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

A FOLLOW-UP REVIEW OF RECOMMENDATION IMPLEMENTATION

NOVEMBER 2023

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

A FOLLOW-UP REVIEW OF RECOMMENDATION IMPLEMENTATION

November 2023

CONTENTS

LIST OF ABBREVIATIONS

ACC	Assistant Chief Constable
AI	Artificial Intelligence
CCTV	Closed Circuit Television
CJI	Criminal Justice Inspection Northern Ireland
DESU	Digital Evidence Support Unit (now known as Cyber Support Units)
DoF	Department of Finance
DoJ	Department of Justice
ICS	Information and Communications Services
ICT	Information Communications Technology
ISO	International Organisation for Standardisation
IT	Information Technology
m	Million
NCA	National Crime Agency
NFIB	National Fraud Intelligence Bureau
OCTF	Organised Crime Task Force
OSINT	Open-Source Intelligence
Police Service	Police Service of Northern Ireland (previously abbreviated as PSNI)
ROSIE	Researching, Open-Source, Internet and Email (now known as Open Source Intelligence (OSINT)
TNA	Training Needs Analysis
UK	United Kingdom

CHIEF INSPECTOR'S FOREWORD

Cyber crime is a complex, growing and constantly changing issue that the Police Service of Northern Ireland need adequate resources to deter, detect and investigate.

The rapid development of and current focus on Artificial Intelligence highlights the global opportunities and threats it presents and what it could mean for policing cyber crime in the future. All the more reason why the Police Service of Northern Ireland need effective organisational structures and the right people with the right skills as well as the technology and tools that support their response to cyber crime prevention, detection and investigation.

I am conscious that this Follow-Up Review took longer to complete than anticipated and that some of the recommendations have been superseded by the passage of time, developments across Government and technology. However, there are still improvements to be made to ensure the increasing need for analysis and investigation keeps pace with the dynamic environment and threats from ever advancing technologies and sources of threats.

Speeding up justice is a shared aim of the Criminal Justice Board and backlogs in analysing devices feeds into the narrative of forensics being a "catch all" reason for delay. This report unpacks some of that narrative.

I hope this Follow-Up Review report assists the Police Service of Northern Ireland and the Department of Justice in better tackling cyber crime in this jurisdiction and how service demand can be met more effectively in the future.

I am grateful to the Police Service of Northern Ireland and Department of Justice officials for their assistance during this Follow-Up Review.

My thanks also to David MacAnulty, Lead Inspector, and Inspector Muireann Bohill.

Jacqui Durkin
Chief Inspector of Criminal Justice in Northern Ireland
November 2023

Criminal Justice Inspection Northern Ireland
a better justice system for all

CHAPTER 1: INTRODUCTION

BACKGROUND TO THE FOLLOW-UP REVIEW

In June 2017, Criminal Justice Inspection Northern Ireland (CJI) published an inspection report on *How the criminal justice system deals with cyber crime in Northern Ireland* (the 2017 Inspection Report).[1] The Inspection Report made one strategic recommendation and six operational recommendations that were addressed primarily to the Police Service of Northern Ireland (the Police Service), one was addressed jointly to the Department of Justice (DoJ) and the Police Service.

This Follow-Up Review was originally scheduled in the *2020-21 Inspection and Follow-up Review Programme*, however, it was rescheduled following Ministerial requests for Reviews and resource issues. This allowed the Police Service more time to progress recommendations and an opportunity to assess if the intentions of the recommendations had been achieved over this time. However, it also meant that there had been significant developments in the area of cyber crime that could impact on the accepted 2017 Inspection Report recommendations.

Context and Developments since 2017

Cyber crime affects organisations, essential services, businesses and individual citizens. It has become a more common element of criminality. Cyber criminals identify weaknesses in individual or business security to steal passwords, money and data. Common cyber threats include:

- Hacking - including of social media and email passwords;
- Phishing - bogus emails asking for security information and personal details;
- Malicious software – including ransomware through which criminals hijack files and hold them for ransom; and
- Distributed Denial of Service (known as DDoS) attacks against websites – often accompanied by extortion.

Cyber crime has continued to grow in scale and complexity since the 2017 Inspection. At the time of writing (2023) there was an estimated cost to the United Kingdom (UK) of billions of pounds which did not account for the significant personal damage to individual victims. It was reported that overall fraud which included cyber crime accounted for 40% of all offences in England and Wales.[2]

1 CJI, An Inspection of how the Criminal Justice System deals with Cyber Crime in Northern Ireland, June 2017 available at https://www.cjini.org/TheInspections/Inspection-Reports/2017/April-June/Cyber-Crime.

2 Office for National Statistics, Crime in England and Wales, April 2023 available at https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables.

There have been well publicised cyber-attacks on high profile organisations such as the National Health Service *WannaCry* cyber-attack[3] which demonstrated that no area of society is immune from attack. An initial estimated loss of £20 million(m) was followed by a cost of £72m from the Information Technology (IT) requirements to restore data and systems. Critically, 19,000 medical appointments were cancelled over a one-week period. BBC News also reported on cyber crime[4] that in 2022 in the UK, ransomware groups extorted more than £370m ($457m) which was a significant $311m reduction from 2021 however, the number of attacks was on the rise. A more recent attack on Capita Group, which runs services for the National Health Service, councils and military, estimated a cost of £25m[5].

In September 2022, the Northern Ireland Safe Community Survey[6] reported that in 2019-20, 15% of people surveyed had been the victim of cyber crime with a further 19% having experienced an attempt against them. The most common type of cyber crime experienced by victims was online banking misuse, which made up 54%.

There are other serious crimes which are cyber-enabled such as child abuse, other types of sexual offending and online abuse which highlighted the need for a significant investment by the Police Service to deal with all cyber crime. There have been more pressures on Police Officers than ever to consider digital evidence when investigating crimes with digital evidence becoming a key element in many investigations. This has increased the demand on forensic examination of mobile and other digital devices.

Police Service Cyber Crime Structure

Cyber crime overall was under the control of the Assistant Chief Constable (ACC) for Crime. Diagram 1 was provided by the Police Service to show the structures and teams under the overall control of the ACC that dealt with cyber crime.

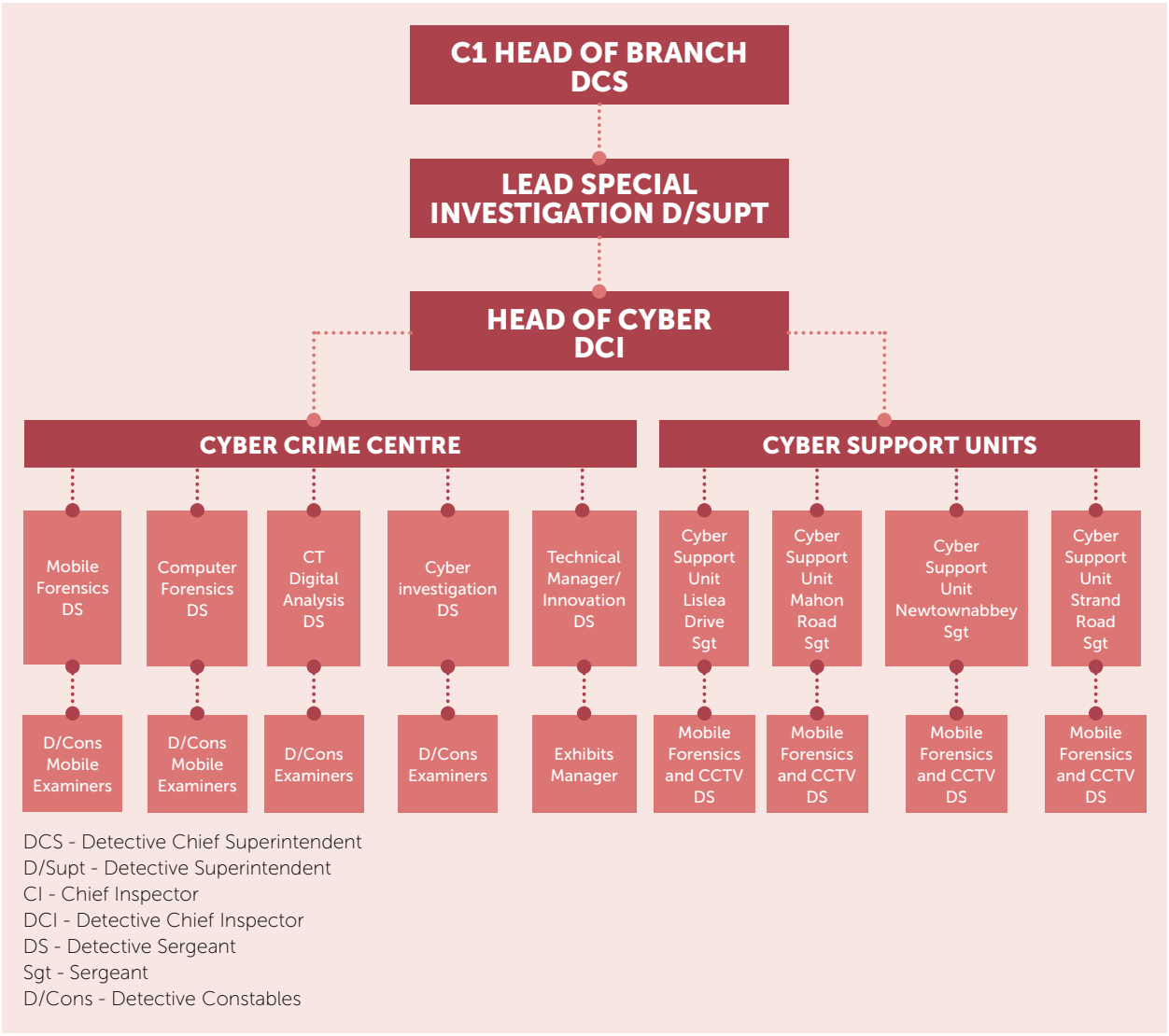
3 National Health Executive, October 2018 available at https://www.nationalhealthexecutive.com/articles/wannacry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-were-cancelled.

4 BBC News, Cyber-crime gangs' earnings slide as victims refuse to pay, 19.1.2023 available at https://www.bbc.co.uk/news/technology-64323980.

5 The Guardian, Cyber-attack to cost outsourcing firm Capita up to £25m, 4.8.2023 available at https://www.theguardian.com/business/2023/aug/04/cyber-attack-to-cost-outsourcing-firm-capita-up-to-25m#:~:text=Capita%20confirmed%20on%20Friday%20that,taken%20to%20secure%20the%20data.

6 DoJ, Cyber Crime: Findings from the 2019/20 Northern Ireland Safe Community Survey, September 2022 available at https://www.justice-ni.gov.uk/sites/default/files/publications/justice/cyber%20crime%20findings%20from%20the%202019%20NISCS.PDF.

Diagram 1: Cyber Crime Organisational Structure in the Police Service



DCS - Detective Chief Superintendent
D/Supt - Detective Superintendent
CI - Chief Inspector
DCI - Detective Chief Inspector
DS - Detective Sergeant
Sgt - Sergeant
D/Cons - Detective Constables

Cyber crime was considered by the Police Service as a wide term to describe two main sections; cyber dependant crime and cyber enabled crime.

- ***Cyber dependant crimes*** were those that can only be committed using a computer, computer networks or other forms of information communications technology (ICT). Examples of these include developing malware (computer software) for financial gains, hacking into other computers or networks to steal, damage or destroy data or computer systems. Investigations into cyber dependant crime was carried out by the Cyber Crime Team based at the new Cyber Crime Centre that also dealt with other significant areas such as online fraud.
- ***Cyber enabled crimes*** were traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other ICT. These included malicious communications, cyber bullying and indecent images. Most of the work involved the analysis of mobile telephones (phones) and Closed Circuit Television (CCTV) which was carried out by Cyber Support Units which replaced Digital Evidence Support Units (DESUs).

The strategic position of cyber crime within the Police Service was under review at the time of this Follow-Up Review. The Cyber Crime Team was moved to the control of Serious Crime Branch (known as C2) and subsequently moved, after Follow-Up Review fieldwork, to the Organised Crime Branch (known as C1). This would predominately involve cyber crime investigations. Inspectors were advised that future alignment with the Scientific Support Branch remained under consideration.

There were four Cyber Support Units that, as part of the Cyber Crime Centre, service both mobile phone digital examinations and CCTV for the organisation. The Cyber Support Units were located in Lislea Drive, Newtownabbey, Strand Road (L'derry/Derry) and Mahon Road (Portadown). A concern was raised by those interviewed in the Police Service that the cyber crime structures within the Police Service needed to be clearer and it was hoped that the ongoing internal review would resolve this.

Table 1 gives a breakdown of requests over the last three years made to both areas of the Cyber Crime Team and the Cyber Support Units. The Cyber Crime Team provided computer and mobile device services and the Cyber Support Units provide mobile and CCTV services. There were no records available for 2020 for items completed in Cyber Support Units.

Table 1: Numbers of requests for evidence retrieval made to (in) and processed (out) by the Cyber Crime Team and to Cyber Support Units 2020-22.[7]

	2020				2021				2022			
	Cyber Crime Team		Cyber Support Units		Cyber Crime Team		Cyber Support Units		Cyber Crime Team		Cyber Support Units	
	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out
Computers	931	1026			657	895			553	550		
Mobiles	218	393	4667		194	276	4021	1541	119	153	3070	1490
CCTV			11904				13009	13243			15447	14708

It was suggested by the Cyber Crime Team the 'numbers out'/those that have been completed in Cyber Support Units would closely match the numbers submitted as it was considered that the Cyber Support Unit had comparatively low operational queues. Table 1 above evidences that there was a significant number of requests for mobile phone analysis not being processed. The performance level was well below the Cyber Crime Team. One of the reasons cited was staffing issues in the Lislea Drive Cyber Support Unit. This evidence supported the anecdotal views from Court users that backlogs in device examinations were causing delays at Courts. Table 1 also reflects the steady increase in the number of requests being made for CCTV analysis, but both computer and mobile phone requests were reducing year on year.

7 Received from the Police Service June 2023.

The Follow-Up Review

This Follow-Up Review required the Police Service Cyber Crime Team to conduct a self-assessment outlining progress against recommendations made in the 2017 report. The Inspection Team considered this update provided by the Police Service and interviewed Police Officers and staff from across the area of cyber crime. Inspectors also attended a number of local Cyber Crime Team locations. In assessing whether recommendations were achieved, partially achieved or not achieved, Inspectors took cognisance of the fact that the landscape of how cyber crime was dealt with had changed significantly since the recommendations were made in 2017. The Inspection Team also considered whether the recommendations had been superseded by new practices and systems.

CHAPTER 2: PROGRESS AGAINST RECOMMENDATIONS

STRATEGIC RECOMMENDATION **1**

The Police Service 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).

Status: Not Achieved.

Organisational response

- *Police Service cyber crime have officers trained in the analysis and tracking of crypto currencies, and block chain in general, and can be tasked by investigation teams. Officers trained in Chainalysis reactor within Cyber Crime Centre.*
- *A Superintendent is leading on the Police Service's response to cloud computing. cyber crime have the technology to obtain cloud data once legislation supports this.*
- *Darknet progress has been made to capture evidential product from the Darknet.*
- *Two Cyber crime Officers are trained and have licences for Chainalysis (analysis tool to analysis crypto currency wallets and their origin with built in intelligence capability). Five further officers to be trained in 2023 (if budget permits). Licences were provided by the NCA (Cyber Unit).*

Response received at Factual Accuracy Check stage:

- *A Strategic Assessment of cybercrime is regularly completed as part of the annual Strategic Assessment on Serious and Organised Crime, as well as the Annual Threat Assessment for the Organised Crime Task Force.*
- *PSNI refers and contributes to both local and national assessments. Specifically supplied with this response are the National Fraud and Economic Crime assessment from City of London Police who hold that portfolio and the latest Organised Crime Task Force assessment which PSNI cyber provided relevant input for.*

Inspectors' assessment

As discussed at the outset of this Follow-Up Review, there had been significant strategic changes and developments since CJI's last inspection. There were a number of cyber crime related strategies as outlined in the following paragraphs.

A Department of Finance (DoF) strategic approach on cyber crime had been developed since the 2017 Report. A new Northern Ireland Cyber Security Centre, an agency of the DoF, had been established. It had a prominent role in the delivery of the UK Government Cyber Security Strategy 2022-2030 and was an advocate for cyber security in Northern Ireland. The Cyber Security Centre aimed to work with public, private and third sector organisations to improve their ability to defend against cyber-attacks, increase their knowledge of cyber threats, and become more cyber resilient. The Northern Ireland Cyber Security Centre formed part of the overall UK cyber response to incoming threats and attacks.

The DoJ indicated that the remit of the Organised Crime Task Force Cyber Engagement Group needed to be reviewed. This Group contributed to the delivery of the Northern Ireland Organised Crime Strategy 2021-2024,[8] however, the Inspection Team were told by DoJ officials that there was cross-over with other groups/organisations and that a review of this subgroup was needed as part of a wider amalgamation of all cyber crime strategic approaches.

The Home Office had established a Policing Cyber Resilience Leadership Board of which the Police Service and the DoJ were members. They had met once at the time of writing and another meeting was scheduled in September 2023. The purpose of this Leadership Board was to identify gaps and overlaps between approaches. There was also a UK Cyber Security Treaty being developed by the Home Office. The DoJ was engaging on this and worked with senior members of the Police Service Cyber Crime Team to ensure Northern Ireland was appropriately considered and reflected. The Home Office was also engaged with the DoJ following a consultation on the Computer Misuse Act 1990. A senior member of the Cyber Crime Team was to be included in discussions around the practical application of this legislation in Northern Ireland.

In relation to the specific requirements of the recommendation, a Strategic Assessment of Cyber Crime was produced by the Police Service in 2017, one month after CJI report publication. Several areas raised in the report were not referred to, for example it did not contain sufficient data, trends and statistics. It provided little assessment of the potential future demand on the Police Service. There was insufficient reference to aspects of vulnerability with a focus on the age of victims. The strategic positioning of cyber crime in the Police Service had significantly changed since 2017.

Inspectors recognised that the Police Service corporately and the Cyber Crime Team had a role to play in the wider cyber crime threat across the UK as outlined comprehensively in the National Fraud Intelligence Bureau, Fraud and Cybercrime Annual Assessment 2022-23 conducted by the City of London Police. The Inspection Team also acknowledged the key role that the Police Service played in the wider Organised Crime Task Force, in which cyber crime was one of the key elements.

8 *OCTF, Organised Crime Strategy Northern Ireland 2021-24, March 2021* available at https://www.octf.gov.uk/files/octf/2022-02/organised-crime-strategy-2021-24_0.pdf.

As outlined above, cyber crime within the Police Service was under review at the time of this Follow-Up Review. The Cyber Crime Team was moved to the control of Serious Crime Branch C2 and subsequent to Follow-Up Review fieldwork moved to the Organised Crime Department C1. This would predominately involve cyber crime investigations. During fieldwork, the location of where the remainder of cyber-enabled crimes such as the use of mobile phones and computers to commit offences was under review.

It was clear from those interviewed that there were internal Police Service procedures in place regarding the performance of evidence retrieval from devices. For example, monitoring backlogs of evidence retrieval was being reported at weekly and monthly meetings. Performance varied from team to team with some of those interviewed aware of backlogs of a year and another team in a different location felt that they were on top of requests and were processing them within several weeks.

Some of the rationale for the differences provided to the Inspection Team included a problem with resources and staff retention, for example, having received a high level of training, some staff were being attracted by the private sector which offered higher salaries. Inspectors heard many examples of how viewing indecent images in particular caused a toll on their mental wellbeing, and this was also a factor in staff retention and sick absences. CJI have considered wellbeing in greater depth in the 2023 *Leadership and Wellbeing Support* Inspection[9]. The management team accepted that overall, the area of cyber crime was somewhat protected financially compared to other policing areas, but there was a lack of awareness as to how the cyber crime area was to be strategically restructured again in 2023 and how that would impact on the levels of work output.

The Inspection Team recognised that the entire area of cyber crime had moved on significantly since 2017. Cyber crime was evolving at an ever-increasing rate and becoming more complex. This had placed financial demands on the Police Service to develop technology and training to keep pace with this ever-changing landscape. It was clear that the intentions of the original recommendation were not met. The anticipated strategic changes within the Police Service around cyber crime structures and organisation should be used as an opportunity to readdress the concerns raised in this recommendation. The intent of this strategic recommendation, particularly around the areas of strategic realignment for the various cyber crime approaches above, demand modelling and better understanding future demand on the Police Service remains an area of concern for the Inspection Team.

This recommendation is assessed as **Not Achieved.**

9 *CJI, Leadership development and wellbeing support within the criminal justice system in NI 28.2.23* available at ***https://www.cjini.org/TheInspections/Inspection-Reports/2023/Jan-Mar/Leadership-development-and-wellbeing-support-withi.***

OPERATIONAL RECOMMENDATION **1**
The Police Service 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[10];** • **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.**
Status: Not achieved.

Organisational response

The Police Service cyber crime has an establishment of approximately 100 officers to service the digital forensic demand – this is separated between cyber crime and Cyber Support Units.

- *NUIX is in use and allows officers to more readily review data extracted from seized computer devices. NUIX is utilised to allow reviewing of product from computer examinations, however current infrastructure limits the review locations within the police estate. Work is ongoing to address this.*
- *Budget constraints have inhibited the progress of automation and NUIX review capabilities, however the Police Service cyber team currently scoping this with Information and Communications Services (ICS). There are multiple barriers, such as linking to the Police Service digital strategy, and competing demands for ICS resource, and limited revenue funding.*
- *The Cyber Network is now available across the Police Service estate and is ripe for expansion of NUIX capabilities. Between 10.03.20 – 29.06.23, a total of 1169 individual cases have been examined by the Cyber Crime Centre (each of which with varying numbers of individual exhibits), 376 of these cases have utilised NUIX for review.*
- *All Digital forensic officers are police officers.*
- *Police Service cyber support officers are available to attend scenes when needed and provide training regarding on-site capabilities to better inform the gathering of evidence.*
- *Cyber enabled fraud is the remit of the Economic Crime Unit and other departments.*

10 An IT company software platform for indexing, searching, analysing and extracting digital information.

Inspectors' assessment

The area of cyber crime had not been significantly impacted by budget cuts despite reported Police Service financial pressures outlining a funding gap of £141m[11]. The four Cyber Support Units had been developed and in use since the 2017 CJI Inspection Report. For example, the Cyber Crime Team were able to recruit for staff vacancies except for the Cyber Support Unit at Lislea Drive. Demand was increasing as shown earlier in this Follow-Up Review and becoming more complex and changing in nature.

Criminals did not have the same constraints as faced by the Police Service and were able to improvise, change and develop quickly when needed. The Inspection Team heard from those interviewed that they were constantly challenged by new technologies which required a Police Service response, for example in new training or new software or hardware. This may become problematic given the reported ongoing financial pressures on the Police Service budget. The Lislea Drive area office had been impacted by long term absences which were still ongoing at the time of writing and had contributed to a year-long backlog in requests for device reviews. Some parts of the Cyber Crime Team were able to meet demands however, the backlogs of requests from Lislea Drive being sent to other areas had an overall negative impact on the Cyber Crime Team's ability to deal with the long backlog of cases. For example, Inspectors were told that items submitted in May 2022 were only being reached in May 2023. Inspectors were told that data was being routinely used in Cyber Governance meetings however, there remained gaps in how management information was being used to deal with the numbers of backlog cases, time taken and the demands placed on the various Cyber Crime Centre teams and Cyber Support Units.

Another aspect of this operational recommendation was the role out of NUIX software to support Investigators by taking complex systems and data and making it easy to understand. NUIX was considered to be well established and used at the time of the Follow-Up Review, however there remained challenges in future development of Artificial Intelligence (AI) automation as this required further investment. The roll out of NUIX as required in the recommendation, was described as ongoing. External resourcing had caused general issues with forensic teams sending items to England for examination but having difficulty getting examiners to attend Court for case hearings. This had proved too time consuming and costly and was being phased out.

Civilianisation (civilian police staff working alongside Police Officers) was being considered as part of a possible blended approach between the Scientific Support Branch and Cyber Teams for the purposes of International Organisation for Standardisation (ISO) accreditation at the time of fieldwork for the Follow-Up Review however, a wider roll out of civilianisation was still under consideration for the future. The approach was broadly welcomed by those interviewed but there were a lot of unknowns around how it would be established, strategically led and resourced. This part of the recommendation was considered not achieved.

11 *BBC News, Police Service budget could become impossible to manage, says Chief Constable, 4 May 2023* available at ***https://www.bbc.co.uk/news/uk-northern-ireland-65483888.***

Training and awareness also remained a problem. Online intranet guides were available to Officers for example on how to use Faraday bags[12]. Those interviewed voiced ongoing concerns that too much was being asked with blanket requests for unknown evidence on devices. For example, Inspectors were told a mobile phone would be submitted requesting evidence, which was sometimes vague and wasted an inordinate amount of time. It was suggested that there should be compulsory Continuous Professional Development for front-line Police Officers to maintain up-to-date awareness. This aspect of the recommendation was considered not achieved.

Even though the new Cyber Crime Centre and establishment of Cyber Support Units demonstrated that this area had moved-on since the 2017 Inspection Report, the levels of demand continued to present problems. As outlined previously in the Organisational Response above, Inspectors were advised at a late stage of report development that strategic assessments of cyber crime were regularly completed as part of the annual Strategic Assessment on Serious and Organised Crime, as well as the Annual Threat Assessment for the Organised Crime Task Force. However, Inspectors were not provided with a copy of these assessments and there was not a specific cyber crime up-to-date strategic assessment since the one provided in 2017. Training, awareness, the use of automation and the availability of NUIX had not been sufficiently developed as expected.

Overall, this operational recommendation was considered **Not Achieved.**

OPERATIONAL RECOMMENDATION **2**
Approaching two years from the transfer to Action Fraud it would be appropriate for the Police Service 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.
Status: Achieved.

Organisational response

No response received.

Inspectors' assessment

The Police Service produced a report in July 2018 which made 12 recommendations. It recommended that the Police Service should:

1. *Initiate high level contact with Action Fraud/The National Fraud Intelligence Bureau (NFIB) to communicate the current challenges being experienced by the Police Service as a result of Action Fraud membership and seek solutions.*
2. *Seek a confirmed date from Action Fraud for the introduction of the online reporting tool.*

12 A specially designed bag to prevent the loss of electronic information on a device.

3. *Request NFIB provide victim reports on a weekly basis to allow any non-compliance issues to be identified and addressed as a priority.*
4. *Recommence recording of all fraud offences and outcomes locally.*
5. *Take steps to improve officer and staff knowledge on the role of Action Fraud.*
6. *Monitor service performance in respect of recorded frauds using Saturn*[13].
7. *Continue to utilise the NFIB reporting codes on Niche Records Management to allow for improved understanding of fraud types and assist in reporting to NFIB.*
8. *Appoint an Analyst with responsibility for improving Police Service knowledge of fraud impacting Northern Ireland.*
9. *Explore the concept of establishing an end-to-end management process for fraud investigation within their organisation, with a view to improving investigative outcomes and reducing re-victimisation.*
10. *Consider whether a survey of older people or people with a disability should be conducted to ascertain whether the Action Fraud service is truly accessible to these groups.*
11. *Initiate high level contact with the Public Prosecution Service and Courts Service to examine the feasibility of prosecuting fraud offences committed outside the jurisdiction.*
12. *The Police Service Executive Team should consider whether the Police Service membership of Action Fraud is beneficial and whether it represents value for money.*

The cyber crime reporting system Action Fraud was to be replaced, as set out in the UK Government Fraud Strategy.[14] This policy paper indicated that Action Fraud was to be replaced with a state-of-the-art system for victims to report fraud and cyber crimes to the Police service. It also highlighted that reviews of Action Fraud repeatedly identified shortcomings and there was a commitment to spend £30m across three years to replace Action Fraud with a completely new service.

Fraud and related cyber crime incidents in Northern Ireland were generally still reported to Action Fraud or to the Police Service. Northern Ireland had an established '*Scamwise NI Partnership*', which was chaired by the Police Service, which brought together over 45 organisations to combat the threat of fraud. The partnership had awareness campaigns to inform the community about the risk and range of scams, and information sharing between organisations. As discussed previously, the Inspection Team were concerned that there was overlap between this work and that of the DoF Cyber Security Centre.

The Police Service were still following the national approach and those interviewed were aware that victims should be directed towards Action Fraud. It was clear that this was no longer a valid approach given the significant issues raised against Action Fraud and the changing system at a UK national level. When considering this recommendation, the Police Service had reviewed Action Fraud and the recommendation was technically achieved but, developments since 2017 have rendered this recommendation no longer applicable and the significant failings of Action Fraud and its replacement will need to be reviewed in any future CJI full inspection.

13 Saturn is a Police Service internal Management Information System.
14 UK Government *policy paper: Fraud Strategy: stopping scams and protecting the public, May 2023* available at https://www.gov.uk/government/publications/fraud-strategy/fraud-strategy-stopping-scams-and-protecting-the-public.

This recommendation is assessed as technically **Achieved.**

OPERATIONAL RECOMMENDATION **3**
The Police Service should review online access for first response Officers with a view to either extending ROSIE[15] 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.
Status: Not achieved.

Organisational response

ROSIE, which is now referred to as Open Source Intelligence (OSINT), is no longer the remit of Cyber Crime Centre. ICS are currently implementing technology to allow open source viewing on common terminal within the police estates.

Inspectors' assessment

ROSIE was considered by the Cyber Crime Team an antiquated term, and was no longer used. OSINT was being used at the time of review. The majority of Officers in Cyber Support Units were trained to use the system regardless of the terminology. Inspectors were told that front-line Police Officers still faced significant issues regarding access to this information which meant making requests of trained Officers. The process for getting information from open-source websites could be done by district intelligence. This should in theory, have managed demand away from Cyber Support Units and Cyber Crime Teams however, Inspectors heard that there were still too many open-ended requests for evidence retrieval from devices still being made.

The increasing use of ever-advancing technology in devices along with an increasing degree of complexity meant that it was unlikely that the Police Service would be able to fund open-ended specialist training for this area. Raising awareness amongst operational Police Officers may help in this regard but without continuing and increasing requests being made.

This operational recommendation was **Not Achieved.**

15 Research, Open-source, Internet and E-mail.

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.**
Status: Achieved.

Organisational response

DESU's are no longer in existence. Four Cyber Support Units are located throughout the province, who as part of Cyber Crime Centre, service both mobile phone digital examinations, and CCTV for the organisation. The Cyber Support Units are located in Lislea Drive, Newtownabbey, Strand Road and Mahon Road. Their capability to examine mobile phones continues to increase, and are now closely aligned to the capabilities of the Cyber Crime Centre. A considerable investment of technology and training has been made since 2020, therefore increasing the overall capability of the Police Service to meet the demand of digital forensic. CSU [Cyber support Unit] officers now produce work to an evidential standard, and produce evidence for court. CCTV recovery and processes is now owned by the Cyber Crime Centre, and supported by ICT Level 2 staff members, in conjunction with Police Officers.

Inspectors' assessment

DESUs had become Cyber Support Units. Inspectors spoke with a range of Police Officers and staff members across these Units who were positive about their working conditions and their ability to deal with the levels of backlogs. Some teams reported that they were 'sheltered' by their managers from the pressures of backlogs. The exception was Lislea Drive which, Inspectors were told, had seen no improvements overall in backlogs and staff morale was low.

As discussed at strategic recommendation 1 above, there were considerations of whether to amalgamate elements of the Cyber Crime Team with the Scientific Support Branch which would mean civilianisation, at least in part, would be inevitable. Agreement had been reached for Cyber Support Unit Officers to give evidence in the Crown Court.

Staffing levels and caseloads (as discussed earlier in this report) remained a concern and the future demand model still needed to be addressed, however Inspectors reflected that this recommendation could be considered ✅ **Achieved** as Cyber Support Units were well established.

OPERATIONAL RECOMMENDATION **5**

Before the end of 2017, the Police Service 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.

Status: Partially Achieved.

Organisational response

TNA has been designed and implemented for all work streams within Cyber Crime Centre. There is now a Staff Training Competence and Development Committee to provide cost effective and deliverable training. This allows the ability to track staff development and provides oversight of performance. The TNA was initially drafted in 2018, and is currently being revised align with ISO 17025 (external quality standards).

Inspectors' assessment

Following this recommendation, a TNA had been completed for Cyber Crime Centre staff. The College of Policing had developed a high-level curriculum for front line Officers that was designed to bridge the gap between the front-line Officers and those within the Cyber Crime Team. However, this had yet to be implemented due to limited resources and challenges in providing digital trainers to explain the new investigative opportunities.

Training was described as 'good' to the Inspection Team during this Follow-Up Review. All of those within the Cyber Crime Centre interviewed had received comprehensive training with a caveat that new programmes were difficult to get because of pressures on Police Service resources. The Cyber Crime Centre team made 'bids' along with every other Police Service area, which may mean problems in future training. For example, Inspectors were advised that the required training budget was around £250,000 and they had received £8,000.

Training for front line Officers was available, but Inspectors were told that too many requests were still being made to examine devices, for example, without sufficient detail of what was being sought. This was a significant problem with the increasing number and complexity of devices that were available. Online training was viewed as helpful by those Officers interviewed. A TNA for all front-line Police Officers (baseline capability) had not yet been completed and was part of a next stage of the Cyber Strategy to be looked at now that the Cyber Support Unit project was completed and embedded within the Police Service.

The TNA had been completed and in that regard the recommendation can be considered achieved, however as discussed previously, Inspectors were told that awareness amongst front-line Police Officers around what can be done in the Cyber Crime Centre and Cyber Support Units and limiting the numbers and level of requests needed to be reviewed.

Inspectors assessed this recommendation was **Partially Achieved.**

OPERATIONAL RECOMMENDATION **6**

The Department of Justice, in consultation with the Police Service of Northern Ireland, 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.

Status: Achieved.

Paraphrased From the DoF website[16]

Since the publication of the 2017 report the DoJ and the Police Service have worked in partnership with the Department of Finance and Department for Economy to develop a cross-Departmental Strategic Framework for Action (Strategic Framework) on Cyber Security which was published on 29 March 2018. It closely aligns to the UK Cyber Security Strategy, sets out what top level areas need to be addressed through collaborative working across the public and private sectors to help ensure we capitalise on the economic opportunities this presents, but equally ensure we are as well protected as we can and when necessary have the right support infrastructures in place to respond effectively and efficiently to cyber-attacks and crimes.

The Strategic Framework recognises cyber security as a strategic priority and is aligned with the UK National Cyber Security Strategy and adopts the national strategy's three strategic themes of Defend, Deter and Develop. A cross-departmental Cyber Leadership Board has been established. Work is also underway to develop the appropriate business cases for the establishment of a Northern Ireland Security Centre.

In the interim the Police Service of Northern Ireland and DoJ refreshed the Organised Crime Task Force Cyber Crime subgroups which became one Cyber Engagement Group. The Terms of Reference included a communications focus, with the identification of opportunities for awareness campaigns. We are working on the development of a communications plan to cover the full range of the Organised Crime task Force work including cyber crime.

Police Service Response

Police Service Cyber Crime Centre have two dedicated officers who engaged with all sectors of the public, from schools and youth group, to business and government, delivering cyber security messaging. The engagements were enumerated as follows:

Engagements 2020 – 2023

- *Protect – 229 engagements;*
- *Prevent - 134 outreach engagements; 121 presentations.*

16 *Department of Finance, Cyber Security – A Strategic Framework for Action, 23 April 2018, updated 10 February 2022* available at *https://www.finance-ni.gov.uk/publications/cyber-security-strategic-framework-action.*

Inspectors' assessment

The 2018 *Strategic Framework* contained measures 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. Furthermore, a Cyber Security Centre was launched on 10 February 2020.[17] It aimed to deliver, in part, the Strategic Framework document.

This was a comprehensive review which was updated last in 2022. At the time of writing, the Police Service were 'chairing' the Cyber Engagement Subgroup. Raising awareness was referred to as 'ongoing' and one of the main functions of this subgroup. Taken with the investment in the Cyber Security Centre, there was evidence that this CJI operational recommendation was **Achieved**. However, the success and outcomes achieved from this approach as well as the potential for strategy overlap and sub-group duplication need to be reviewed and may be inspected by CJI in the future.

17 *Department of Finance, 10 February 2020* available at https://www.finance-ni.gov.uk/news/cyber-security-centre-launched-0.

CHAPTER 3: CONCLUSION

This Follow-Up Review was completed six years after the original inspection. This provided a long timeframe in which to gauge whether recommendations were achieved or still relevant given the developments of cyber crime and the changes within the Police Service since 2017. The development of technology and devices such as mobile phones and computers which are now being routinely used throughout society, has increased our susceptibility to become victims of cyber crime. Cyber crime has become more commonplace while becoming ever more complex and sophisticated. This has meant more pressures on the Police Service to examine more devices and investigators having to be constantly engaged with keeping up with cyber crime developments.

The 2017 Inspection made one strategic and six operational recommendations. Of these, three were achieved, three were not achieved and one was partially achieved. The Police Service were a key part of the wider cyber crime strategic approach through the Organised Crime Task Force group and nationally as part of an Annual Assessment of Fraud and Cyber Crime in the UK. However, the strategic recommendation was directed at identifying under-reporting and recording. It also sought to deal with the issue of tackling future demand on the Police Service. The Police Service were reviewing how cyber crime was strategically positioned and were developing a new model at the time of this Follow-Up Review. This meant that the analysis that was required in 2017 was equally required in 2023. The Police Service were also examining ways of aligning with the Scientific Support Branch which may mean a degree of civilianisation which Inspectors recommended in 2017. Inspectors were of the view that the strategic realignment of cyber crime needed to be conducted as a matter of priority as this Follow-Up Review identified long standing strategic issues were still to be addressed. There was also an opportunity to re-examine the oversight by the DoF and the DoJ, as the DoJ had identified redundant and overlapping approaches dealing with cyber crime.

The operational recommendations from the 2017 Inspection also called for better training and awareness, but this was still an issue in 2023 which was in part attributed to insufficient funding being made available and also the ever changing and complex nature of cyber crime which meant front line Officers needed to be continually updated and trained on new developments.

The UK Government had identified Action Fraud as having failed and the Police Service now needed to re-evaluate its ongoing use of Action Fraud.

The development of Cyber Support Units was a significant positive development from 2017. They were in the main working well. This Follow-Up Review revealed that backlogs remained a problem overall and that the steps taken in 2017 had not materialised into a significant reduction in delay that was needed. There remained a need to have better statistical analysis and management information available to support a demand model for cyber crime. Delay in the Court system had been attributed in part to the difficulties in retrieving digital evidence, but as discussed, this was an ever-growing problem with the proliferation of digital devices in everyday life and the increasingly complex modes of cyber crime.

Criminal Justice Inspection
Northern Ireland
a better justice system for all

First published in Northern Ireland in November 2023 by

Criminal Justice Inspection
Northern Ireland
Block 1, Knockview Buildings
Belfast BT4 3SJ
www.cjini.org

@CJININews

CJINI

Criminal Justice Inspection NI