

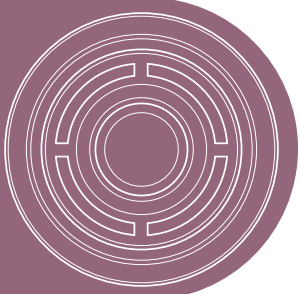


# CYBER CRIME:

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

June 2017





## **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



## Contents

List of abbreviations	4
Chief Inspector's Foreword	6
Executive Summary	8
Recommendation	10
<b>Inspection Report</b>	
Chapter 1: Introduction	12
Chapter 2: Strategy and governance	19
Chapter 3: Delivery	29
Chapter 4: Outcomes	52
<b>Appendices</b>	
Appendix 1: Types of Cyber Crime	57
Appendix 2: Methodology	59
Appendix 3: Terms of Reference	63
Appendix 4: Investigation Pathways for Cyber Crime in PSNI	67



## List of abbreviations

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

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

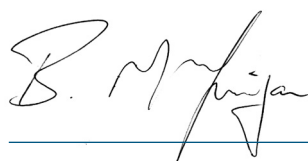
This report highlights the differences between cyber-enabled and cyber-dependant crime and outlines the response we should receive from the criminal justice agencies. Frontline police officers do need to know how to investigate cyber-enabled crime, such as where stolen goods are sold on-line or emails 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.*



Copyright© Criminal Justice Inspection Northern Ireland  
All rights reserved

First published in Northern Ireland in June 2017 by  
**CRIMINAL JUSTICE INSPECTION NORTHERN IRELAND**  
Block 1, Knockview Buildings  
Belfast BT4 3SJ  
[www.cjini.org](http://www.cjini.org)

