or, finally where it is believed that it is important to report the incident to police in order that police can secure and preserve evidence, or prevent loss (i.e. CCTV, recover large amounts of money transferred from bank accounts before the criminal can remove it). https://www.psni.police.uk/crime/fraud/Reporting-Fraud/

109 Real lives, real crimes. A study of digital crime and policing. Her Majesty's Inspector of Constabulary. July 2015. https://www.justiceinspectorates.gov.uk/hmic/our-work/digital-crime-and-policing/real-lives-real-crimes-a-study-of-digital-crime-and-policing/

110 Ibid.

3.50 There had been a number of teething difficulties with Action Fraud across England and Wales, including confusion among businesses when they had been victim of a 'live' cyber attack, which caused delays in reporting, and in turn risked causing increased harm to the businesses involved. As a result, Action Fraud was moving to a 24/7 reporting capability from late 2016 with 'live attacks' triaged to establish if an immediate response was required.

3.51 Inspectors were aware that the PSNI had concerns that there were offences which Action Fraud recording may not include, for example cyber crimes with no financial loss (which could include ransomware or blackmail where the demand had not been paid); and attempted offences like phishing, spear-phishing or whaling (see Appendix 1), where the data was required for intelligence purposes and trend analysis.

3.52 A quarterly Force Cyber Profile was issued to the PSNI by the National Fraud Intelligence Bureau (NFIB) which provided a statistical analysis of crime trends, types and emerging techniques. This included data from technical sources, for example, interventions in place by law enforcement agencies to intercept data making its way to criminals, and included sink holes, honey nets and spam traps[111]. It also provided details of the reports to Action Fraud from NI. The report distinguished between cyber crimes[112] and cyber attacks.[113]

3.53 Inspectors were provided with the cyber force profile for Northern Ireland for the last quarter in 2015 which showed that reported cyber-dependent crimes are relatively low at 34 for the period, although impact was more significant with a total financial loss in the region of £268,000, the highest financial loss was £173,000, and 33% of victims stating the crime had a significant or severe impact on their lives. Cyber-enabled crimes were at a similar level (40) with a total loss of £22,000.

3.54 The profile showed how activities linked to cyber crime were taking place in Northern Ireland, including the various types of malware attacks ranging from 0.29% to 3.84% of the national level.

3.55 The PSNI Cyber Crime Problem Profile made reference to the Action Fraud Force Profile, although at District level there was little knowledge of the profile information or how it related to the District or policing priorities. It was not clear how the analysis contributed to the PSNI Cyber Control Strategy.

3.56 Whilst there was wide recognition of the merits of a national approach to an international problem, there were some concerns expressed to Inspectors about the effectiveness of Action Fraud, the numbers of cases that were investigated, the potential delays in investigations and whether the Action Fraud reporting procedures had a sufficient victim focus.

111 These are technical terms for programmes to intercept spam, unsolicited messages or other data.
112 A single act involving a computer which is prohibited by law, (more likely to be cyber-dependent).
113 A collection of activities undertaken via computers and computer networks towards a specific purpose such as stealing money, stealing information or damaging property. (more likely to be cyber-enabled)

3.57 There was also the wider issue about reporting crimes directly to a national body based in London, when traditionally most local people would instinctively contact the PSNI when they had been the victim of a crime, and it was suggested to Inspectors that this, combined with the cumbersome reporting arrangements,[114] could result in some victims discontinuing their report. Inspectors were not aware of the 'drop-off' rate for Northern Ireland but understand that in some areas of England and Wales this had been significant.

3.58 Figures obtained by an industry body through Freedom of Information requests to police forces in England and Wales showed that of the 248,200 crime reports to Action Fraud in 2014-15, only 28% (69,000) were disseminated to local police forces for investigation, and of that 28% only 17% (12,000) resulted in a judicial outcome.[115]

3.59 Data provided to Inspectors for 2015-16 for Northern Ireland showed that the proportion of cases referred to the PSNI from Action Fraud for investigation was 15.6% which was significantly lower than the case in England and Wales. Cases were referred to the PSNI by Action Fraud where it was believed that the suspect resided in Northern Ireland, or if the victims of fraud (perpetrated by a suspect who lived elsewhere) lived in Northern Ireland. Of the cases referred to the PSNI however, the proportion which had a judicial outcome was almost double that of England and Wales (32.2% compared to 17%).

3.60 In overall terms this means that just 5.4% of frauds reported in Northern Ireland had a judicial outcome, and if the level of under-reporting was taken into account, this was likely to be an over-estimate of the true position.

3.61 The Action Fraud IT system was not compatible with the PSNI system (or with some other UK Forces) although work had commenced to address this. There was a cumbersome process for transferring cases to the PSNI, however a review within C1 (Reactive and Organised Crime Branch) Economic Crime Unit (ECU) and a manual trawl of the records had led to:

- live-time monitoring of cases;
- tasking of investigations and investigative strategies to Reactive Crime or District policing as appropriate; and
- tasking of victim care deployments.

3.62 This had undoubtedly contributed to the higher proportion of judicial outcomes.

114 It takes about 20 minutes to complete the Action Fraud report form. Once started it has to be completed in one session so the person reporting must have all relevant information to hand, e.g. names, dates, information about the suspect and details of how the money was lost. www.actionfraud.police.uk

115 Partners against crime. How can industry help the police to fight cyber crime? Tech UK. October 2015. http://www.techuk.org/insights/reports/item/6102-techuk-calls-on-police-and-industry-to-work-together-to-tackle-cyber-crime

3.63 The PSNI internal review had also introduced organisational procedures so that officers dispatched to an incident identified on the Command and Control system as a 'fraud' would automatically receive a Niche-generated task, which required the officer to confirm:

- details had been passed to Action Fraud, a reference number obtained and updated on Niche, and if there was a vulnerable victim, that the District Contact Management Support Unit had been updated; and
- if there was 'no fraud' officers were reminded that even if the victim did not wish to report the incident, it still must be reported to Action Fraud.

3.64 At the time of writing this new procedure was being introduced so Inspectors cannot comment on the impact it had made to recording and reporting, but it was a welcome initiative and had the potential to significantly reduce the number of frauds not being reported to Action Fraud at the earliest opportunity.

3.65 At the time of the inspection C1 E-Crime Unit was considering an initiative developed by Surrey Police to identify and support vulnerable victims of fraud and to provide preventative and support measures to protect victims and safeguard them from further targeting. Crucial to the initiative was the wider message of crime prevention and advice. Inspectors would see this as a valuable contribution to victim support and preventing repeat victimisation and look forward to seeing how this develops.

3.66 At District level there were mixed views about Action Fraud. District Command Teams were knowledgeable about the role of Action Fraud and the reporting process. However Inspectors were advised that there was very little feedback or management information about the numbers or types of cases reported to Action Fraud from the District, the numbers referred back to the District for investigation or the outcomes in respect of those cases. District Command Teams were not aware of the PSNI Cyber Force Profile, victim profiles or reported crime in relation to their respective areas of command. Neither were they in a position to state with any authority how fraud and financially motivated cyber crime were affecting the District or of any pattern, trend or analytical information that would allow preventative or awareness-raising measures to be taken.

3.67 Amongst first responders there were varying degrees of knowledge about Action Fraud. Whilst most operational officers spoken to by Inspectors were aware of Action Fraud and the reporting procedures, some officers had a more limited knowledge of the referral process, and some did not fully understand the reporting procedures or the distinction of cases which constituted a 'call for service'.

3.68 There was a widespread view among District police that members of the public and the business community had a limited knowledge of Action Fraud and would, in the first instance, contact their local police station. This is similar to what Inspectors found during the stakeholder consultation where many had little awareness of, or contact with, Action Fraud.

Operational recommendation 2

Approaching two years from the transfer to Action Fraud it would be appropriate for the PSNI to formally review the effectiveness of the recording and investigation of fraud and financially motivated cyber crime in Northern Ireland, and the service, support and advice provided to victims. This should be completed within nine months of the publication of this report.

District Policing

3.69 Cyber-enabled crimes were primarily investigated at District level by Reactive Crime or Local Policing Team (LPT) officers. (Frauds also fell into this category, led by the C1 E-Crime Unit, as referred to above.) There was capability for digital forensic examination of mobile phones at DESU level. For the more complex investigations or digital forensics, support and assistance were available from the CCC.

3.70 There was limited data on the types of cyber-enabled crime reported to Districts, but that provided to Inspectors, together with the interview discussions with District police indicated that the main types of offences included harassment, blackmail and sexual offences.

3.71 Many of these cases were traditional everyday crimes which had moved online. Verbal disputes, insults, harassment and abuse had moved from face-to-face encounters to online activity on Facebook and other social media sites. Investigations could be complicated by issues of evidence retrieval or if the perpetrator was outside the jurisdiction.

Case Study Four

A Tyrone teenager tragically took his own life in 2015 after having been the victim of webcam blackmail. The perpetrator had committed the crime from another country and following work through the NCA and Europol, the PSNI identified the alleged offender who was arrested, charged with the assistance of the Romanian Police and Justice Authorities and appeared in a Bucharest Court.

3.72 As referred to previously, fraud was not included in the data but Inspectors were advised that this was also one of the main types of crime that District police were called to deal with and involved credit card fraud and various types of scams, many of which were as a result of phishing. It was a common theme in discussions with District police that many of the scams were reported well after the event which limited the potential for investigation.

3.73 A number of the LPT officers spoken to by Inspectors were conscious of the complexities of cyber crime and said they would benefit from more training. Some officers said they had very limited training. Many did not feel confident in giving advice to victims about what could

be done to protect themselves from cyber crime, or of the advice and resources that were available online to assist. Some said they 'muddled through' investigations and others said that any advice they gave was based on their common-sense experiences.[116] Officers were aware however that advice was available from the District, Reactive Crime and the DESUs. There was comprehensive information available to police officers on *PoliceNet* (the PSNI's intranet site) covering all aspects of cyber crime;[117] and whilst officers were aware of this resource, many said they did not have time to study it.

3.74 Restricted access to the internet for day-to-day policing was raised with Inspectors as an impediment to effective policing. The availability and use of the internet was, for a number of very valid reasons, tightly controlled in the PSNI, and the access to go online for investigative purposes was given to a cadre of officers who were ROSIE (Research, Open-source, Internet and E-mail) trained. This training enabled officers to undertake internet searches, create email addresses and social media profiles for investigative purposes and to record and present evidence. At the time of writing there were 229 ROSIE trained officers in the PSNI, although not all were first response officers: 74% were in Crime Operations Department. Districts were concerned about the availability of these officers, particularly outside office hours.

3.75 There was a separate, but related issue about access to open-source material available on the internet for routine policing purposes. So much daily activity had moved online that access to open-source internet material was fundamental to many of the most basic police investigations. The two examples most frequently given to Inspectors were those of missing persons and stolen property. Unless ROSIE trained, officers were unable to access non-private social media sites to establish if there was information relevant to the report of a missing person. Similarly, in the case of stolen property, investigating officers could not check for example eBay, Gumtree or other online market-places, if the stolen property had been offered for sale. This appears to Inspectors to be overly-restrictive.

Operational recommendation 3

The PSNI should review online access for first response officers with a view to either extending ROSIE training to ensure there is a sufficient number of trained officers to meet the operational demand, or alternatively to provide stand-alone internet terminals in operational police stations for investigating officers, with an appropriate level of awareness and guidance provided to all operational officers.

116 See also HMIC study of digital policing which also found a mixed picture of police knowledge of, and training in, digital crimes and modern technology. Real lives, real crimes. A study of digital crime and policing. Her Majesty's Inspector of Constabulary. July 2015. https://www.justiceinspectorates.gov.uk/hmic/our-work/digital-crime-and-policing/real-lives-real-crimes-a-study-of-digital-crime-and-policing/

117 This includes information on Cyber crime Contacts; first responders; cyber support units; phishing; malware; ransomware; webcam blackmail; DDoS attacks; network intrusion; man-in-the-middle; surface web/deep web/dark web; market places; PBX hacks and online covert deployments.

3.76 It would be the view of Inspectors that this overlaps with the DESU function and this should be incorporated as part of the DESU review (see operational recommendation 4).

District E-Crime Support Units

3.77 The DESUs were a District Policing Command resource for first-stage digital forensic examination of mobile phones primarily for cyber-enabled crime. DESUs were located at District level and some Branches in Crime Operations Department had a part-time DESU capability. The DESU officers had good communication with operational District and Reactive Crime officers, and an effective support mechanism from the CCC for the more complex cases.

3.78 The role of the DESUs included digital forensic examination of seized mobile phones, CCTV recovery, identification and conversion to evidential standard, and ROSIE and open-source searches for District and Reactive Crime investigating officers. DESUs did not have an investigative function.

3.79 The examination backlogs varied across the units from several weeks to over six months. There was a prioritisation process to examine the devices in cases where there were risk or harm considerations.

3.80 Mobile phone ownership and use extended to all types of criminality and DESUs estimate that approximately 60% of seizures were from Reactive Crime/Public Protection Units and 40% from District LPTs. As was the case with the CCC, increasing phone capacity had extended examination times.

3.81 The requirements for CCTV retrieval and examination had grown with increasing numbers of businesses having security systems, and with city and town centre CCTV schemes across Northern Ireland which generated demand for video evidence.

3.82 DESUs were staffed by police officers who were required to give evidence in Magistrates' Courts. If a case was required for the Crown Court then the examination of the device had to be repeated and the evidence presented by a CCC officer. This appeared to create inefficiency and Inspectors could see no reason why this should be the case for routine digital forensic examinations of mobile phones.

3.83 The digital forensic functions performed by the DESUs were critical to effective investigation of crime. However Inspectors were aware of concerns having been expressed about their capacity, workload and availability to provide advice and support to District police outside office hours. Inspectors understand that a Review of the DESUs[118] was being undertaken by a senior officer in DPC and was due to report in 2017. CJI welcomes this review as an opportunity to re-examine the effectiveness of the provision of digital forensics for Reactive Crime and District policing.

118 This is a PSNI Service First Continuous Improvement Project. Annual Policing Plan for Northern Ireland. Northern Ireland Policing Board. Annual Policing Plan for Northern Ireland 2016-2017.March 2016. http://www.nipolicingboard.org.uk/final_pdf_-_policing_plan_2016-17.pdf

Operational recommendation 4

The DESU Review should address:

- the DESU staffing level and case load against historic and potential future demand, and increasing device capacity (informed by the outcomes of Strategic Recommendation 1);
- the potential for DESU officers to give evidence on digital forensic examinations in Crown Court; and
- whether there is scope to civilianise elements of the DESU role, for example, CCTV retrieval and examination.

The Public Prosecution Service

3.84 With the exception of the larger fraud cases which were handled by PPS Fraud and Departmental Section, prosecution files for cyber-enabled crime from the Districts and Reactive Crime were allocated to the PPS Regional Prosecutors, and these were processed in a similar way to other volume crime files.

3.85 Many of the cyber-enabled crimes had complex and lengthy evidential material from phones and computers and, depending on how it was presented by police, could be time consuming to examine and consider. Inspectors were advised that voluminous phone data was regularly submitted to the PPS where the investigating officer had not highlighted the relevant evidential portions. Good technical evidence strengthened the prosecution cases and many of the specialist PSNI Departments, for example Crime Operations, presented complex evidence with analytical supporting information.

3.86 The prosecutors that Inspectors spoke to had generally good working relationships with police officers in the DESUs. As in the case of cyber-dependent crime, the digital forensic examination backlogs had caused delays, and Inspectors were advised that as a result, there had been cases where abuse of process applications had been made to the Court.

3.87 It was the view of Prosecutors in the PPS Regions that some District LPT officers were inexperienced in investigating cyber-enabled crimes and this showed in the gathering and presentation of evidence for prosecution files.

Awareness and Education

3.88 Internal PSNI and external awareness and education amongst the business and wider community in Northern Ireland were significant factors in respect of both cyber-dependent and cyber-enabled crime, and were key aspects of the Prevent and Protect strands of the OCTF and PSNI Control Strategies for cyber crime.

Police Training

3.89 Proper training and awareness was vital for police officers in all areas of crime prevention and investigation, and this was particularly so in the fast-changing world of cyber crime.

3.90 HMIC recognised that bringing the handling of digital cases within the general skill set of every police officer required them to have the necessary understanding of technology and its implications for the investigation of crime. Raising the skill base of officers and police staff who were likely to be required to deal with these cases was essential.[119]

3.91 In England and Wales training had been an integral aspect of the UK Cyber Security Strategy with training in tackling cyber crime delivered to police forces. Online National Centre for Applied Learning Technologies (NCALT) modules[120] were rolled out in 2013, although uptake had been poor. The College of Policing and police forces had also delivered a classroom-based course for police investigators.[121]

3.92 The PSNI was aware of the need for training and awareness for officers in relation to cyber crime, and had commenced an internal education programme to develop knowledge and understanding at various levels in the service.

3.93 The PSNI control strategy identified training as an issue and had an outcome to increase the capacity and capability of the PSNI to tackle cyber-dependent and cyber-enabled crime in Northern Ireland. Activities included:

- development and expansion of the skills and capacity of the CCC;
- CCC staff to share knowledge of cyber crime within PSNI; and
- maintain up-to-date NCALT training for officers and staff.

3.94 From 2014 cyber crime training for officers joining the PSNI had been an element of the Student Officer Training Programme (SOTP) as part of Stage 1.[122] This was a one hour lesson which explained the term 'cyber crime' and the role of the CCC and DESUs. It also gave an

119 Real lives, real crimes. A study of digital crime and policing. Her Majesty's Inspector of Constabulary. July 2015. https://www.justiceinspectorates.gov.uk/hmic/our-work/digital-crime-and-policing/real-lives-real-crimes-a-study-of-digital-crime-and-policing/

120 NCALT is a collaboration between the College of Policing and the Metropolitan Police. The programme is divided into modules:
- Cyber Crime and Digital Policing;
- Cyber Crime and Digital Policing Investigations;
- Digital Communications, Social Media, Cyber Crime and Policing; and
- Cyber Crime and Digital Policing Introduction. Real lives, real crimes. A study of digital crime and policing.

Her Majesty's Inspector of Constabulary. July 2015. https://www.justiceinspectorates.gov.uk/hmic/our-work/digital-crime-and-policing/real-lives-real-crimes-a-study-of-digital-crime-and-policing/

121 The UK Cyber Security Strategy. Report on Progress and Forward Plans. December 2014. Cabinet Office. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf

122 The Student Officer Training Programme is an initial 22 week training programme (Stage 1) and those who successfully complete it attest as Probationary Constables for a two year period and are assigned to a Local Policing Team. Probationary constables return to the Police College for Stage 2 and 3 training during this period before being confirmed in the rank of a Constable.

overview of the Association of Chief Police Officers (ACPO) Good Practice Guide for digital evidence, the items which may be encountered at a scene search for electronic evidence, and the procedures for submitting items for examination to the CCC or DESU.

3.95 Stage 2 training was a two-hour lesson aimed at developing the students' knowledge of cyber-enabled crime and the techniques used by police to investigate these, and the lesson contained various scenarios including frauds, Action Fraud, online harassment, child abuse and stolen property on online market-places. There was very comprehensive pre-read material which students undertook by self-directed learning.

3.96 For serving officers who joined the PSNI prior to 2014 cyber crime training was through NCALT modules, by self-directed learning from the resources on *PoliceNet*, or through District Training. Inspectors understand that NCALT cyber modules were not mandatory for PSNI officers and there had been a low take-up rate. Comment was made earlier about officers accessing online resources, and officers spoken to by Inspectors said that cyber crime had not been included in District Training, although Inspectors understand that some Districts had covered it.

3.97 There was training for Reactive Crime officers as part of the ICIDP (initial detective training) and prior to commencing officers were required to have successfully completed the NCALT cyber crime modules. To use the internet for investigative purposes officers had to be appropriately trained (the course was entitled ROSIE and was referred to at pars 3.74/.75). Although it was intended to deliver the full ROSIE package to trainee Detectives, this had been reduced to two days due to the restricted internet access available to operational officers.

3.98 Officers from the CCC delivered elements of internal PSNI initial and detective training.

3.99 Officers from the CCC had received specialist training relating to their role and the digital forensic extraction methodologies. Some of the training had been at national ROCU level. The nature of technology development meant that much of this training was bespoke and had to be sourced from the private sector. Whilst this was essential it was also relatively expensive.

3.100 The process for PSNI Serious Crime Branch (C2) to bid for training commitments was through the PSNI's Training Branch. Inspectors understand that this had been problematic due to the highly specialist nature of the requests and the associated costs. For the PSNI to maintain operational effectiveness in this fast developing area, training is vital and needed to be considered as part of operational recommendation 5.

3.101 It was recognised in the PSNI that training appropriate to role was essential to effectively investigate cyber-dependent and enabled crime and to support the needs of victims, however it was the view of Inspectors that the training provided did not meet those needs.

Operational Recommendation 5

Before the end of 2017, the PSNI should complete a training needs analysis (TNA) for cyber crime, cognisant of the outcome of strategic recommendation 1, and that cyber crime training across all levels is reviewed against the TNA to identify and address training gaps.

Business and the wider Community

3.102 In addition to the responsibilities for investigating cyber crime and the associated digital forensics, the PSNI had committed significant effort and resources into the prevention and protection aspects in an attempt to increase awareness of cyber crime and internet safety.

3.103 Over and above the national initiatives that operated in Northern Ireland, for example, Get Safe Online, Cyber Essentials and CiSP, the OCTF Cyber Crime Sub Group and Cyber Crime Industry Group had representation from the business community and academia.

3.104 The D/Chief Inspector CCC chaired the OCTF Cyber Crime Industry Group to engage and share intelligence with the business sector. There were excellent links between the PSNI and business, academia and members of the public through public events, media releases and talks to raise awareness across Northern Ireland.

3.105 The Business Crime Co-ordination Group, chaired by the PSNI had justice agencies and business representation working to progress the Business Crime Action Plan, and as referred to in Chapter 2, elements of this related to cyber crime.

3.106 In addition to these the PSNI had engaged with a wide cross-section of groups and individuals across Northern Ireland to promote cyber crime awareness and prevention. It had been involved in a number of public events with other organisations in the cyber security field and most recently, the CCC was involved in events at shopping centres in Belfast, Lisburn and Londonderry/Derry to mark Get Safe Online Day in October 2016, which received good media coverage.

3.107 The PSNI was fully involved in many of the Government and industry initiatives, including the Scamwise NI partnership and the 'Little Book of Big Scams' was launched in November 2016 at Stormont.[123]

123 https://www.psni.police.uk/news/Latest-News/10112016-scamwise-launch/

3.108 There was comprehensive online information, advice and links to resources on the PSNI website in relation to cyber crime and internet security to protect businesses and individuals. It provided business fraud advice regarding: money laundering; proceeds of crime and asset seizure; employee and insider threats; and mandate fraud.[124]

3.109 There was also support for a number of self-help websites and online facilities for businesses and individuals including:

- Cyber Information Sharing Partnership (CiSP).[125]
  - CiSP members received cyber threat and vulnerability information. Since the launch of CiSP in March 2013, it had continued to grow with over 1,700 organisations and 4,400 individuals signed-up for this free service.[126] Inspectors understand that at the time of the inspection there were approximately 80 organisations which were members of CiSP in Northern Ireland.
- Cyber Essentials: provided businesses small and large, in all sectors, with clarity on good basic cyber security practice.[127]
- Get Safe Online: offered free advice for individuals and businesses on a comprehensive range of areas, for example, protecting yourself, your computer, your children and guidance in respect of shopping, banking and communicating safely online.[128]

3.110 A cyber crime portal on the PSNI website allowed businesses and individuals to report non-emergency cyber incidents to the police.[129]

3.111 CCC staff were also involved in a criminal diversion programme aimed at 15 to 17-year-olds. The scheme had three levels which were:

1. Cyber Choices education pack - parent-focussed and used at road shows and with community groups;
2. Cyber Centurions programme - to identify technically skilled individuals to develop in an academic environment and compete in nationally organised events; and
3. TEACH (Teaching Ethical Alternatives to Child Hackers) Programme an industry/academia-led initiative to divert young people from the criminal route at a one-day workshop to educate them on offences and the potential consequences of hacking.

3.112 The Ulster University and the PSNI had also launched 'Cybersafe'; a five week course to provide people with a better understanding of how to stay safe online.[130]

---

124 Mandate fraud is also known as Creditor Fraud, Payment Diversion Fraud and Supplier Account Takeover Fraud. This is where criminals change the account details for supplier or customer accounts in order to gain control and benefits from unauthorised payments. PSNI. https://www.psni.police.uk/crime/fraud/business-information/
125 Cyber Information Sharing Partnership. https://www.cert.gov.uk/cisp/
126 Cyber Information Sharing Partnership. https://www.cert.gov.uk/cisp/Cyber
127 Cyber Essentials. http://www.cyberstreetwise.com/cyberessentials/?&nginxId=00a723bf-b201-4414-c412-1bf6a3196d7d
128 Get Safe Online. https://www.getsafeonline.org/
129 https://www.psni.police.uk/crime/cyber-crime/
130 Chief Constable's report to the Northern Ireland Policing Board 3 March 2016.

3.113 The PSNI had initiated discussions with academia with a view to commencing a limited number of PhD internships, which would perform a similar function to the volunteer 'Cyber Specials' in England and Wales referred to in Chapter 2. This was at an early stage but Inspectors saw considerable merit in this, for both parties, and look forward to seeing how this progresses.

3.114 This work was vitally important, as public and business awareness was limited, and more needed to be done by the PSNI, and others, to raise awareness, encourage self-help, prevention and increase levels of reporting (see operational recommendation 6). However, this was a significant drain on the resources of the CCC and had to be balanced against the investigative and digital forensic demands on the unit.

3.115 The PSNI was not currently funded for the dedicated Cyber Protect officers[131] which operated in England and Wales. However the Justice Minister advised the Northern Ireland Assembly that a business case was being developed to enable funding to be provided under the National Cyber Security Programme.[132]

3.116 There had been regular press coverage and media releases, and a number of Districts had given out information locally through Facebook pages on various aspects of cyber crime and internet security.

3.117 At District level the PSNI had included elements of cyber crime, in particular internet safety, in its engagements with schools and young people as part of the Citizenship and Safety Education Programme.

3.118 One of the general functions of police was to prevent crime and this should be in the forefront of all officers' minds when dealing with reports of cyber-enabled crime, and more generally when in contact with businesses, individuals and vulnerable groups as part of their daily duties. However, as referred to previously, many of the officers that Inspectors spoke to were not confident about giving preventative advice about cyber crime and internet safety. There was a need for improved tailoring of support and advice to victims of digital crime and potential future victims. It would be the view of Inspectors that this should be examined as part of the training needs analysis referred to at operational recommendation 5.

3.119 Similarly, Crime Prevention Officers who were very confident and experienced at giving crime prevention advice to businesses and individuals about traditional and acquisitive crimes, were less sure about providing advice about cyber crime, and none of the Crime Prevention Officers who spoke to Inspectors had received specific cyber crime training.

3.120 The PSNI had invested time and resources to raise public awareness about cyber crime and internet security. Nevertheless, based on the level of cyber crime, the recognised under-reporting, and the widespread concern highlighted in the survey results (see Chapter 4), much more needed to be done across Northern Ireland to raise public awareness and encourage preventative measures and good internet safety. Whilst the PSNI needed to be involved, CJI did consider this to be solely a role for police (see operational recommendation 6).

131 The role of the Cyber Protect officers included *inter alia,* to deliver cyber security advice to the public and business community.
132 Northern Ireland Assembly. Written Answer. AQW 3305/16-21 Answered 16 September 2016.

Police and Community Safety Partnerships (PCSP)

3.121 The general functions of the NIPB included making arrangements for obtaining the co-operation of the public with the police in the prevention of crime.[133] As part of this the functions of a PCSP[134] included *inter alia*, to make arrangements for obtaining the cooperation of the public with the police and enhancing the community safety in the District. Seven of the PCSPs had undertaken initiatives to help educate children and young people about how to stay safe online.[135]

3.122 Inspectors were advised that four of the 2016-17 action plans from PCSPs submitted to the NIPB included plans to tackle cyber crime:

- Armagh, Banbridge and Craigavon - a schools engagement programme included cyber safety.
- Causeway Coast and Glens - a schools programme which included cyber safety.
- Fermanagh and Omagh – an awareness campaign about cyber crime for all ages to reduce the embarrassment of reporting.
- Mid and East Antrim – an agreement to contribute to cyber crime initiative with regional agencies and the PSNI.

3.123 Inspectors regard the PCSPs as having an important role at local level to provide education and awareness of cyber crime and the resources available to protect individuals and members of the business community as part of their community safety role, and this should be fully integrated into the Cyber Strategy for Northern Ireland.

---

133 Section 32 Police (Northern Ireland) Act 2000

134 The functions of a PCSP shall be -

(a) To provide views to a relevant district commander and to the Policing Board on any matter concerning the policing of the district;
(b) To monitor the performance of the police in carrying out—
(i) the policing plan in relation to the district; and
(ii) the local policing plan applying to the district or any part of the district;
(c) To make arrangements for obtaining the co-operation of the public with the police in preventing crime and enhancing community safety in the district;
(d) To make arrangements for obtaining the views of the public about matters concerning the policing of the district and enhancing community safety in the district and to consider fully any views so obtained;
(e) To act as a general forum for discussion and consultation on matters affecting the policing of the district and enhancing community safety in the district;
(f) To prepare plans for reducing crime and enhancing community safety in the district;
(g) To identify targets or other indicators by reference to which it can assess the extent to which those issues are addressed by action taken in accordance with any such plans;
(h) To provide any such financial or other support as it considers appropriate to persons involved in ventures designed to reduce crime or enhance community safety in the district.

References in this section to enhancing community safety in any district are to making the district one in which it is, and is perceived to be, safer to live and work, in particular by the reduction of actual and perceived levels of crime and other anti-social behaviour. Justice Act (Northern Ireland) 2011

135 Northern Ireland Assembly. Written Answer AQW 143/16-21. Answered 7 June 2016.

4 Outcomes

The Experience of Cyber Crime

4.1 The risk of becoming a victim of crime remained lower in Northern Ireland (8.8%) than in England and Wales (15.9%). These figures compare with 10.0% and 17.0% (respectively) in 2013-14. [136] Results from the 2014-15 Northern Ireland Crime Survey (NICS) estimated that 8.8% of all households and their adult occupants were victims of at least one NICS crime, this represented the lowest victimisation rate since the measure was first reported in 1998 (23.0%). However, it should be noted that the NICS excluded data relating to fraud.

4.2 In respect of cyber crime the circumstances were different, and as seen in earlier chapters:

- the PSNI assessed the vast majority of cyber crime is not reported;
- the cost of cyber crime to Northern Ireland was significant;
- almost one fifth of people here had been the victim of a scam in the last three years;
- cyber crime was a growth area in all sectors in Northern Ireland; and
- nine out of 10 large organisations had reported suffering a cyber breach and one in 10 people will be a victim of cyber crime.[137]

4.3 As a result, it was unsurprising that cyber crime survey information showed considerable concern among the public in Northern Ireland:

4.4 A report on public confidence on the policing of cyber crime by PSNI[138] found that:

- there was considerable concern amongst internet users about cyber crime;
- two thirds were concerned about identity theft or online fraud. Concern was also high in respect of fraudulent emails, encountering unsolicited material online and cyber-bullying;
- there were concerns about cyber crime when children were online;
- only one in four respondents were aware of any measures that the PSNI took to tackle cyber crime, although awareness of measures was slightly greater when those with no children under 18 were excluded;

136 Experience of Crime: Findings from the 2014/2015 Northern Ireland Crime Survey. DOJNI Analytical Services Group Research and Statistical Bulletin 8/2016. February 2016

137 https://www.psni.police.uk/news/Latest-News/2016-10-18-get-safe-online-day/

138 Public confidence in the policing of cyber crime. Summary report of findings. Millward Brown Ulster report to the Northern Ireland Policing Board. February 2014.

- most internet users took at least some measures to try and protect themselves from being a victim including only using trusted sites or having security software;
- educating the public about avoiding becoming a victim of cyber crime was most likely to be cited, especially by internet users and those with children under 18, on how the police should prioritise resources;
- almost 10% considered they had been a victim of cyber crime; of those just over 10% reported it to the police. Even fewer contacted the police, or other organisations, for advice;
- overall confidence in the police had the greatest impact on the likelihood of reporting cyber crime; and
- not believing the police could do anything, a perception that the crime was not serious enough, that it would be wasting police time, or that police wouldn't take it seriously, were the key reasons for non-reporting.

4.5 Cyber crime was one of the top five themes that arose in public meetings during the NIPB's consultation on Policing Plan priorities.[139]

4.6 A more recent survey found that 22% of people in Northern Ireland said they had a limited understanding of cyber crime, and the fear of cyber crime was significant: 94% said they were somewhat or very concerned about their online safety and security.[140] The survey also found that 50% of people who had been a victim of cyber crime thought it was too trivial to report, and 53% felt nothing could be done.

4.7 A scam reporting website; Scamwise NI, was launched in November 2016 and was visited 10,000 times in its first six weeks which the PSNI believed indicated the level of concern about the increasing number of ways criminals were trying to defraud the public.[141]

4.8 The Crime Survey for England and Wales had excluded fraud and computer misuse data. Questions about these offences were first included in the survey in October 2015, so full-year data will not be available until early 2017. Estimates of the scale however, were in the region of 5.6 million offences, which was a similar magnitude to the current headline figure covering all other criminal offences; when published crime figures will soar. Subsequent year-on-year comparisons will provide a more accurate picture of the trend over time, but the headlines associated with this apparent doubling of the crime rate are likely to further increase concern among businesses and the wider public about cyber crime.[142]

139 Northern Ireland Policing Board. Outcome of Public Consultations on Policing Plan Priorities. October 2015 http://www.nipolicingboard.org.uk/policing_priorities_consultation_report_2015.pdf
140 https://www.psni.police.uk/news/Latest-News/2016-10-18-get-safe-online-day/
141 http://www.belfasttelegraph.co.uk/news/northern-ireland/10000-visit-new-scam-reporting-website-in-first-six-weeks-35320834.html
142 https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2016#what-is-happening-to-trends-in-crime

4.9 In stakeholder meetings with Inspectors a number of business representatives had a very limited knowledge of the cyber threat or what businesses could do to help protect themselves. Many did not see cyber crime as a current priority for their business. Most however, recognised that cyber crime was a growing area and that they would have to do more in the future.

4.10 Inspectors were told by stakeholders that many victims of cyber crime and cyber-related fraud were unclear about the reporting arrangements. They wanted a clearer system for signposting to the appropriate investigative and support agencies. This theme was also evident in a recent business representative group report which made a recommendation to improve the effectiveness of the reporting channels for victims of cyber crime as well as the end-to-end response to cyber crime and fraud by UK law enforcement.[143]

4.11 The limited understanding of cyber crime referred to previously, and the uncertainty about reporting arrangements were also apparent in the timing of reports to the police. Inspectors heard of instances where reports of cyber-enabled crimes had been delayed, which limited the opportunities for police to take action or mitigate the victim's loss.

4.12 Inspectors were also advised during stakeholder consultation that some businesses were dissatisfied about the lack of feedback from police and Action Fraud on the progress and outcomes of investigations where cyber crime had been reported, and this was a disincentive for future reporting.

4.13 Earlier chapters of this report outlined the various measures taken at national and local level to raise awareness of cyber crime and internet security. It highlights the comprehensive online resources; the involvement of businesses, academia and PCSPs, together with the work that is being progressed through the OCTF and Business Crime Action Plan and the various measures and initiatives undertaken by the PSNI. However, despite all of these, there appears to be a disconnect with the outcomes not translating into a widespread public understanding of the threat from cyber crime, confidence in the policing of cyber crime, and the need for businesses and individuals to take increased responsibility for their own online security.

4.14 It was CJI's view that an approach was required that would extend beyond that which could be delivered by the police. The Cyber Strategy for Northern Ireland was the most appropriate vehicle to address cyber crime in a more strategic way.

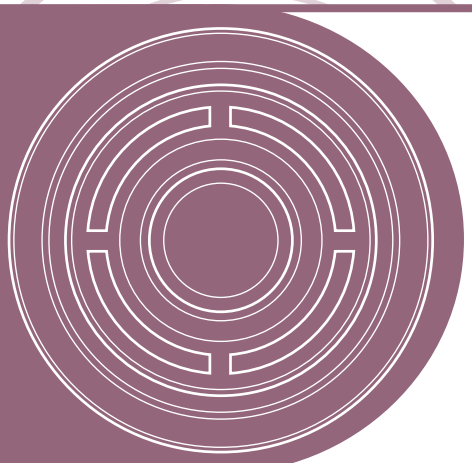
4.15 Inspectors understand that work to deliver the OCTF Cyber Strategy for Northern Ireland had initially been led by the PSNI until it became clear that the criminal justice system was only one element of the wider strategy. The launch of the National Cyber Security Strategy 2016-21 contextualised this further in terms of a wider strategic approach across all sectors.

143 Cyber Resilience: How to Protect Small Firms in the Digital Economy. Federation of Small Businesses. June 2016. http://www.fsb.org.uk/docs/default-source/fsb-org-uk/fsb-cyber-resilience-report-2016.pdf?sfvrsn=0

4.16 As a result, the core group who had been progressing the Strategy commissioned consultants to develop a draft Action Plan on behalf of the DOJ, Department of Finance and Department for Education to be published in partnership with the Department for the Economy and industry partners, Belfast City Council, Invest NI and the Centre for Secure Information Technologies (CSIT). CJI welcomes this wider strategic approach. At the time of writing Inspectors understand that the Action Plan will be produced in early 2017, with a high level report prepared for the draft Programme for Government consultation in late December 2016.

Operational recommendation 6

The DOJ, in consultation with the PSNI, should ensure that the Cyber Strategy for Northern Ireland contains a comprehensive approach to address public concern and to increase awareness and understanding of the public and business community in Northern Ireland about cyber crime and internet security.



Appendices

Appendix 1: Types of Cyber Crime

Cyber Crime is a broad term which includes, *inter alia*, the following offences:

Cyber-dependent

- Creation and spread of malware (intrusive software installed on a computer without consent) for financial gain
  - Viruses
  - Worms
  - Trojans or Trojan Horses (disguise themselves as a normal programme to trick users into downloading malware).
- Network intrusions and hacking for personal or industry data
  - Gather personal data or information of use to criminals
  - Deface websites
  - Be employed as part of a denial of service (DoS) or DDoS attack
  - Use of Structured Query Language (SQL)144 injections to manipulate data e.g. banking details.
- Distributed denial of service DDoS attacks to cause reputational damage for criminal purposes or terrorism (an attack against a website/network with the intention of making it unavailable to users, e.g. flooding with traffic).
- Ransomware (a type of malware that demands a ransom) Cryptolocker (a type of malware that encrypts data – can be used to demand a ransom).
- Malware (a virus introduced to a computer usually through phishing or spam. Once introduced can pass information to another device).
- Spam (unsolicited messages sent via the internet to large numbers of users, for the purposes of advertising, phishing, spreading malware).
- Botnets or Bots (a compromised controlled computer which involuntarily send messages simultaneously to a computer or server).
- Spyware (software that obtains covert information about another's computer activities by transmitting data covertly from their hard drive).
- Scareware (malicious computer programs designed to trick a user into buying and downloading unnecessary and potentially dangerous software, such as fake antivirus protection).
- 'Man in the middle' attacks – when communications are intercepted between parties and the criminal sends a communication which the targeted party believes is from the other party, e.g. for the transfer of funds.
- Adware (software which delivers advertisements or pop-ups can contain malware).

144 An SQL injection is a programming language designed for managing data. A cyber attack can execute malicious SQL Statements to control a web application's database server. This allows hackers to manipulate data. Organised Crime Task Force. Annual Report and Threat Assessment 2016. www.octf.gov.uk

Cyber-enabled

- Fraud.
- Purchase illegal materials/illegal market-places.
- Child sexual exploitation
  - Online grooming
  - Indecent images of children.
- Cyber bullying / harassment.
- Cyber hate crime.
- Phishing / Smishing / Vishing (emails / SMS messages / phone calls that mimic legitimate organisations to get the user to visit a bogus website or download malware).
- Spear-phishing / Whaling (deliberately selected targets for phishing / deliberately selected wealthy individuals).
- Trojan horse email (an email offering something interesting to the user but when open created security vulnerability).
- Virus-generated email.
- Revenge porn.
- Online stalking.
- Blackmail.
- Webcam blackmails.
- Serious and organised crime.
- Identity theft.
- Sexting (sending sexually explicit photographs or messages via a mobile phone).
- Pharming (the fraudulent practice of directing Internet users to a bogus website that mimics the appearance of a legitimate one, in order to obtain personal information such as passwords, account numbers).
- Online romance frauds / dating frauds (a confidence trick where feigned romantic intentions towards a victim, gaining their affection, are then used to commit fraud).
- Social engineering (a strategy for obtaining information not normally divulged by preying on natural curiosity/willingness to trust).
- Insider threat (disgruntled employee or targeted infiltration).
- Courier fraud (when the offender attends the victim's address to collect a credit card following a phone call / e mail purporting to come from a credit card company claiming that the victim's card has been compromised).

Appendix 2: Methodology

Methodology

The inspection will be based on the CJI Inspection Framework for each inspection that it conducts. The three main elements of the inspection framework are:

- Strategy and governance
- Delivery, and
- Outcomes.

Constants in each of the three framework elements and throughout each inspection are equality and fairness, together with standards and best practice. CJINI inspection methodology can be found at www.cjini.org.

Research and review

Collection and review of relevant documentation such as previous inspection and other reports, the PSNI and other CJA policies and procedures, management information, minutes of meetings and related documentation.

Inspectors carried out a series of engagements with stakeholders and criminal justice agencies. These included:

February 2016

- BCC/DOJ/PSNI Business Crime Event at Belfast City Hall
- Meeting with DOJ Head of Firearms Explosives and Organised Crime Branch
- Meeting with PSNI D/Superintendent C2 Specialist Investigation Unit

March 2016

- Meeting with Chair of NIA Justice Committee

April 2016

- Meeting with PPS Assistant Director Appeals and International Section
- Meeting with Hospitality Ulster
- Meeting with Security Manager Castle Court Shopping Centre Belfast
- Meeting with Belfast City Centre Management
- Meeting with NIPB Director of Policy

May 2016

- Meeting with Director of the Northern Ireland Retail Consortium
- Meeting with Northern Ireland Independent Retail Trade Association
- Meeting with Regional Executive, Retailers Against Crime
- Meeting with Head of Policy NICTS
- Meeting with Head of Security Ulster Bank / Royal Bank of Scotland
- Meeting with officials Department of Justice Community Safety Branch
- Meeting with officials Department of Justice Organised Crime Branch
- Meeting with Confederation of British Industry Northern Ireland

June 2016

- Meeting with Chief Executive Ulster Farmers' Union
- Meeting with Chief Executive Northern Ireland Chamber of Commerce and Industry
- Meeting with Chairman and Business Development Officer Ulster Federation of Credit Unions
- Meeting with PCSP Manager Newry, Mourne and Down District Council
- Meeting with Director and Press and Parliamentary Officer NI, Federation of Small Businesses
- Meeting with Regional Services Manager NFU Mutual

July 2016

- Meeting with Chief Superintendent PSNI Business Crime lead and other officers
- Meeting with Assistant Information Commissioner for Scotland and Northern Ireland
- Meeting with Head of Security at ASDA
- Meeting with PCSP Manager Armagh City, Banbridge and Craigavon Borough Council
- Meeting with PCSP Manager Fermanagh and Omagh District Council
- Meeting with PCSP Manager Derry City and Strabane District Council
- Meeting with Head of Security First Trust and Allied Irish Banks

September 2016

- Meeting with D/Superintendent Economic Crime Unit, PSNI
- Meeting with D/Chief Superintendent C2, PSNI
- Meeting with D/Chief Inspector Head of Crime Training, PSNI
- Focus Group Police Analysts, PSNI
- Meeting with D/Chief Inspector Cyber Crime Centre, PSNI
- Meeting with District Commander Ards and North Down

October 2016

- Meeting with District Command Team Derry City and Strabane
- Meeting with District Command Team Fermanagh and Omagh
- Focus Group DESU Sergeants
- Focus Group DESU Constables

- Meeting with Chief Inspector Belfast City District
- Meeting with Superintendent Belfast City District
- Focus Group Belfast City District LPT Constables
- Meeting with Superintendent Mid Ulster District
- Meeting with Chief Inspector Mid Ulster District
- Focus Group Inspectors Mid Ulster District
- Focus Group LPT Sergeants and Constables Mid Ulster District
- PSNI / Get Safe Online / Action Fraud / RAC / FSB / DOJ Cyber Crime Event in Belfast City Centre
- Meeting with Chief Inspector Foundation Training
- Focus Group Digital Forensic Officers PSNI CCC
- Focus Group Investigators PSNI CCC
- Meeting with D/Inspector PSNI CCC
- Meeting with D/Chief Superintendent C2
- Focus Group PSNI Crime Prevention Staff
- Meeting with Superintendent District Policing Command
- Meeting with D/Superintendent C2

November 2016

- Meeting with PPS Prosecutors, Central Casework Section
- Meeting with ACC Crime Operations
- Focus Group PPS Prosecutors Western and Southern Region
- Meeting D/Chief Inspector CCC
- Meeting D/Sgt Economic Crime Unit.
- Meeting Chief Superintendent PSNI Business Crime lead.
- Focus Group PPS Prosecutors Belfast and Eastern Region

Fieldwork

- Terms of reference will be prepared and shared with the PSNI and the other CJAs prior to the initiation of the inspection. Liaison officers from the CJAs should be nominated for the purposes of this inspection.
- PSNI as the primary organisation will be given the opportunity to complete a self-assessment of its approach to dealing with business and cyber crime and any management information deemed relevant.
- Interviews and focus groups will be conducted with the PSNI and other CJA staff, and relevant stakeholders to give an insight into the issues affecting business and cyber crime.
- Progress in the development of management information and performance management data will be examined.
- Evidence of planning and decision-making leading to performance improvement and recognition of future development will be gathered, and
- Where appropriate benchmarking and identification of best practice within and outside Northern Ireland.

Feedback and writing

Following completion of the fieldwork and analysis of data a draft report will be shared with PSNI and the other CJAs for factual accuracy check. The Chief Inspector will invite the PSNI and the other CJAs to complete an action plan within six weeks to address any recommendations. If the plan has been agreed and is available it will be published as part of the final inspection report. The inspection report will be shared, under embargo, in advance of the publication date with PSNI and the other CJAs.

Inspection publication and closure

- The final report is scheduled to be completed by December 2016.
- A report will be sent to the Minister of Justice for permission to publish.
- When permission is received the report will be finalised for publication.
- Any CJINI press release will be shared with PSNI and the other CJAs prior to publication and release, and
- A suitable publication date will be agreed and the report will be issued.

Appendix 3: Terms of Reference

CJINI Inspections

1. **Business Crime: an Inspection of how the Criminal Justice System deals with Business Crime in Northern Ireland**
2. **Cyber Crime: an Inspection of how the Criminal Justice System deals with Cyber Crime in Northern Ireland**

Terms of Reference

Introduction

Criminal Justice Inspection proposes to undertake inspections of how the Criminal Justice System (CJS) deals with business and cyber crime.

There are significant overlaps across the areas of business and cyber crime and Inspectors will take a combined approach for preliminary work and stakeholder consultation.

The inspection will focus on the three main elements of the CJINI inspection framework as they apply to business and cyber crime: these are strategy and governance, delivery and outcomes.

The main organisation to be inspected will be the Police Service of Northern Ireland as the core agency involved in the prevention and investigation of business and cyber crime. However, other areas of the CJS are central to the effective delivery of justice in these areas and the inspection will incorporate the Public Prosecution Service and the Northern Ireland Courts and Tribunals Service. This will include the overall CJS response to business and cyber crime including co-operation and partnership working.

The Inspections will not seek to repeat issues which arose in separate inspection work, for example on Serious and Organised Crime[145] and Child Sexual Exploitation,[146] but will, where appropriate, make reference to these. Cyber terrorism is outside the scope of the Cyber Crime Inspection.

145 Serious and Organised Crime: an Inspection on how the Criminal Justice System deals with Serious and Organised Crime in Northern Ireland. November 2014. CJINI.

146 Child Sexual Exploitation in Northern Ireland. A Report of the Independent Inquiry. 19 November 2014. http://www.cjini.org/CJNI/files/f0/f094f421-6ae0-4ebd-9cd7-aec04a2cbafa.pdf

Context

In mid 2015, the NPCC (National Police Chiefs' Council) agreed a definition for business crime. The definition is 'Any criminal offence that is committed against a person or property that is associated with the connection of that person or property to a business.' Business crime therefore encompasses a wide range of offences and crime types including rural and agri-crime, serious and organised crimes such as ATM thefts and tiger kidnappings, shoplifting and violence against retail staff, fraud and illegal trade. Clearly businesses are now also at major risk of being the victims of cyber crime.

The costs of business crime are widespread and include not only the financial costs to the business for physical losses, for example of goods or money, but also the potential impact on customer confidence, time spent engaging with the criminal justice process, increases in insurance premiums and loss of future income where the business is unable to provide a service to its customers or carry out its normal day-to-day activities.

The criminal justice system, and PSNI in particular, have a key role to play in preventing, detecting, investigating and prosecuting crimes against businesses and in working in partnership with the business community to offer crime prevention advice and support. Business crime was the subject of a stakeholder event at the Committee for Justice in May 2015 with a subsequent report and actions for the Department of Justice and PSNI. It is therefore an important issue for politicians, the media and communities.

The use of computers and information technology is a significant and increasing part of everyday life. Internet usage has increased dramatically: the internet was accessed every day, or almost every day, by 78% of adults (39.3 million) in Great Britain in 2015, compared to 35% (16.2 million) in 2006; social networking was used by 61% of adults; 76% of adults bought goods or services online; and 86% of households had internet access.[147]

Cyber crime is a growth area, it is an activity which offers anonymity and allows criminals to operate outside the jurisdiction, and this makes it substantially more difficult for the police to investigate and apprehend offenders.[148] Anti-virus providers generally conclude that security attacks globally are in the billions and levels are increasing.[149] Estimates of the cost to the economy of cyber crime vary but the sums are significant and increasing.

Experience of crime in general in Northern Ireland is low, but a report on public confidence in the policing of cyber crime by PSNI found that there was considerable concern amongst internet users about cyber crime including identity theft or online fraud. Concern was also high in respect of fraudulent emails, encountering unsolicited material on line and cyber bullying. Almost 10% considered they had been a victim of cyber crime, of those just over 10% reported it to the police.[150]

147 Internet Access – Households and individuals 2015. Statistical Bulletin. Office for National Statistics. 6 August 2015.
148 Real Lives, Real Crimes. A study of digital crime and policing. HMIC 2015
149 Cyber Crime: a review of the evidence. Research Report 75. Summary of key findings and implications. Home Office. October 2013
150 Public confidence in the policing of cyber crime. Summary report of findings. Millward Brown Ulster report to the Northern Ireland Policing Board. February 2014.

Aims of the Inspection

The aim of the inspection is to examine and assess arrangements for dealing with business and cyber crime across the criminal justice system in Northern Ireland, with specific emphasis on the PSNI.

The objectives of the inspection are to:

- Examine the effectiveness of organisational strategies with regard to business and cyber crime, including the approach to prevention and enforcement.
- Examine the response to business and cyber crime - how operational delivery is structured to meet the needs and expectations of stakeholders and victims. To determine effectiveness and potential areas for improvement.
- Examine and assess the outcomes of strategies and delivery mechanisms for business and cyber crime against targets and expectations.
- Examine management information and the performance of the justice agencies in addressing business and cyber crime.
- Examine how the above aspects of business and cyber crime arrangements are benchmarked against good practice.
- Other matters of significance as they arise during inspection will also be considered.

Methodology

The inspection will be based on the CJI Inspection Framework for each inspection that it conducts. The three main elements of the inspection framework are:

- Strategy and governance
- Delivery, and
- Outcomes.

Constants in each of the three framework elements and throughout each inspection are equality and fairness, together with standards and best practice. CJINI inspection methodology can be found at www.cjini.org

Research and review

Collection and review of relevant documentation such as previous inspection and other reports, the PSNI and other CJA policies and procedures, management information, minutes of meetings and related documentation.

Fieldwork

- Terms of reference will be prepared and shared with the PSNI and the other CJAs prior to the initiation of the inspection. Liaison officers from the CJAs should be nominated for the purposes of this inspection.
- PSNI as the primary organisation will be given the opportunity to complete a self-assessment of its approach to dealing with business and cyber crime and any management information deemed relevant.
- Interviews and focus groups will be conducted with the PSNI and other CJA staff, and relevant stakeholders to give an insight into the issues affecting business and cyber crime.
- Progress in the development of management information and performance management data will be examined.
- Evidence of planning and decision-making leading to performance improvement and recognition of future development will be gathered, and
- Where appropriate benchmarking and identification of best practice within and outside Northern Ireland.

Feedback and writing

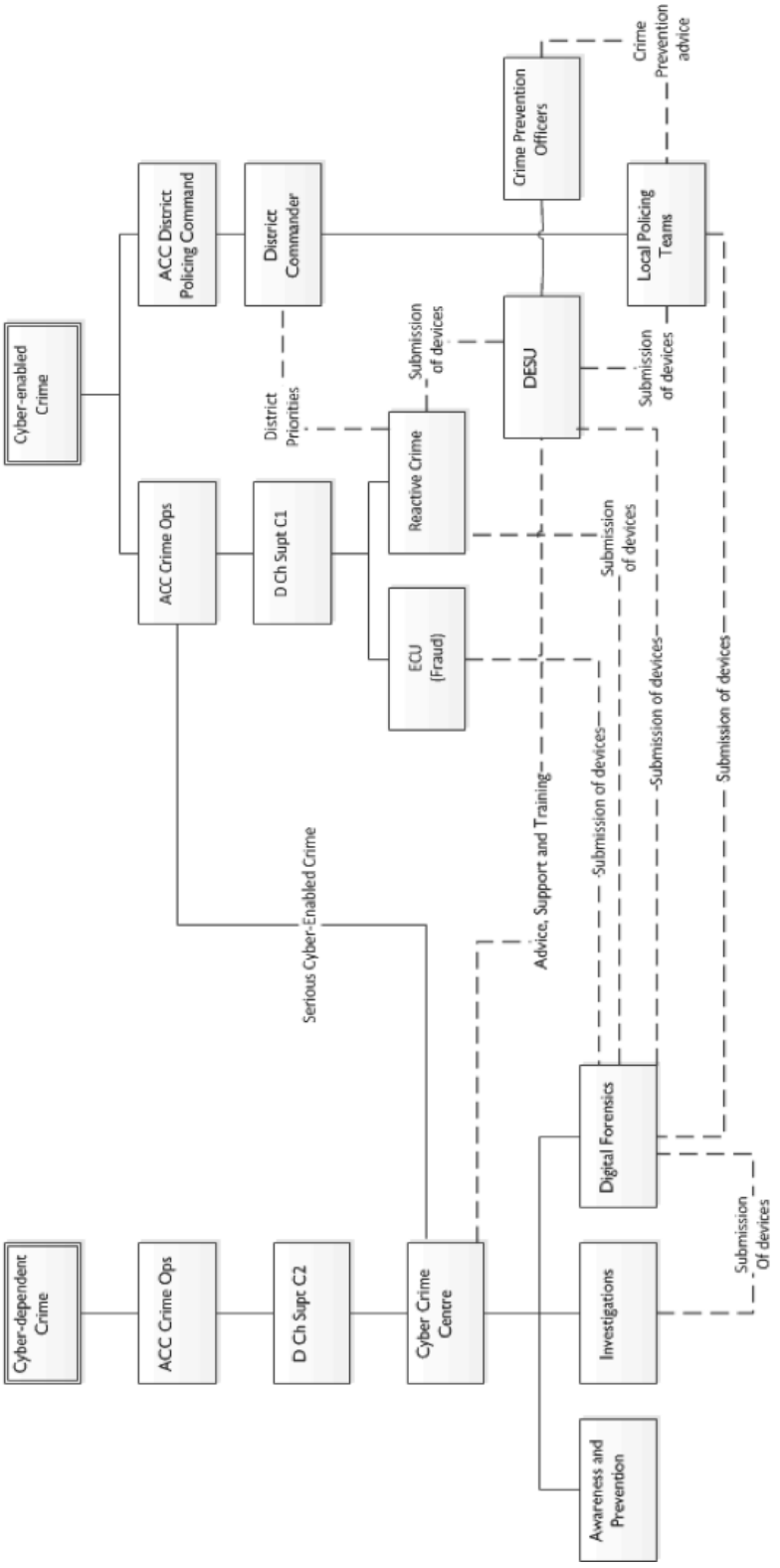
Following completion of the fieldwork and analysis of data a draft report will be shared with PSNI and the other CJAs for factual accuracy check. The Chief Inspector will invite the PSNI and the other CJAs to complete an action plan within six weeks to address any recommendations. If the plan has been agreed and is available it will be published as part of the final inspection report. The inspection report will be shared, under embargo, in advance of the publication date with the PSNI and the other CJAs.

Inspection publication and closure

- The final report is scheduled to be completed by December 2016;
- A report will be sent to the Minister of Justice for permission to publish;
- When permission is received the report will be finalised for publication;
- Any CJINI press release will be shared with the PSNI and the other CJAs prior to publication and release; and
- A suitable publication date will be agreed and the report will be issued.

Appendix 4

Investigation Pathways for Cyber Crime in PSNI



First published in Northern Ireland in June 2017 by
CRIMINAL JUSTICE INSPECTION NORTHERN IRELAND
Block 1, Knockview Buildings
Belfast BT4 3SJ
www.cjini.org