Northumbria Police and Crime Panel	**16 January 2018**
Cyber-Crime: Report for the Police & Crime Panel	
Report of Northumbria Police - D/Superintendent 7947 Michael Barton	

1. PURPOSE

To provide the police and crime panel with a themed report in relation to the police response to cyber-crime.

2. BACKGROUND

The response to cyber-crime is applied in line with the 2013 HM Government Serious & Organised Crime Strategy strands of ‘Protect’, ‘Prevent’, Prepare’ and ‘Pursue’ – often referred to as ‘the 4 P’s’.

This provides for a structured approach to crime prevention, diversion of potential offenders, readiness / capability, and bringing offenders to justice.

The North East Regional Specialist Operations Unit (NERSOU) have recently recruited a dedicated team of officers and staff to coordinate cyber ‘protect’ and ‘prevent’ work across the 3-force region, and Northumbria Police have excellent connectivity with that team.

3. ‘PROTECT’

‘Protect’ is crime prevention and due to the nature of cyber-crime, this work is vitally important as bringing offenders to justice in a traditional policing context (e.g. such as we do when we experience a rise in acquisitive or violent crime) is simply not always possible due to the scale and nature of the criminality.

It has often been said that law enforcement agencies will not ‘arrest & detect’ their way out of this problem hence it becomes all the more important to protect those people and businesses that are vulnerable to being targeted.

This has led to concerted and coordinated efforts by Northumbria Police and the NERSOU to structure activities across the force area to try and mitigate the risks to a wide range of potential victims including children, vulnerable adults, local business, and the public sector.

Highlights from 2017 / early 2018 include:

- ✓ Cyber Volunteer Programme. A strong programme has been developed using 21 cyber volunteers who come from a range of diverse ICT backgrounds. The team will be used to assist local businesses in protecting their IT systems from attack, offering investigative advice to officers, assisting the ICT department with internal information security and complete themed project work to protect vulnerable victims whilst on-line.

- ✓ ‘Operation Signature’ (supporting vulnerable victims of cyber-crime and fraud) is now live across the force and in support of this approach all NPT’s are receiving training via a package devised and produced by People Development. This is a huge step in our approach to consistently assessing vulnerability, victim needs, and preventing further offending.

- ✓ ‘Get Safe On-line’. This is a public / private sector partnership supported by HM Government and leading organisations in banking, retail, internet security and other sectors. Implementation of the national cyber-protect programme and access to on-line advice and structured national campaigns / local events with a completed 2017 programme and an agreed programme ready for delivery throughout 2018.

- ✓ Cyber Business Breakfasts being held at St James' Park and the Stadium of Light during early 2018. These are free for businesses to attend, during which NERSOU officers will demonstrate a live hack into a website, showing how cyber criminals find and exploit IT weaknesses. This then leads into cyber volunteer service and how they would have identified this weakness, giving businesses the opportunity to get upstream of the attack and mitigate the vulnerability.

- ✓ On-going business engagement to grow membership of the Cyber Security Information Sharing Partnership (CiSP). The CiSP is a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business.

- ✓ Cyber-crime security survey. The 3 regional forces and OPCC's have coordinated with the Institute of Directors and the Federation of Small Businesses, a cyber-security survey with a view to identifying the vulnerability of local businesses to allow targeted engagement for the delivery of protect advice – such as cyber essentials accreditation.

- ✓ Mitigating the threat and vulnerabilities of children to Online Child Sexual Exploitation (OLCSE). There is extensive partnership work taking place that includes Safetyworks!, Get Safe Online events, Neighbourhood Policing Team inputs, and collaboration with Creative Fuse – a mixed economy of academics from five local universities who have been challenged with not repeating 'protect' messages, but shaping the behaviour of children on-line in order to stay safe.

- ✓ Continued use of the police cadets and mini police to deliver peer to peer messaging in their school environment. Notable is that one of our mini-police recruits devised a poster that is now being use nationally by Get Safe Online and received an award from their Chief Executive.

4. <u>'PREVENT'</u>

'Prevent' is centred upon identifying those individuals who are at risk of being drawn into cyber-crime and engaging with them to divert them accordingly. This is a developing area of work, and one that NERSOU has already made significant progress with.

Prominent areas of progress and plans for 2018 include:

- ✓ Cyber Prevent Workshop – NERSOU is one of only two regions who are hosting a prevent workshop at Northumbria University in March, alongside Cyber Security Challenge, NCA and industry partners. The aim of the workshop is to invite 16 nominals who are at risk of engaging in cybercrime, with their parents, giving workshops on coding, careers and legal, moral and ethical implications of cybercrime.

- ✓ Schools referrals – schools are a key pathway into cyber prevent, as many young people experiment with school networks. During 2018, the 'prevent' team seek to raise awareness in this sector to increase referrals to the team.

- ✓ Diversions / coding clubs – the team intend further scope and identify coding clubs in area. The 'prevent' team have attended a Coda Dojo in Gateshead where young people are taught coding and ethical hacking. It's important that in such environments relationships are built and education / diversion take place.

✓ Gaming – a known like exists between gaming and cybercrime. Prevent team to attend retro gaming event in June 2018 at Gateshead.

✓ The National Crime Agency (NCA) actively identifies individuals who are demonstrating a low level involvement in cyber-crime (hacking forums etc.) where prosecution is not appropriate. The coordination of the 'cease and desist' letters is part of the 'prevent' teams' responsibility.

✓ The team have already begun to identify and intervene with young people in the cusp of such offending. This has included delivery of a conditional caution to compel an offender to work with the prevent team, and another case where an offender is engaging in a restorative justice approach in speaking to, and helping businesses understand the threats posed to them.

5. 'PREPARE'

In context of the 4 P's, 'Prepare' is about ensuring that we have the necessary capabilities to respond to cyber-crime incidents, and to provide those affected by cyber-crime with effective criminal justice and victim support.

In respect of force capability to investigate cyber dependent (computer misuse) offences such as malware, ransomware, denial of service attacks etc. we subscribe to the minimum standards as outlined by NPCC in that we have 1 D/Sgt, 2 DC's, and 1 Researcher trained. Demands placed upon the force to conduct such investigations are, as it stands generally limited and any offences that require a more specialised approach can be readily allocated and dealt with by NERSOU or the NCA – both of whom have dedicated teams trained to investigate higher level / more complex offences.

In terms of tackling OLCSE we do have a Paedophile Online Investigation Team (POLIT) that has increased significantly over the last 6 months to include additional supervision, detectives and victim ID staff. This has also coincided with all trainee detectives being allocated low risk indecent image investigations which delivers valuable learning for trainee investigators across the force.

The demands placed upon the unit in relation to OLCSE is constantly monitored and as we progress through the next 12-18 months, the capability (i.e. the size) of the team will require on-going review due to the increase in demand that is emanating from more complex and wide ranging enquiries, the use by offenders of new platforms, the increased demand from the NCA, the expected increase in work from the NERSOU (undercover) uplift, and the on-going demands placed upon us by internet vigilante groups.

In terms of our wider approach to the investigation of cyber-crime, there are many positives to report in terms of increased / improved capability, and the last 6 months has cemented our position as being a force at the front of delivering digital policing capabilities. We are in an enviable position, supported by headlines that include:

✓ Implementation of Digital Evidence Suites. Enabling front-line officers to self-service for basic digital forensic examination of mobile telephones, CCTV and Body Worn Video (BWV). Huge take up of mobile phone examination and CCTV processing resulting in less demand for specialist investigations and quicker turnaround / submission of evidence.

✓ Re-structure of the Digital Forensic Unit (DFU) enabling a more efficient service and backlog reduction. At the end of 2016 the backlog stood at circa 14 months. It is now (within 12 months) circa 12 weeks and reducing further.

- ✓ Within the DFU, installation of a secure storage area network and imaging / pre-processing facility which creates efficiency, will support in-sourcing, and underpin ISO 17025 requirements.

- ✓ Phase 2 of the Digital Media Repository (DMR) now operational. Sharing of multimedia evidence to CPS is now in place.

In terms of the skills of our staff, whilst notable progress has been made in respect of operational staff completing the College of Policing mainstream cyber-crime training modules, there is further work to complete during 2018. Force capability to conduct covert open source research, deliver a professional digital media investigator resource, and ensure the whole workforce is equipped with the constantly evolving digital skills they need to investigate various levels of cyber-crime are issues that require on-going prioritisation.

The North East Transformation Innovation and Collaboration (NETIC) cohort of the 7 regional forces has recently held a cyber-crime symposium and agreement has been reached between Chief Officers and PCC's that collaboration should invigorate and underpin our approach to selected cyber-crime specialist capabilities. Linked to the paragraph above, notable areas for collaboration do include research and development and training.

Lastly, in terms of 'preparedness' it is vital that we test our internal resources appropriately to ensure that we respond efficiently and effectively should a cyber-attack occur that poses risks to our or another agencies IT infrastructure. As such there are several 'tests' planned for 2018 that include:

- ✓ A Local Resilience Forum (LRF) cyber exercise during the first quarter of 2018.
- ✓ Silver Commander 'Hydra' (immersive learning) training at Follingsby Park.
- ✓ Regular internal security tests such as the use of 'phishing' emails.

6. 'PURSUE'

As the title suggests 'Pursue' is concerned with the arrest, detection and prosecution of those committing cyber-crime and within those investigations ensuring that any identified victims are safeguarded.

6.1 Cyber Stalking & Harassment

Cyber stalking and harassment is a crime which is hugely debilitating and devastating for a victim and often underlying such offences is other equally serious domestic abuse and controlling / coercive behaviour. We recognise that identifying what at times can be obvious, but at other times hidden or subtle behaviour by the offender by his/her use of technology is crucial in understanding and mitigating risk.

It is with this in mind that Northumbria Police, with the support of the Violence against Women & Girls (VAWG) funding allocated to the Office and the Police and Crime Commissioner are beginning to develop an improved approach to tackling cyber stalking and harassment. A pilot in Sunderland Local Authority area will see a team of specialist officers alongside a specialist domestic abuse support worker from Wearside Women in Need deliver a comprehensive response to all allegations of cyber stalking and harassment. This includes full responsibility for investigation and victim support in those cases that are wholly or substantially based upon on-line / cyber stalking or harassment, and providing advice to other investigators and first responders with a view to maximising evidence gathering at the earliest opportunity. The team will also provide training for other Northumbria Police officers, support and guidance for local specialist services, and awareness raising materials for victims, their friends and family, and members of the public.

The police team will consist of a detective supervisor, and officers who are domestic abuse specialist investigators as well as those who have been trained in open source and digital media investigation. This will ensure that the police will be able to recognise the digital forensic opportunities that are present with such cases and maximise the evidence collection opportunities. As this takes place, the risks that are present with the individual allegation will be considered by careful analysis of the background that is present in each case to ensure that a full understanding of the issues is achieved. This will not only enable the best possible chance to bring the offender to justice, but crucially to help the police and the specialist domestic abuse support worker to identify risks and put in place partnership plans to mitigate them. In essence this is a complete and professional approach to delivering a rounded and inclusive multi-agency response for every identified victim.

6.2 Northumbria Police POLIT & OLCSE

The work of both Northumbria Police and NERSOU in this regard is extensive and it could be the subject of an entirely separate paper. That being the case, the following update is provided to share the context of the 'pursue' work, the extent of the activity, and some highlights from 2017.

As it has for all of 2017, the force response to online child sexual exploitation (OLCSE) remains in excess of the expectations / minimum standards of NPCC in that we extensively target offenders who proactively share indecent images of children (IIOC). During 2017 POLIT have taken enforcement action against no fewer than 220 offenders.

Within this cohort of offenders there has been some very prominent cases involving predatory paedophiles who have committed the gravest of crimes all over the world. The recent imprisonment of Paul Leighton and his anticipated extradition to the USA demonstrated some outstanding joint working with Homeland Security and the FBI to protect victims as far afield as Canada, Australia and the across several states in the USA.

In Northumbria we are also bear the demands placed upon us by 2 very active internet vigilante groups, and during April 2017 our approach in dealing with them received the upmost scrutiny in the High Court. It was very pleasing that the policies and processes adopted by Northumbria Police were beyond reproach and as a result we are now being consulted on the formulation of revised national policy.

The cyber-crime unit remain connected to the child abuse image database (CAID) and grading / upload / contributions to CAID are suitably performance managed by the digital forensic unit (DFU) manager. We perform well in this area with no cause for concern.

The work of the Victim ID police staff is also showing very encouraging signs despite being a new role, and having been devised largely 'in-house' as national guidance and training was very limited. This is a vital role in connecting IIOC with victims to deliver safeguarding interventions and that being said it is pleasing to be able to report the following from the first 3-4 months:

- ✓ The Victim ID staff are also connected other forces and the NCA.

- ✓ They are being tasked by the POLIT supervision with cases identified by the DFU as potentially containing first generation IIOC and those which involve multiple victims.
- ✓ Processes have been established for national dissemination of Victim Identification bulletins.

✓ Early notable outcomes include:

- A child identified in the force area based upon intelligence from South Yorkshire. Child identified by school badge and safeguarding implemented by local NPT.

- Op Muster – Investigation into widespread internet based grooming and use of live streaming – to date 400 identifiable victims have been catalogued and the officers are applying an identification strategy which has already seen 6 child victims identified and safeguarded within the UK.

- 2 child victims identified relating to other POLIT work which has led to 1 UK victim being identified and safeguarded and a further dissemination to Austria via an Interpol referral.

In short, Victim ID officers are quickly establishing themselves as an important interface and function in the response to OLCSE. They are definitely improving our response in conjunction with law enforcement agencies across the UK and beyond, and ultimately identifying victims of abuse that would have previously been left vulnerable.

6.3 NERSOU & OLCSE

NERSOU report that the threat from OLCSE, in the main stems from social media applications such as 'Snapchat', 'WhatsApp', 'Kik', 'Instagram' and 'Facebook'. Data obtained outlines that in 68% of cases the offender incites the sharing of indecent content, and in 32% of crimes, the offender attempts to facilitate contact offending.

NERSOU has recently been provided with funding to deliver a significant uplift in Under-Cover on Line (UCoL) capability, and it is this offending profile that drives the undercover policing activity within the unit who are at present actively supporting several live CSE investigations across the region.

Not unlike the Northumbria response, the NERSOU activity is extensive, and the following cases are highlighted as how the unit is actively identifying very high risk offenders and safeguarding children:

✓ Op Marva, an online grooming investigation that secured evidence of a perpetrator grooming the online profile of a 14 year old male, engaging in sexualised chat and sending indecent videos to the 'child'. The male has subsequently been identified as a male from the Northumbria force area who coaches a girl's U14 football team. The male has been arrested and safeguarding has been addressed by local officers.

✓ Further investigations secured evidence of a male who was grooming the online profile of a 14 year old girl. The male was identified as residing in the London area with his wife and 2 small children. The male was employed as a primary school teacher in a mixed sex school.

✓ Another investigation of a very similar nature also identified a male engaging via an online teen chat site. This male was identified as a retired headmaster, who was also a Government Policy advisor, regular BBC contributor and member of National Association of Head Teachers.

✓ NERSOU staff has ensured that evidence has been disseminated to support the arrests of these males and all safeguarding has also been dealt with locally.

7. RECOMMENDATION(S)

Members of the police and crime panel note the content of the report.