SCOTTISH POLICE AUTHORITY
ÙGHDARRAS POILIS NA H-ALBA

Agenda Item 2.4

Meeting	**SPA Policing Performance Committee**
Date	**19 March 2025**
Location	**Video Conference**
Title of Paper	**Policing in a Digital World Programme Annual Report**
Presented By	**CS Conrad Trickett**
Recommendation to Members	**For Discussion**
Appendix Attached	**Yes - Policing in a Digital World Programme Annual Report 2025**

PURPOSE

The purpose of this briefing paper is to provide the members of the Scottish Police Authority (SPA) Policing Performance Committee with an update on the progress and direction of the Policing in a Digital World Programme (PDWP).

This paper will specifically provide a progress report in relation to:

Agenda Item 2.4: Policing in a Digital World Programme Annual Report

Members are invited to discuss the content of the Policing in a Digital World Programme Annual Report 2025.

1. SUMMARY

1.1 Please find attached the Policing in a Digital World Programme (PDWP) Annual Report 2025, which provides an overview of the journey since publication of the first PDWP Annual Report in March 2024, and documents the work over the last calendar year in terms of the various projects and work streams and the planned deliverables for 2025/26.

1.2 It outlines detail of capabilities delivered since the last annual report, including digital evidence detection dogs trained to detect a wide range of digital devices, and digital forensics vans allowing for 'at-scene' triage of digital devices. Another success of this year is the introduction of Police Cyber Alarm (PCA) which supports developing the Scottish intelligence picture and enables businesses to be aware of the threats their network face daily, providing them with the opportunity to take the necessary remediation measures.

1.3 Looking to the year ahead PDWP will support the delivery of key milestones set out within the Police Scotland Three-year Business Plan through workstreams to better prevent, protect, prepare and pursue fraud and cybercrime. These activities include, the establishment of a cyber and fraud specialist division, enhancing Police Scotland's existing digital forensic capability and obtaining internationally recognised accreditation for digital forensic activity, and to develop cyber and online training for the workforce.

2. FINANCIAL IMPLICATIONS

2.1 There are financial implications associated with the update in terms of the deliverables for 2025/26, which are subject to governance and budget approval.

2.2 Despite the current financial challenges to meet the ambition of the strategy, significant investment in our people, technology, estates, processes and structure is paramount.

3. PERSONNEL IMPLICATIONS

3.1 There are personnel implications associated with this update in terms of the associated projects and deliverables. Longer term, organisational change will be proposed in relation to structures required to enhance capabilities to prevent and deal more effectively with cyber dependant and enabled crimes.

4. LEGAL IMPLICATIONS

4.1 These are addressed and mitigated through the provision of our Rights Based Pathway which ensures that the introduction of new technologies is legally and ethically compliant.

5. REPUTATIONAL IMPLICATIONS

5.1 There may be reputational implications for Police Scotland if the improved capabilities and capacity are not delivered.

6. SOCIAL IMPLICATIONS

6.1 There are no social implications in this report.

7. COMMUNITY IMPACT

7.1 There are no community implications in this report.

8. EQUALITIES IMPLICATIONS

8.1 There are no equality implications in this report. All relevant documents will be completed in line with the formal investment governance process e.g. at Business Case stage. This will include a full consideration of rights-based challenges within relevant EQHRIA and DPIAs

9. ENVIRONMENT IMPLICATIONS

9.1 There are no environmental implications in this report.

RECOMMENDATIONS

Members are invited to discuss the content of the Policing in a Digital World Programme Annual Report 2025 designed to provide the SPA PPC with an update on its progress and direction.

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Policing in a Digital World Programme (PDWP)

Annual Report 2025

Contents

Assistant Chief Constable's Foreword

In taking on the role of Senior Responsible Officer (SRO) for the Policing in a Digital World Programme (PDWP) recently in February 2025, I would firstly like to provide a note of thanks to ACC Andy Freeburn for his leadership in tackling the challenges faced in this ever-changing cyber landscape.

Since publication of the first Policing in a Digital World Annual Report in March 2024, I am pleased to report there have been further significant developments since then, supporting deliverables we have set out to achieve as part of our future target operating model.

Since the last report, we have seen the publication of Police Scotland's 2030 vision and 3 Year Business plan setting out the Chief Constable's Strategic direction for the Service. This will see Police Scotland evolve with an overarching operating model that is fit for the challenges of today and tomorrow. It is critical that given the threat that cybercrime poses to the people, communities, businesses and assets of Scotland, we must adapt and modernise our policing model to respond effectively and continue keeping people safe in both the physical and digital world.

As an organisation, we are continuing to transform our service in how we respond to the evolving threat of cybercrime. We are delivering on this commitment through investment in our officers and staff, on the frontline and in specialist roles, so that they have the confidence, training, skills, tools and support to meet these new challenges.

Police Scotland continue to recognise and respond to online crime, which keeps evolving, being one of our biggest threats to our communities. I commend the introduction of digital evidence detection dogs trained to detect a wide range of digital devices and digital forensics vans, allowing

for ‘at-scene’ triage of digital devices. Both these capabilities have had a successful impact on our ability to protect those we serve and support investigations with a digital element. Another success of this year is the introduction of Police Cyber Alarm (PCA) which supports developing the Scottish intelligence picture and allowing business to be aware of the threats facing their networks on a daily basis, allowing them to take the necessary remediation.

In this journey, Police Scotland has a joint commitment with the Scottish Police Authority (SPA) to support decision making and to maintain public trust and confidence in the organisation, when adopting the use of technology. This Rights Based Pathway (RBP), referred to last year, will continue to support Police Scotland’s use of new technology and will be critical as we explore the use of Facial Recognition technology in 2025, as discussed at the Scottish Police Authority (SPA) Biometrics Symposium in April 2024.

Strategic Partnerships are key to tackling the evolution of Cyber and Fraud, which this year will be embedded within our new Cyber and Fraud Command, sitting as a key pillar in the Chief Constable’s 2030 vision. There is therefore a need for Police Scotland to continue to collaborate across the entire cyber sector in Scotland.

This leaves me to thank everyone for continuing to support Police Scotland in this journey through this challenging area of policing and I look forward to hopefully sharing further successes to come.

ACC Stuart Houston

Policing in Scotland

In September 2024, Chief Constable Jo Farrell outlined ‘Our 2030 Vision’ which focussed on the four key areas of:

- Safer Communities
- Less Crime
- Supported Victims
- A Thriving Workforce.

Within these publications the ambition was set to “establish a cyber and fraud specialist division to enhance our response in Scotland” and “develop our capability through cyber and online training for the workforce, ensuring support and guidance for officers and staff.” This approach is necessary to ensure that a future target operating model is scalable and fit for purpose, by giving our staff the resources and tools to provide improved services to the public of Scotland while also supporting greater involvement with partners in mitigating the threat of cyber and fraud.

The Policing in a Digital World Programme (PDWP) will support the delivery of key milestones set out within the 3 Year Business plan through workstreams to better prevent, protect, prepare and pursue fraud and cybercrime. These activities include, the establishment of a cyber and fraud specialist division, delivery of Police Cyber Alarm (PCA), enhancing Police Scotland’s existing digital forensic capability and obtain internationally recognised accreditation and to develop cyber and online training for the workforce. Above all, create efficiencies and keep pace with technological developments.

PDWP continue to work in collaboration with internal business areas and external partner agencies in line with the milestones to embed a harm prevention approach to all aspects of public policy.

In addition to our own strategic approach, our work seeks to align with wider UK law enforcement, including the following strategic visions, UK Fraud Strategy and National Policing Strategy for Fraud, Economic and Cybercrime.

UK Fraud Strategy

The UK Fraud Strategy entitled ‘stopping scams and protecting the public’ was launched by the Home Office on in May 2023, announcing the UK Government’s ambition to reduce fraud by 10% by 2025. It sets out how this can be achieved under a three-pillar approach (Pursue Fraudsters, Block Fraud, Empower People). Police Scotland will work towards shaping our operating model to this UK Fraud Strategy approach.

National Policing Strategy for Fraud, Economic and Cyber Crime

The City of London Police (CoLP) ‘National Policing Strategy for Fraud, Economic and Cybercrime’ was released in November 2023 to serve as the implementation plan for UK policing to improve collective response to fraud, economic and cybercrime through the delivery of key cross cutting strategic objectives.

The CoLP co-ordinates and leads the policing response as the National Police Chiefs Council (NPCC) Portfolio lead for economic and cybercrime and the National Lead Force for fraud. CoLP have set out key strategic objectives within their document, with the objectives therein linked to a nationally set commitment for policing which is translated into a ‘4P’ (Prevent, Protect, Prepare, Pursue) format, with deliverables for each threat area under fraud, money laundering and asset recovery and cybercrime. Police Scotland will continue to align our work under this ‘4 Ps’ approach, which will be further elaborated on within this report to again ensure align to wider UK Law enforcement strategy.

2024 in Review

Policing in a Digital World Programme (PDWP)

PDWP was formed with the clear aim to transform how Police Scotland responds to the evolving threat of cybercrime. The team has embedded a 4P's approach to dealing with cyber-related threats (Pursue, Protect, Prepare and Prevent), in line with the aforementioned UK strategies and also the NPCC led 'Team Cyber UK' methodology.

We must ensure all officers and staff on the frontline and in specialist roles have the knowledge, skills, tools, and support to confidently and effectively tackle cybercrime. In doing so, Police Scotland will be better equipped to prevent, respond to and investigate such crimes to keep people safe in public, private and virtual spaces.

PDWP routinely work with various internal stakeholders to enhance safety, prevention and resilience activity in relation to cybercrime. Key departments include;

- **Cybercrime Investigations and Digital Forensics**
- **Serious Organised Crime Financial Investigation Unit (SOCFIU**)
- **Cybercrime Harm Prevention (CHP)**

Following on from our last Annual Report and throughout 2024, PDWP have delivered a number of capabilities including Police Cyber Alarm, Digital Evidence Detection Dogs, Digital Forensic Vans and Data Ethics / Rights Based Pathway.

Police Cyber Alarm (PCA)

As part of Police Scotland's Cyber Protect activities in line with the milestones set out in the Chief Constable's 3 Year Business plan, PCA was launched across Scotland in August 2024 for use by businesses and organisations to monitor threats and receive regular vulnerability reports.

This work strengthens the UK law enforcement approach to collaboration through sharing capabilities as the PCA is an NPCC product managed and delivered by the CoLP with a 3rd party security software organisation, Pervade Software, providing the network structure.

This capability frequently identifies and updates organisations as to the potential weaknesses within their network security ensuring that every opportunity is taken to secure Scottish businesses from becoming a victim of cyber-attacks.

As of 7th February 2025, 98 organisations have signed up to utilise the PCA capability with more businesses exhibiting interest and requesting to join every month. CHP have promoted the tool at 16 Cyber Security conferences countrywide, with more scheduled for the year ahead.

The PCA capability also provides Police Scotland access to cyber data that was not previously available that tracks potential suspicious trends and behaviours in real time, develop digital intelligence to direct targeted resources, raise awareness and enhance capture of evidential material.

Digital Evidence Detection Dogs (DEDD)

PDWP, in conjunction with Operational Support Division (OSD) have introduced the new specialism of Digital Evidence Detection Dogs to detect hidden devices and hardware at locus. This aligns with the key milestone of investing in capabilities to prevent, protect, prepare and pursue cybercrime.

Where the organisation previously relied solely upon human search techniques (conventional and specially trained officers) to locate and identify digital devices, this has now been supplemented with this new capability.

In April 2024, 3 dedicated handlers and 4 dogs were introduced to provide a national capability which up until now has been facilitated through the provision of mutual aid from other Police Forces. As of February 2025, the Digital Evidence Detection Dogs have been deployed on 134 occasions across all territorial divisions for a variety of crime types identifying 416 digital devices which illustrates the necessity of this capability.

Digital Forensic Vans (DFV)

The provision of DFV since May 2024, has provided suitable and safe working environments for our officers and staff and has delivered an enhanced service to the people and communities of Scotland.

DFV are utilised for the examination of digital devices to provide optimum prospects of identifying investigative lines of enquiry at locus, while reducing delays in the owner being deprived of their device(s) for extended periods of time for the purpose of examination. This provision not only meets the milestone set out in the 3 Year Business plan for enhanced capabilities of digital forensic laboratories to create efficiencies, it also contributes to other milestone criteria with regards to an enhanced service to the communities and welfare for Police Scotland staff.

A survey was also carried out with our officers and staff following implementation of DFV provided the undernoted feedback and overall positive impact on their wellbeing:

“The Cyber Vans have had a significant positive impact on my day to day working environment.”

“The van is excellent for working practice and wellbeing.”

Data Ethics / Rights Based Pathway

As outlined in last year’s Annual Report, PDWP have worked in close partnership with our Data Ethics team and the Scottish Police Authority (SPA), on the development and delivery of Police Scotland’s Data Ethics Strategy and Framework. Based within the Chief Data Office (CDO), the Data Ethics team who are responsible for this pathway, help various projects to navigate the “Rights Based Pathway” (RBP), identifying and addressing any ethical considerations posed by the use of data-driven technology.

The RBP is designed to support decision making and to maintain public trust and confidence in Police Scotland in respect of its adoption and use of technology. The Data Ethics Triage (DET) process is an integral part of the RBP and ensures that Police Scotland can demonstrate a consistent and proportionate approach to assessing ethical and public interest considerations around new technology. Where a DET identifies a requirement for further scrutiny, the RBP now ensures there are formal mechanisms to seek further internal and external advice and challenge. Where required, the RBP also provides a route to public and stakeholder consultation. A post-implementation review stage has now been introduced, to ensure no unintended ethical consequences are identified following operational use of any data driven technology.

A review of the RBP commenced in 2024 to ensure it is meeting strategic objectives, and that there are defined end-to-end processes to manage projects through the Pathway. The review incorporated 'lessons learned' and observations captured by the CDO since the pilot began in Summer 2023.

The results of this review have highlighted the positive impact that the RBP has had across the organisation. The RBP has enhanced Police Scotland's existing governance procedures, provided improved opportunities for engagement with SPA and other key stakeholders. The RBP has established a single route for all new technology to navigate, ensuring that Police Scotland continues to innovate in a responsible manner.

External partnerships will be key to influencing our direction and ratifying our model which has public trust and confidence at the centre.

Cybercrime Investigations and Digital Forensics

Cybercrime Investigations and Digital Forensics provide national coverage and specialist operational support to all Divisions across Scotland.

They comprise of:

- **Cybercrime Investigations** - responsible for providing specialist support and undertaking investigations into high-end cyber-dependent crimes.
- **Digital Forensics** – responsible for carrying out examinations and analysis of digital devices/CCTV as well as providing expert advice, specialist recovery services and reports for court. The department works closely with the Internet Investigations Unit (IIU) as well as carrying out National Online Child Abuse Protection (NOCAP) investigations and enforcement activity.

In the calendar year of 2024, the Cybercrime Gateway approved a total of 4577 Electronic Request Forms (ERF's) relating to examinations at Cyber Kiosks, equating to a total of 9201 digital devices. The Gateway further to this approved a total of 3867 ERFs for examination at DF Labs, relating to a total of 10634 devices and offences ranging from the Misuse of Drug Act 1971 (MDA) offences, domestic incidents, Serious and Organised Crime (SOC) and murder enquiries.

A further 5891 devices were triaged at locus by NOCAP teams across the Force, requiring only 22% of those (1278 devices) to be seized for further examination at a Digital Forensic Laboratory.

Cyber Investigations received a total of 165 Cryptocurrency Support Requests within 2024.

Case Study – Op EDITORIAL

Op EDITORIAL was an investigation that resulted in a significant prison sentence for a 21-year-old Cyber security student from the West of Scotland for creating and administering a DDOS (Distributed Denial of Service) tool known as MYRA.

On 18th July 2024, Amar Tagore, 21, of West Dumbartonshire pled guilty without challenge to Computer Misuse Act (CMA) Offences and Money Laundering totalling over £45,000 and was jailed for a total of 21 Months.

In November 2022, following receipt and development of the intelligence from Essex Police, Police Scotland executed a search warrant at the home address of TAGORE.

Upon entering the property officers found him to be active on his computer with a terminal window open and supporting ‘users’ on MYRA access platform, Discord. Following live examination and capture of the terminal data, officers became aware that the suspect appeared to have been carrying out Internet Protocol (IP) registrant checks for an IP connected to an Australian airport.

Urgent action was taken by officers to stop any further attacks and notify partner agencies and as the enquiry unfolded, further information was obtained from overseas, with multiple devices being subject of forensic analysis.

Detective Sergeant Kelly Thorburn, the case officer, stated;

“The case presented significant challenges, requiring a review of over several million data points, including live and static digital forensic data, server data, financial data, cryptocurrency data, open-source data and communications data, and required the ingesting of live Digital Forensic videos and use of Optical Character Recognition, including duplication removal.”

The resultant outcome was a single overarching report, in excess of 100 pages, collated by the team, focussed on bringing together all case artefacts to cover the attribution, administration of marketing, communication/sales set up, payment and infrastructure used to run the service, that was broken down and discussed with the Crown Office to broach the presentation of data in court and how to get the technical data understood by a sheriff and jury.

Operation Editorial saw the boundaries pushed in terms of live Digital Forensic Capabilities to ensure capture of relevant evidence, including from Discord channels, and mitigation of a live running attack at the time of warrant enforcement.

Subsequent de-briefs have been held with Crown and Police Scotland highlighting key learning points for the future around the presentation of complex digital investigations, which are now being built into inputs on the Scottish Police College Digital Media Investigator (DMI) courses and at our Digital and Data Skills Academy.

The team have since received an award for ‘innovation’ from the International Digital Investigation Awards, from the Home Office in October 2024.

Serious and Organised Crime Financial Investigation Unit (SOCFIU)

Cyber and Fraud investigation is managed internally under separate functions, specifically Financial Investigation teams and Cybercrime spread force wide, creating obstacles in terms of resources, equipment, training and capacity. With 95% of fraud now committed online, this has resulted in further overlaps and a dependency on collaborative working between fraud departments and cybercrime units who currently have competing demands as separate entities.

In the calendar year of 2024 there were 58 enquiries or operations investigated by SOCFIU, these enquiries having a total value of crime recorded as £188,821,353. The department supports a variety of Divisions and departments to exploit all Proceeds of Crime Act (POCA) opportunities and identify Money Laundering investigations for designation.

In relation to these investigations, there have been 153 suspects investigated, 34 warrants executed, 55 persons arrested and £7,655,951 of recoveries/items seized.

The charges being investigated/preferred relate to; Money Laundering offences s327, s328 and s329 POCA 2002, Fraud & Theft, IP theft and Copyright Theft, MDA offences, Embezzlement, Human Trafficking, Criminal Justice and Licensing (Scotland) Act 2010 Section 30(1)(b), Criminal Justice and Licensing (Scotland) Act 2010 Section 28(1) and Bribery offences.

One enquiry regarding Cryptocurrency has been referred to civil recovery via an expedited referral relating to over $40 million of cryptocurrency contained in USB devices.

Case Study:

Operation Tailpiece is an enquiry into fraud committed against an elderly victim in Biggar, Scotland. The victim was defrauded to the value of approximately £2.14 million via vishing, courier and safe account fraud.

She was contacted via phone call by an unknown male suspect who claimed he worked for the Financial Conduct Authority. The victim was falsely informed that her bank accounts and savings were at risk and over a course of several weeks she was coached through de-investing her investment portfolio and purchasing around £2million in gold bullion. Couriers from the Greater London area were given the victim's address and directed to drive to Scotland and collect the gold bullion over four collection dates.

The movements thereafter of the gold are currently unknown and it has not been subsequently traced by Police Scotland. There have been further victims identified as being linked to Op TAILPIECE in England within the Greater London area, and it is assessed that this is where the organised crime network is largely based.

Cybercrime Harm Prevention (CHP)

CHP work with the public, private and voluntary sectors to raise awareness and promote prevention activity for cyber enabled harms and frauds. The team work with strategic partners to work towards the Scottish Government's Cyber Resilient Scotland Framework, ensuring organisations such as national critical infrastructure plan and prepare for, can respond to and recover from cyber-attacks as well as supporting victims to return to a new normal.

In support of this they have launched several large-scale online engagement campaigns to raise awareness of online dangers to improve community safety and have a sustainable legacy of collaboration and education.

Child Online Safety – East Ayrshire Pilot and National Rollout

The CHP team piloted and rolled out a campaign to address Sextortion messaging, identifying it had remained unchanged for years and previous campaigns had failed to engage effectively.

This involved breaking down victim profiles to gain deeper understanding to identify the target audience, ensuring messaging resonates in intended audience as well as remains inclusive for all victims the team collaborated with partners to ensure a best practice approach.

Working with a Local Policing Division (LPD) to host two online safety webinars for parents and carers in partnership with the local Education Authority, enabling the ability to include harder to reach audiences which will be developed for nationwide implementation. This allowed key prevention messages to be shared widely and provided the audience an opportunity to ask questions.

Sextortion Campaign (Fearless/Awareness Raising)

The campaign was designed in collaboration with young people to ensure that the language and platforms used were relevant for the young people of today. Short videos were created targeting young people, for use on social media with further materials including views of Police, Fearless and NSPCC to raise awareness of sextortion with corporate parents and those working with young people.

Awareness sessions by Police and Fearless were also delivered to professionals working with children throughout Scotland. The team has also engaged with key organisations, presenting to the Social Work Scotland Adult and Children's Committees and the Scottish Government National Strategic Forum. A new resource on harmful behaviours online, covering sextortion and non-consensual image sharing, has been created for officers to support this piece. Continuous Professional Development (CPD) sessions were held for youth engagement officers and community policing teams to deliver sextortion resources locally.

Bringing the Target Operating Model to Life

Our work over the last year has allowed for the formulation and adaptation of our objectives centring around the nationally recognised ‘4 P’ approach of Pursue, Prevent, Protect and Prepare.

This enables Police Scotland to:

- Focus on an improved victim experience (overarching outcome).
- Deliver an effective investigative response (Pursue).
- Target local cybercrime prevention messaging (Protect).
- Work to identify and divert people vulnerable to engaging in cybercrime (Prevent).
- Engage with businesses and organisations to help them develop effective measures to mitigate threats and risks associated with cybercrime and, where appropriate, engage in testing and exercising (Protect).
- Develop Centres of Excellence and provide guidance to the wider force, helping mainstream cyber skills and knowledge into most areas of policing (Prepare).
- While also adding in the overarching components of People, Partnerships and Horizon Scanning. (Prepare)

The evolution of this approach has created a holistic and sustainable model for developing Police Scotland’s cyber capabilities and preparedness for future threats.

As part of the 3 Year Business plan, the establishment of a new, permanent multi-disciplinary digital and data innovation product team within Police Scotland to support officers and staff in all areas of policing in finding efficiency and power real innovation is a key enabler within the Horizon Scanning element of the Target Operating Model (TOM).

With public trust and confidence at heart, the teams within PDWP, CHP, SOCFIU and Cybercrime Investigations and Digital Forensics, are working together to deliver the target operating model in line with UK Law Enforcement strategies, NPCC methodology and 3 Year plan milestones set out within the Chief Constable’s 2030 vision.

Cyber and Fraud Command

Following on from the PDWP Annual Report 2024 the Fraud Strategy and Operating Model project had, in part, began work towards the Chief Constable's 2030 Vision. The scope of the project is to support Police Scotland to effectively tackle the issue of fraud and develop and implement a revised Cyber and Fraud Target Operating Model (TOM), to bring about the holistic change necessary to better support the public and become a 'centre of excellence' in the reporting and triage of such crimes. The revised Cyber and Fraud Target Operating Model includes delivering:

- Joining the Fraud Cybercrime Reporting and Analysis Service (FCCRAS).
- Establishing a single strategic lead for fraud within Police Scotland (Assistant Chief Constable Level).
- Fraud Hub - Establishing a National Fraud Unit to provide organisational oversight, consistency and support for the establishment of a national investigative model.

Building on this and in line with the Chief Constable's vision, the Programme team have been collaborating with internal departments who will form part of our new Cyber and Fraud Command under Specialist Crime Division (SCD). This has included collaboration between PDWP, Cybercrime Investigations and Digital Forensics, SOCFIU and CHP, to develop a timeline for a staged implementation plan commencing in April 2025. This takes into consideration the necessary organisational governance, resourcing and financial impacts to develop a phased approach which will maximise the change while minimising disruption and meeting necessary requirements.

A senior management team to support the implementation of Cyber and Fraud Command will be established, headed up by a Detective Chief Superintendent, seeking to implement this new command in a phased approach using the 4 P format. The following provides an insight into activity which would we are seeking to align under this new approach.

Pursue

This focuses on our ability to pursue individuals, groups and larger organisations involved in the most serious cyber and fraud threats to Scotland by prosecuting and disrupting this criminal activity.

Through collaboration and critically analysing the threats facing Scotland, PDWP understand the need to collaborate with national and international law enforcement, to provide a multi-disciplinary approach to tackling cyber and fraud.

Within this work, there was an identified need to provide new capabilities to our investigation and intelligence teams which would enhance our ability to investigate cyber related offences.

Cryptocurrency

Since 2019, Police Scotland has experienced a circa 2000% increase in cryptocurrency related criminality.

As technology evolves, serious and organised crime groups are quick to adapt and utilise new methods to help obfuscate their activities with the use of cryptocurrency being one such method.

Police Scotland currently have made significant strides forward in terms of capability and now have two track and trace tools aligning them with much of UK and leading international law enforcement.

Police Scotland does not have a dedicated cryptocurrency team and development of capabilities outside of cybercrime is progressing. Police Scotland's proposed Cyber and Fraud Command will allow for a refresh of organisational approach and responsibilities in relation to cryptocurrency. This will align with other UK law enforcement approaches which have seen the setup of dedicated cryptocurrency teams.

Police Scotland is working nationally to align approaches, sitting on the cross-sector Cryptocurrency Working Group looking at approaches, training and development including designing a training pathway to include expert witness testimony.

Police Scotland officers have given evidence on Cryptocurrency in Scottish Courts on multiple occasions, including in the High Court, and their testimony has been accepted as competent.

Dark Web

Whilst most cyber and fraud crime occurs via the surface web, or what would generally be described as the internet, there is another part of the internet, known as the dark web, which is increasingly used to commit crime, often on an industrial scale.

As a result, the dark web has become easily accessible for today's criminals to arrange the supply of commodities (e.g. controlled drugs, counterfeits, firearms, data), commit acts associated to human trafficking and be a method for facilitating other crimes, such as extortion, fraud, ransomware attacks and livestreaming of sexual abuse.

Police Scotland are seeking to increase our presence on the dark web and enhance our investigative ability. This will enable us to pro-actively deploy specialists to enable a greater assessment and understanding of the threat to our communities.

Dark web intelligence development has been brought under Cybercrime Investigations who engage UK wide with the Dark Web Intelligence, Collection and Exploitation (DICE) network.

Police Scotland officers have received dark web training with a view to obtaining dark web tools and threat intelligence software to bring us in line with the rest of UK Law Enforcement.

ISO17025

Police Scotland is continuing to progress towards ISO/IEC 17025:2017 accreditation of our five Digital Forensics (DF) laboratories, which will be assessed by the United Kingdom Accreditation Service (UKAS).

The first of these laboratories is the Aberdeen lab for which the application to UKAS is complete. The UKAS assessment requires policies and procedures to address and comply with the standards set out in ISO/IEC 17025:2017. Aberdeen and Inverness labs are now working to these policies and procedures which we refer to as ‘Steady State’ while awaiting assessment for capture and preservation of data from mobile devices.

Over the coming months, Aberdeen lab will continue in preparation for UKAS assessments anticipated to take place around February 2026 for Pre-assessment and April/May 2026 for full assessment. Meanwhile, preparations are progressing for the remaining DF labs that will be subject to accreditation – with the other labs are working towards ‘Steady State’ dates throughout 2025.

A Technical Assurance Team will be created to support the DF labs and the Cybercrime Quality Assurance Team. Technical Assurance activities will include validation and verification of the equipment and software used in the forensic examination of digital devices which will be an ongoing requirement for accreditation. Following the assessment by UKAS at the Aberdeen DF site all feedback, and any remedial action, will be collated and submitted to UKAS for consideration. All feedback and actions will be communicated to senior management teams as well the other DF labs.

It is anticipated that formal accreditation for Aberdeen will be granted between October 2026 and March 2027. Once accreditation has been granted, subsequent surveillance visits will follow as well as UKAS assessment visits for Inverness and the remaining labs. After accreditation, each lab will move out of the scope of the project and into the business-as-usual space.

Prevent, Protect and Prepare

The teams within PDWP, CHP, SOCFIU and Cybercrime Investigations and Digital Forensics, all champion cyber security and online safety. This also includes a need to support vulnerable people, remote communities through collaborative working internally and in collaboration with third sector, statutory and charity organisations.

Collectively the teams have identified and developed strong working relationships with a number of organisations across the cyber landscape in terms of law enforcement, public, private and third sector partners. They engage in national collaborations with the National Cyber Security Centre (NCSC), CoLP, and Regional Organised Crime Units (ROCU) with a focus on supporting victims of cyber dependant crime as well as cyber enabled crimes such as domestic abuse in the digital space, offering guidance on recognising and reporting cyber-enabled stalking as well as various social engineered scams.

CHP furthermore provide tailored guidance, resources and reassurance while engaging inclusively to expand outreach. Their efforts include bespoke CHP guidance for individuals and organisations, helping victims recover from cybercrime and enhance resilience.

Reaching out beyond the immediate scope of project work, however in line with milestones set out in the 3 Year Business plan, PDWP work closely with the innovation team and other internal business areas. This is in tandem with external partners to highlight, develop and invest in our capabilities surrounding data science, AI and analytics to support both our organisational strategies.

Understanding of emerging crime trends, the technology used by or potential targets for criminals, is paramount to the success of proactive policing in the digital world now and in the future. Utilising data analytics, horizon scanning and partnering with key professionals all better keep Police Scotland abreast of technological advancements, identify areas of evolving cyber and fraud threats, aid the pursuance of offenders, support decision making toward successful intervention opportunities and ultimately make Scotland an unattractive place for criminality.

A modern, digitally aware and continuously skilled workforce is required to successfully deliver law enforcement against the current and future landscapes of policing. Police Scotland therefore require to ensure our people have the right tools, training and technology to carry out their roles. For specialist roles, we further need to ensure that we can attract the best graduates from top Scottish universities and create career pathways that will help us retain talent.

Cyber Choices Scotland

Cyber Choices Scotland (CCS) sits under Police Scotland's Cyber Prevent strand of the 4 P's which brings alignment to activities within the UK, as part of the Team Cyber UK methodology.

CCS has been developed as a two-fold purpose; the first being a focus within the prevention space of identifying, engaging and diverting those who are on the cusp or potentially susceptible to becoming drawn into cyber criminal behaviour. The additional strand is a clear commitment to the recognition of having a programme in place to allow for relevant and appropriate diversion from prosecution or reporting through COPFS and Youth Justice.

PDWP have over the last year worked with key stakeholders to plan and deliver CCS across its many facets including CyberFirst, YouthLink Scotland, Cyber Scotland Partnership, Scottish Government, Young Scot, The Donaldson's Trust, Local Policing and Police Scotland Youth Volunteers. This has produced a timeline to deliver CCS in April 2025 with an introductory launch to support delivery to coincide with Cyber Scotland Week 2025. Work continues with the national Cyber Prevent network across the UK and the National Crime Agency (NCA), to ensure that where necessary, law enforcement collaboration is achieved and encouraged whilst delivering a framework that is bespoke to Scotland and builds on traditional partnership approaches to delivering solutions.

PDWP are engaging with key stakeholder areas to develop specific processes, identifying training and awareness requirements and promoting new links from national to local policing levels to assist its roll out.

Cyber Scotland Week

Cyber Scotland Week 2025 (Monday 24th February– Sunday 2nd March) focuses on improving cyber resilience across communities with the theme “Can’t Hack It.” Organized by the prevention team, the initiative promotes simple, practical steps to enhance cybersecurity for individuals, businesses, and families utilising internal and external comms. Activities delivered as part of the week were as follows:

- Webinars for Parents & Carers: Targeted sessions, led by CHP, aiming to educate parents on cyber risks and online safety for children.
- Business Engagement: Events such as a U Division business seminar and Northlink Ferries session to highlight cyber resilience for companies.
- Community Outreach: Tailored presentations for schools, rural communities, and older adults will cover topics like password hygiene and social engineering. Resources are being developed for local delivery by police divisions.
- Media & Podcasts: Podcasts, social media soundbites, and animations coordinated by CHP and Corporate Communications that will amplify the campaign's reach.
- Future Scot 2025 Conference – 25th February: Presentations by Cybercrime and CHP staff to the Scottish Government and national parent groups will reinforce the message of cyber safety.

Cyber Scotland Week captures all of the 4P’s approach, collaboration and shared learning across all participants has a clear objective of Prevent, Protect and Prepare, which ultimately facilitates Pursue.

Cyber Scotland Partnership (CSP)

CyberScotland Partnership (CSP) is a collaborative leadership approach to focus efforts on improving cyber resilience across Scotland. Police Scotland continue to work with the Big Partnership, who lead on communication deliverables, and other members of the CSP to ensure current initiatives and relevant prevention advice is made available for dissemination across the partnership’s networks.

CHP are lead on this nationwide partnership of strategic bodies, brought together to promote cyber resilience to global organisations based in Scotland and are key for Police Scotland in the Prevent, Protect and Prepare space.

Scottish Cyber Coordination Centre (SC3)

A number of milestones set out in the 3 Year Business plan focus on Police Scotland's collaboration with Scottish and UK Governments, to capture and embed system-wide learning from major incidents and national emergencies to embed a harm prevention approach to all aspects of public policy.

The Strategic Framework for a Cyber Resilient Scotland, championed by Scottish Ministers, outlines their vision for a digitally resilient nation. In this Framework, they acknowledge the pivotal role of digital technologies in our daily lives, society, and economy.

As Scotland embraces and benefits from digital transformation, it also faces a serious and evolving cyber threat and risk landscape as a result. Following on from several significant cyber-attacks on Scottish Public Sector organisations, Ministers announced that as a matter of urgency they were bringing forward proposals for the establishment of a recognised, authoritative, and collaborative function to combat the accelerating cyber threat. The Scottish Cyber Coordination Centre (SC3) was established to meet this requirement and address key cyber resilience challenges facing Scotland.

Vision for 2027: SC3 will be a focal point for Scotland's cyber security and resilience, providing services to help protect against and respond to the accelerating and evolving threat of cyber-attack while promoting adherence to appropriate standards and best practices across critical functions and infrastructure.

Cyber Symposium – February 2024

As part of PDWP's work to promote partnerships and instigate a better understanding of the cyber threat landscape being enforced worldwide, in February 2024, the programme team hosted an International Cyber Symposium with law enforcement partners from across the UK and abroad.

Representatives from CoLP, the Metropolitan Police, National Crime Agency (NCA), Federal Bureau of Investigation (FBI), New Zealand Police, Australian Federal Police (AFP) and Romanian Police attended, presented and shared organisational structures, operating models and best practices being used in order to meet the ever-emerging threat.

The aim of the symposium was to share current thinking across UK and International law enforcement professionals on the future of law enforcement in tackling to growing threat of cyber and online fraud.

As a key Prepare objective, by exploring the different elements of our organisation, taking cognisance and learning from a UK and worldwide law enforcement approach, we have, and will continue to explore options and opportunities to inform transformation.

Cyber and Fraud Centre Scotland (CFCS) - Multi Agency Fraud Hub

Police Scotland fully recognise there are multiple agencies and organisations who have a footprint in cyber enabled/dependent crime including response, investigation and intelligence. This includes organisations such as the Cyber Scotland Partnership, SC3 and the Cyber and Fraud Centre Scotland (CFCS).

There is therefore a need for Police Scotland to continue to collaborate across the entire cyber sector in Scotland, to pull together the collective resources, so that we become more than the sum of our parts.

In support of this and to enhance stakeholder engagement, Police Scotland Chair the Strategic Fraud Governance Group with partners from Scottish Government, the banking and financial sector and the CFCS. A Multi-agency Fraud Triage Hub pilot was commenced as part of this, with the objective of ensuring that we work in collaboration to tackle and prevent this escalating threat.

Since group's inception, this collaborative approach has grown and developed into a highly effective function, which has seen clear tangible successes and outcome as a result. This includes incidents of fraud valuing over £10 million having been collectively worked on and £3 million of this has been either stopped or recovered. In addition to the proactive work instigated by the group, a result of the real time sharing of information and intelligence around emerging fraud trends and methods has helped identify innovative and effective disruption, intervention and prevention opportunities whilst safeguarding and identifying appropriate support for victims.

This approach ultimately reduces demand on front line policing resources, partner resources and has improved criminal justice outcomes. These activities and outcomes contribute to objectives under each of the three pillars of the UK Fraud Strategy. CFCS are currently exploring funding opportunities with a view to making the Multi- Agency Financial Crime Triage Hub a permanent and key part of Scotland's response to tackling fraud.

Additional UK Collaboration

Numerous cyber threat assessments produced by the NCSC, the National Management Centre and other departments across government cite significant and escalating risks of cyber-attacks on the police digital estate and policing supply chain whether at a local, regional or national level.

Significant ransomware attacks took place on the UK policing supply chain, where companies in possession of policing data suffered large scale data breaches, resulting in private information pertaining to victims of crime, suspects and other members of the public being published on the dark web. It is clear such attacks are likely to continue and have the potential to impact right across policing. For this reason, Police Scotland have been working collaboratively with the CoLP and NPCC to explore how to further forge closer links and collaboration and are now integrated into the UK 24/7 CSI Gold Chief Officer Cadre as part of Operation DA1 (Defend As One).

These close working relationships will continue with the ambition of creating a fully integrated law enforcement model to tackle cybercrime. The benefits of such an approach include efficient working arrangements between law enforcement agencies, early identification and response to emerging threats. In addition, as an organisation it will enable us to be confident, capable and resilient in the fast-moving digital world. To fully maximise the opportunities, we will look to become actively involved in broader initiatives and leverage support and access to funding.

Data Drives Digital

A Data Science Centre of Excellence has been set up within the Chief Data Office, bringing together the technical expertise of Data Scientists, Data Engineers and Data Analysts to focus on releasing efficiencies and delivering operational capability across the organisation.

This unit is the product of extensive engagement and will harness the opportunities present within Artificial Intelligence (AI) to deliver material improvement to policing in Scotland.

Any solutions built will be done so in a way that is secure, ethical, and transparent, making full use of the mature Rights-Based Pathway and Data Ethics Triage process already in place.

Innovation Team

The Innovation team is a small and ambitious department focusing on exploring technology and innovative practices to enhance Policing and support Police Scotland to prepare for future opportunities and challenges. The team are a key enabler with regard to the delivery of the 2030 vision to become a more data driven organisation while being more efficient and increasing productivity.

The innovation team engage with key internal stakeholders to understand organisational developments, avoid duplication, and share where we can add value.

They do this by focusing on four key outcomes:

- Organisational awareness
- Knowledge sharing
- Sandbox testing
- Supported implementation

The Innovation Team work across three ‘innovation time-horizons’ which are segmented, by the development status of technology (or innovative practices) and our ability as an organisation to use it.

Professional Reference Group

PDWP continue to work alongside members of the Professional Reference Group (PRG) to ensure our organisational approach to policing in a digital world is informed by subject matter experts.

Working in collaboration with key stakeholders ensures that our approach is both current and resilient to future long-term societal changes and technological advancement further ensures Police Scotland is prepared and in a state of readiness to tackle new challenges. At the last meeting of the group in December 2024, the group had a focussed discussion on the ethical implications of the use of live facial recognition technology.

Building on the success of the PRG, discussions are ongoing to explore expanding the remit of the group to include areas such as Artificial Intelligence (AI), Biometrics and Data Ethics.

Cyber Training and Capability Project

The PDWP Cyber Training and Capability project seeks to equip Police Scotland's officers and staff with the training, capability and capacity to respond to threats and establish ways to prevent, protect and pursue the ever more inventive and complex use of digital tools and tactics.

The Cyber and Digital Knowledge Hub launched in December 2024 is an accessible policing resource, serving both officers and staff on the front line and those working with specialist departments. It offers a wealth of information to build and enhance understanding of the cyber and digital skills required to undertake investigations effectively.

Training being delivered is across multiple avenues including an E-Learning platform, 1 day in-person classroom sessions, bitesize online sessions, training on demand 24/7 recorded inputs via the Knowledge Hub and further In-person events.

E-Learning training will cover Open-Source Introduction, Open-Source scenarios, Comms Data Introduction, Comms Data Types, the Comms Data Application process and Comms Data – Understanding Data.

Bitesize online learning sessions on Webex initially for the West area and Training on Demand 24/7 recorded sessions on the Knowledge Hub will roll out in early 2025 and will cover Introduction to Cryptocurrency, Dark Web, Comms Data, C3, ERF Process, Introduction to Cyber Security sessions and other Cyber and Digital related CPD. In person events will also continue to be developed, initially covering a Digital Foundation module.

Procurement of advanced training for staff and officers who are in specialist roles which predominately investigate digital, cyber enabled and cyber dependent crimes is currently ongoing. This training targets those who are competent in cyber digital investigation and have a sound understanding and appreciation of cyber enabled/dependent crimes and the investigative opportunities they present. This training is planned to be delivered in early 2025.

Academic Research

Police Scotland's Research and Insights team support the PDWP's portfolio, under Prevent, Protect and Prepare to develop and participate in research studies which align with strategic priorities; ensuring an evidence-led approach is applied to decision making.

The team also collate and coordinate an internal database of research which can be accessed by colleagues across the service to inform the development of strategy.

PDWP are currently supporting the delivery of the undernoted projects and continue to work closely with stakeholders to identify new opportunities to address emerging challenges and knowledge gaps.

- Mapping capacities for a Model of Community Policing of Cybercrime and Digital harm in Scotland (Napier University)
- Understanding young people and adult perceptions of online threats (University of Glasgow)
- Scoping the landscape of Image-Based Sexual Abuse in Scotland (Glasgow Caledonian University)
- Technology and Drug Markets – (University of Glasgow)

In addition, the portfolio has recently secured external funding which allows Police Scotland to participate in two high-profile research consortiums; these workstreams will support the service in developing approaches to protecting officers from online risks and harms, and to enhance the quality, impartiality and reliability of digital forensic investigation.

Academia - Abertay cyberQuarter

PDWP have now received approval to become a member of the Abertay cyberQuarter. The £18m hub was opened in June 2022 within Abertay University, Dundee. The cyberQuarter has been jointly funded by the University, UK Government and Scottish Government, through the Tay Cities Region Deal, providing a new model for supporting the rapidly growing cyber sector in a facility that's the first of its kind in the country.

The initiative brings together students, academics and organisations to help solve global cybersecurity challenges. Following engagement, the key benefits and collaboration opportunities in addition to consultancy include:

- Research and Development (R&D)
- Access to specialist resources, technology and infrastructure.
- Knowledge Transfer Partnership - Projects to address specific strategic challenges, where together new knowledge/expertise is created.

Working closely with all these partners reinforces Police Scotland's ability to operate affectively against the current and future threats of Cybercrime. Our ability to Pursue, Prevent, Protect and Prepare is reinforced by partnership working.

Glossary

A

ACC – Assistant Chief Constable

AFP – Australian Federal Police

AI – Artificial Intelligence

C

CCS – Cyber Choices Scotland

CDO – Chief Data Office

CFCS – Cyber and Fraud Centre Scotland

CHP – Cybercrime Harm Prevention

CoLP – City of London Police

CMA – Computer Misuse Act

CPD – Continuous Professional Development

CSP – CyberScotland Partnership

D

DDD – Data Drives Digital

DDOS – Distributed Denial of Service

DEDD – Digital Evidence Detection Dog

DET – Data Ethics Triage

DF – Digital Forensics

DFV – Digital Forensic Van

DICE – Dark Web Intelligence Collection and Exploitation Unit

DMI – Digital Media Investigator

E

ERF – Electronic Request Form

F

FBI – Federal Bureau of Investigation

FCCRAS - Fraud and Cyber Crime Reporting and Analysis System

I

IP – Internet Protocol

L

LPD – Local Policing Division

M

MDA – Misuse of Drugs Act

N

NCA – National Crime Agency

NCSC – National Cyber Security Centre

NOCAP – National Online Child Abuse Protection

NPCC – National Police Chiefs Council

P

PCA – Police Cyber Alarm

PDWP – Policing in a Digital World Programme

POCA – Proceeds Of Crime Act

PRG – Professional Reference Group

O

OSD – Operational Support Division

R

RBP – Rights Based Pathway

ROCU – Regional Organised Crime Unit

R&D – Research and Development

S

SC3 - Scottish Cyber Coordination Centre

SCD – Scottish Crime Division

SME - Small & Medium Enterprises

SOC – Serious and Organised Crime

SOCFIU – Serious and Organised Crime Financial Investigation Unit

SPA - Scottish Police Authority

SRO – Senior Responsible Officer

T

TOM – Target Operating Model

U

UKAS - United Kingdom Accreditation Service