SCOTTISH POLICE AUTHORITY
ÙGHDARRAS POILIS NA H-ALBA

Agenda Item 2.3

Meeting	**SPA Policing Performance Committee**
Date	**7 December 2022**
Location	**Video Conference**
Title of Paper	**Policing in a Digital World Programme Update**
Presented By	**ACC Andy Freeburn, Organised Crime, CT and Intel**
Recommendation to Members	**For Discussion**
Appendix Attached	**Yes** **Appendix A – Policing in a Digital World**

PURPOSE

The purpose of this paper is to provide members with an update on progress and direction of travel of the Policing in a Digital World Programme.

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

Agenda item 2.3 – Policing in a Digital World Programme

Members are invited to discuss the contents of the report and Appendix A.

1. BACKGROUND

1.1 Police Scotland's Cyber Strategy 2020 '*Keeping People Safe in a Digital World'* was approved by the Scottish Police Authority (SPA) on 30 September 2020.

1.2 In April 2022, Cyber Strategy Implementation Programme and Cyber Capabilities Programme merged to become Policing in a Digital World Programme (PWDP), under the leadership of ACC Andy Freeburn.

1.3 The PDWP aims to transform how Police Scotland respond to the evolving threat of cybercrime. The Programme will enable us to continue keeping Scotland's people, communities, businesses and assets safe in both the physical and virtual world.

1.4 The Programme will embed a 4P's approach to dealing with cyber related threats (Pursue, Protect, Prepare and Prevent), in line with the NPCC led 'Team Cyber UK' methodology.

1.5 It will enable Police Scotland to:

- Focus on an improved victim experience,
- Deliver an effective investigative response,
- Target local cybercrime prevention messaging,
- Work to identify and divert people vulnerable to embarking on cybercrime,
- 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,
- Develop Centres of Excellence and provide guidance to the wider force, helping mainstream cyber skills and knowledge into most areas of policing.

1.6 By ensuring all officers and staff, on the frontline and in specialist roles, have the knowledge, skills, tools and support, Police Scotland will be better equipped to prevent, respond, and investigate cybercrime. We must build the workforce and tools to keep people safe in public, private and virtual spaces.

2. FURTHER DETAIL ON TOPIC REPORT

Current Threat Picture & Response

2.1 Cyber enabled and cyber dependent crime has been increasing exponentially this has grown further during the COVID-19 pandemic. This is an area of increasing risk and Police Scotland wish to ensure that our policing model can respond effectively.

2.2 For these reasons, Tackling Crime in the Digital Age is one of four priorities for policing as outlined in our Joint Strategy with the Scottish Police Authority.

2.3 The following figures provide the scale of the problem and the threat, risk and harm this poses to the communities across Scotland:

- 511% increase of Online Child Sexual Abuse and Exploitation (OCSAE) referrals from 2015-2021.
- 650% increase of referrals regarding child sexual abuse imagery over a 9 year period.
- 17% increase of fraud was recorded in the past 12 months, with a 68% increase over the last 5 years.
- Average of 1500 crime per month, 95% of which are now online.
- Around 40% of businesses across the UK are victims of cybercrime, many of which don't even report it, viewing it as simpler to pay the ransomware attackers, than suffer the reputational damage of the loss of customer's data.

2.4 Police Scotland has made good progress in this space, including significant investment in digital forensics staffing, staff training and the roll out of a First Responders Guide (FRG).

2.5 We have established partnerships across the cyber ecosystem, including being a key stakeholder in the Cyber Scotland Partnership, with a focus on reaching public, private, and 3rd sector/learning and skills development, promoting cyber security and online safety.

Professional Services

2.6 In January 2022, PricewaterhouseCoopers (PwC) following a full tendering process, were commissioned to carry out a "critical friend" review of the Police Scotland Cyber Strategy.

2.7 They subsequently reported that the document provided a clear strategic ambition and intent for Police Scotland, assessing that overall that it is fit for purpose in setting the conditions for implementation at an estimated cost of in excess of £80m over 5 years.

2.8 This work developed our high level strategy by identifying the component parts required for an effective response to the cyber challenges and a Target Operating Model. A high level presentation (appendix attached) has been provided to help inform this up update.

2.9 This is currently under consideration by the organisation and forms part of the wider change prioritisation work, coupled with the ongoing budgetary pressures. This is in full recognition that the development and introduction of new technologies requires significant financial investment and additional resource to assist with the change and transformation process. As an illustration, one software licence for a single product we commonly use, is the same cost as a police officer's annual salary.

Key Areas of Ongoing Work

2.10 Despite the associated costs in delivering technology required to tackle the threat of Cyber enabled crime, balanced against the budget landscape, it remains the ambition and priority of the PDWP to deliver a variety of products and services in a number of project areas, during the 2023/24 financial year.

2.11 With a key focus on the strands of Prevent and Pursue and with a partnership approach at the heart, the Programme is prioritising work in the following areas:

Training and Capability

2.12 This project enables us to transform Police Scotland's capacity and capability to respond to threats. The project will review and implement a full suite of Cyber Training Products from basic to advanced levels.

ISO 17025

2.13 Achieving ISO 17025 accreditation for digital forensics was outlined in the Police Scotland Cyber Strategy as key activity for the PDWP.

2.14 The project will enhance Police Scotland's existing digital forensic capability and obtain formal, internationally recognised accreditation for the digital forensic service. Work on this has commenced with the
Digital Forensic Hub at Muggiemoss, Aberdeen, to be completed within the 2023/24 financial year.

Digital Forensic Re design

2.15 Digital Forensics (DF) Re-Design is a project aligned to a DF service that all of policing relies upon and is vital to reducing harm and protecting the public. It is acknowledged that there is a requirement to review and rebuild the service to meet current and future demands.

2.16 The key objective will be to design and develop a future focussed operating model for DF where the scope of the project will incorporate people, processes, technology and estates. As such, the Programme have identified two areas in support of this future model.

2.17 DF Vans, which would be an extension and improvement on the current in force capability and Digital Detection Dogs, which are specially trained to sniff out digital devices; including mobile phones, laptops and sim cards. This would be a new capability for Police Scotland, bringing about additional capability to DF investigations across the country.

Critical Issues

2.18 This project aims to address the immediate threat, risk and harm from Online Child Sexual Abuse and Exploitation (OCSAE) and the safeguarding and protecting of vulnerable people from online crime and abuse, through the delivery of tactical solution and longer term strategic change.

2.19 The current focus of PDWP is working to introduce a solution for the Internet Investigations Unit (IIU) in the form of an analytics platform, which can be used to improve workflow, enhancing the effectiveness and efficiency in terms of the deployment of our people across Police Scotland, whilst seeking to improve their wellbeing.

2.20 The introduction of software will ensure Police Scotland is flexible, adaptable, resilient and able to respond to shifting threats. The software will provide search facilities across approximately 20 systems, identifying language and patterns which will highlight higher risk cases faster than the current manual systems.

2.21 With referrals in OCSAE increasing 511.2% between 2015 to 2021, this increased capability will improve our response to this, however given the scale and threat posed, we need to continue to embrace the technology available to help target and prevent these types of crime type, appreciating that the associated costs and the recruitment and training of specialist officers and staff.

Cyber Futures

2.22 This work stream focuses on three of the '4Ps', Protect, Prepare, and Prevent to fit with the overall Programme approach and in support of Police Scotland Strategic Objectives.

2.23 The adoption of a public health approach to aid a reduction in cybercrime and will ensure partners from a range of sectors can positively influence and support our objectives.

2.24 Examples on work ongoing in this thematic area include:

Fraud

2.25 Fraud is synonymous with online crime and over the last 5 years this has seen a 68% increase, equating to an average of 1500 crimes per month, 95% of which is online.

2.26 ACC Andy Freeburn, as Chair of the Strategic Fraud Governance Group with partners from Scottish Government, the banking and financial sector and the Scottish Business Resilience Centre (SBRC) is exploring the concept of at a multi-agency triage hub, to ensure that the public and private sector work more collaboratively and consistently in this area.

2.27 In recent months this has seen the joint production of the "Little Book of Big Scams" aimed at increasing the public's awareness and preparedness for scams within the UK, messaging of which has been reinforced in the lead up to the festive period.

2.28 In terms of the wider UK approach, Police Scotland are also participating in the development of Fraud and Cyber Crime

Reporting and Analysis Service (FCCRAS) formerly known as Action Fraud.

2.29 This is being designed to with the following collective objectives of both the victim and law enforcement:

- Improved victim experience and satisfaction,
- Lead to criminal justice outcomes,
- Prevent crime and reduce harm,
- Contribute to an improved understanding of the threat from serious and organised crime,
- Improve systems inter-operability and align with national programmes.

Scottish Cyber Co-ordination Centre (SC3)

2.30 Police Scotland is a key partner in this multi-agency project which will establish the Scottish Cyber Co-ordination Centre, a central coordination function for cyber intelligence sharing, exercising, early warning, best practice, and national incident response and recovery for Scotland.

2.31 The concept was of SC3 was announced during Cyber Scotland Week in February 2022 and will seek to become a recognised, authoritative and collaborative function to combat the accelerating threat of cyber-attack to Scotland, its businesses and people.

Governance

Police Scotland (internal)

2.32 All business cases for transformational change progress through the Investment Governance Framework. Each project reports to a Project Board, then Programme Board, progressing to Portfolio Management Group (PMG) and Change Board. The value and complexities of the project will determine the next/future governance steps, through SPA and Scottish Government.

Policing in a Digital World Professional Reference Group (external)

2.33 Police Scotland and the Scottish Police Authority's joint vision is to deliver comprehensive change to become a centre of excellence in digital and cyber policing.

2.34 Following publication of the Cyber Strategy, the focus since then has been on planning for implementation and engagement with stakeholders and the public.

2.35 The Scottish Police Authority is committed to supporting Police Scotland in building public trust through open and transparent discussion and engagement, promoting and supporting the need to build effective preventative partnerships and secure additional investment.

2.36 It is recognised that the strategy implementation and engagement plan will benefit from collaboration with key industry and public partners led by both Police Scotland and the Scottish Police Authority.

2.37 This will support strategic delivery, while offering informed expertise and effective challenge as Police Scotland progresses with implementation of this future focused strategy.

2.38 This resulted in the creation of the joint (SPA and Police Scotland) Policing in a Digital World Professional Reference Group with the inaugural meeting taking place on 22 September 2002. This is chaired by DCC Malcolm Graham and SPA Board Member Caroline Stuart, with representation from the National Cyber Resilience Advisory Board, Scottish Business Resilience Centre, Academia and the Equality and Human Rights Commission.

2.39 The positive discussions from the initial meeting helped set the agenda, inform the terms of reference and membership, helping to shape the direction of the group.

2.40 The next meeting of the Group is to take place early in the New Year (2023).

Data Ethics

2.41 Police Scotland's Data Ethics function will support the delivery of Police Scotland's Data Ethics Framework and Strategy, to ensure that the organisation has the appropriate mechanisms to identify and address ethical challenges in relation to data and data driven technology.

2.42 Police Scotland completely understand the need to ensure public confidence and appropriate safeguards in utilising such technologies, however the challenge is to balance this against our

statutory obligations in keeping the public safe, whilst making best use of available technologies to assist us in this mission.

2.43 A new Data Ethics Triage process has been implemented that will assess all data related and data driven technology projects that go through Police Scotland's Change process.

2.44 The triage process will identify where ethical challenges may lie, provide a pathway to enhanced internal and external scrutiny and provide advice to projects to ensure that data and data driven technology is used legally and ethically.

2.45 The work of the joint Professional Reference Group with SPA will be key to this and help shape our approach and direction.

3. FINANCIAL IMPLICATIONS

3.1 There are significant financial implications in this report. As outlined previously the work carried out by PwC estimates a cost of in excess of £80m over 5 years to deliver the capabilities required to meet the Cyber Strategy. A modular approach will be adopted by the programme to facilitate delivery within the available resources per financial year.

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

3.3 The Programme is subject to the ongoing prioritisation exercise and in year halt in reform spending. Once the outcomes of both these exercises are known, re-planning and baselining can take place.

4. PERSONNEL IMPLICATIONS

4.1 There are personnel implications in this report. Additional Programme resources are required to deliver next stages. 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.

5. LEGAL IMPLICATIONS

5.1 There are no legal implications in this report.

6. REPUTATIONAL IMPLICATIONS

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

7. SOCIAL IMPLICATIONS

7.1 There are no social implications in this report.

8. COMMUNITY IMPACT

8.1 There are no community implications in this report.

9. EQUALITIES IMPLICATIONS

9.1 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 issues within relevant EQHRIA and DPIAs.

10. ENVIRONMENT IMPLICATIONS

10.1 There are no environmental implications in this report.

RECOMMENDATIONS

Members are invited to discuss the update in the PDW Programme.

SPA – Policing Performance Committee

POLICE SCOTLAND
POILEAS ALBA

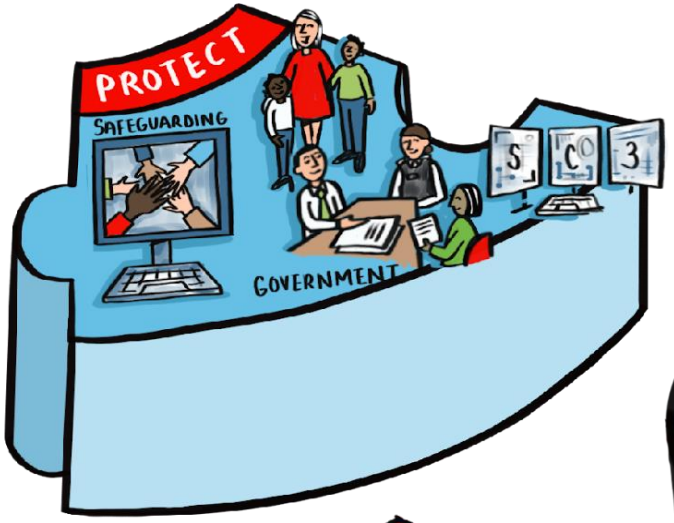
Cybercrime is risking exponentially, especially Fraud and OCSAE

- 511% increase of Online Child Sexual Abuse and Exploitation (OCSAE) referrals from 2015-2021.
- 650% increase of referrals regarding child sexual abuse imagery over a 9 year period.
- 17% increase of fraud was recorded in the past 12 months, with a 68% increase over the last 5 years.
- Average of 1500 crimes per month, 95% of which is online.

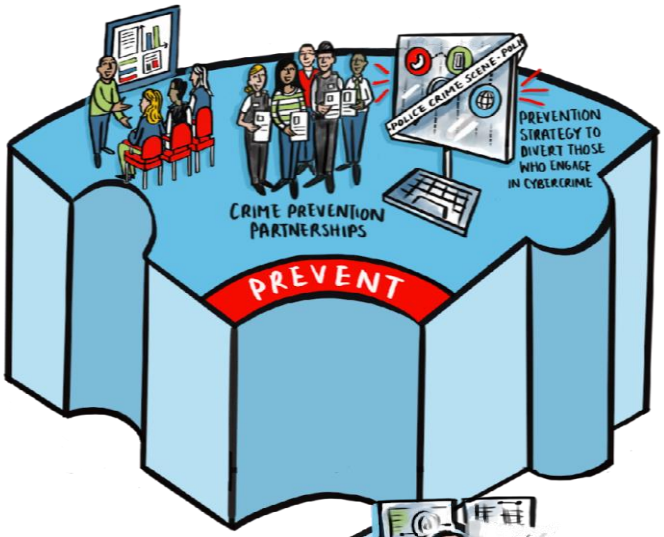
Key target outcomes:

1. Optimised collaborative relationships with Partners,
2. New and enhanced capabilities,
3. Improved tasking of our highest threats,
4. Shifting to a new policing model that is needed for the 21st century
5. Enhanced technology, driving integration, informing decision making, and enabling seamless internal and external collaboration,
6. An equipped and enabled Police Service.

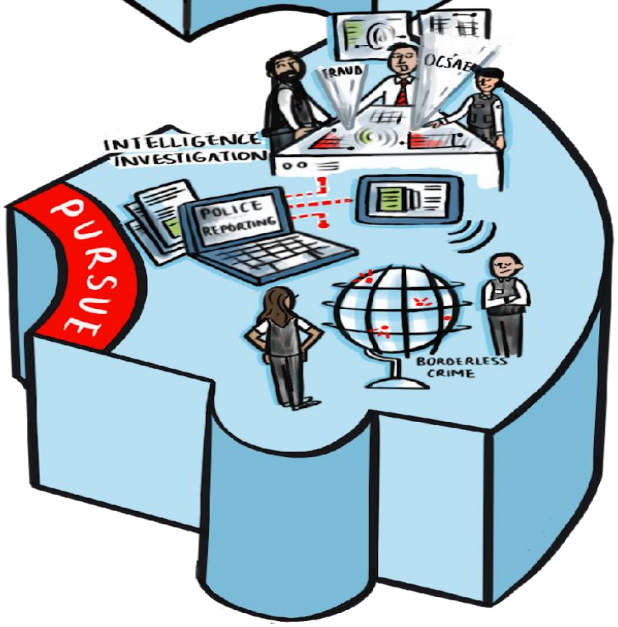
Programme approach

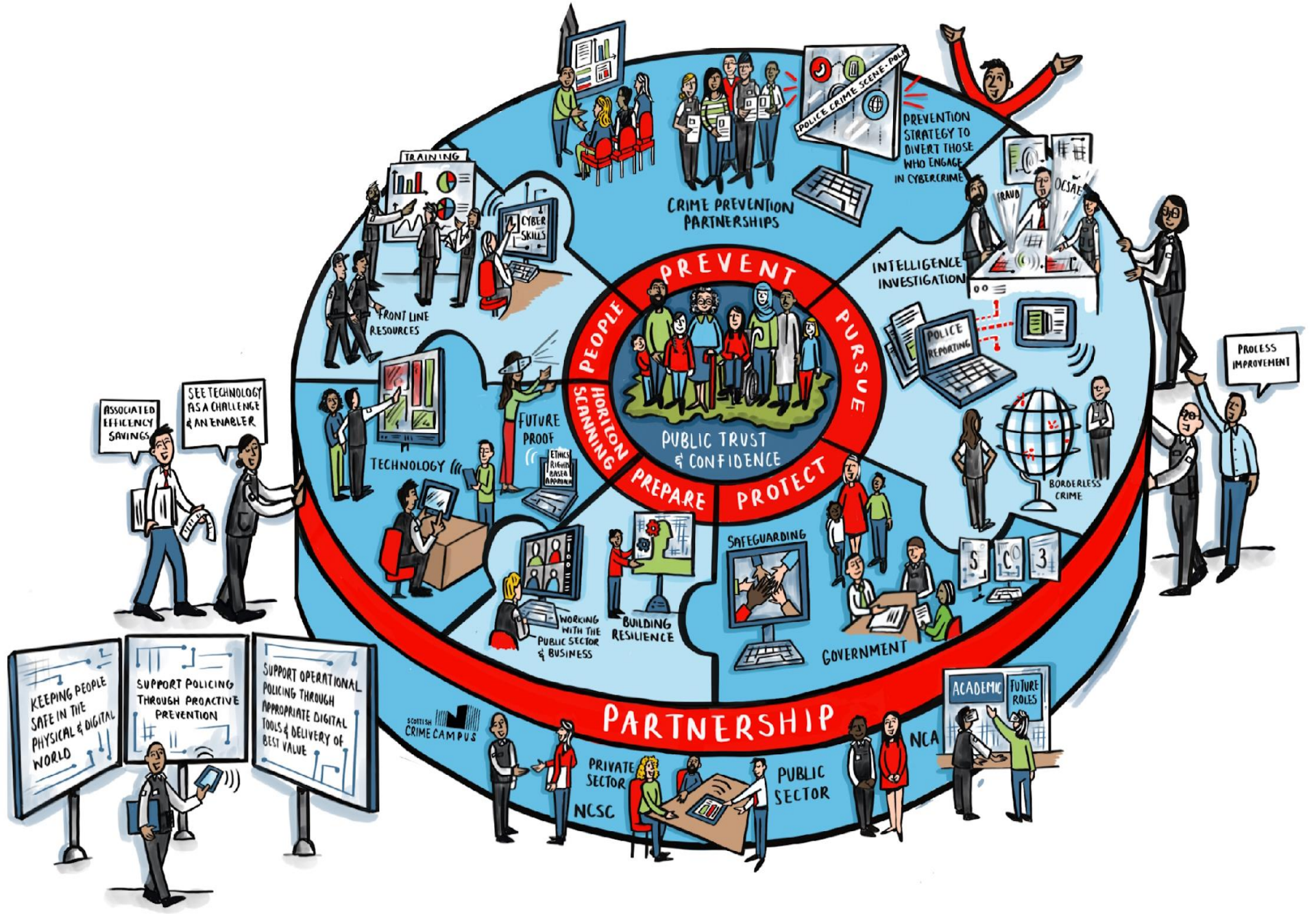


Public at the Centre



Partners Wrapped Around




PREVENT
PURSUE
PROTECT
PREPARE
PEOPLE
HORIZON SCANNING
PUBLIC TRUST & CONFIDENCE
CRIME PREVENTION PARTNERSHIPS
POLICE CRIME SCENE - DO NOT CROSS
PREVENTION STRATEGY TO DIVERT THOSE WHO ENGAGE IN CYBERCRIME
TRAINING
CYBER SKILLS
FRONT LINE RESOURCES
INTELLIGENCE INVESTIGATION
FRAUD
OCSAE
POLICE REPORTING
PROCESS IMPROVEMENT
ASSOCIATED EFFICIENCY SAVINGS
SEE TECHNOLOGY AS A CHALLENGE & AN ENABLER
TECHNOLOGY
FUTURE PROOF
ETHICS RIGHTS BASED APPROACH
BORDERLESS CRIME
WORKING WITH THE PUBLIC SECTOR & BUSINESS
BUILDING RESILIENCE
SAFEGUARDING
GOVERNMENT
S
C
3
KEEPING PEOPLE SAFE IN THE PHYSICAL & DIGITAL WORLD
SUPPORT POLICING THROUGH PROACTIVE PREVENTION
SUPPORT OPERATIONAL POLICING THROUGH APPROPRIATE DIGITAL TOOLS & DELIVERY OF BEST VALUE
SCOTTISH CRIME CAMPUS
PARTNERSHIP
ACADEMIC
FUTURE ROLES
NCA
PRIVATE SECTOR
PUBLIC SECTOR
NCSC