UNIVERSITY OF LIVERPOOL

School of Law and Social Justice

TACKLING DIGITALLY ENABLED COERCIVE CONTROL

Antoinette Raffaela Huber
Barry Godfrey

N8 RESEARCH PARTNERSHIP

Contents

UNIVERSITY OF LIVERPOOL
TACKLING DIGITALLY ENABLED COERCIVE CONTROL

What is Coercive Control?

Coercive control, which often occurs in domestic abuse contexts, was criminalised within the UK in 2015 under section 76 of the Serious Crime Act (Home Office, 2023). Under this Act, a person is guilty of coercive control if they repeatedly or continuously engage in behaviour towards another person that is controlling or coercive; if at the time of the behaviour, they are personally connected; if the behaviour has a serious effect on the victim, or they should have known that their behaviour would have a serious effect on the victim. Their behaviour has a serious effect if it causes the victim to fear, on at least two occasions, that violence would be used against them, or if it causes serious alarm or distress which has a substantial adverse effect on the victim's usual day-to-day activities.

A common characteristic of coercive control in a domestic context is the generation of fear to ensure compliance or entrapment of the victim-survivor. For example, Women's Aid (2024) describes coercive control as "a pattern of acts of assault, threats, humiliation and intimidation or other abuse that is used to harm, punish, or frighten their victim". They also stress that fear impacts upon every aspect of victim-survivor's lives, limiting their human rights and personal freedoms. This is reinforced by Stark (2007:4), who explained that control "prevents women from freely developing their personhood", causing victim-survivors to become isolated, regulated, and ultimately 'trapped'. Refuge (2022) identifies coercive control as a key indicator for domestic homicide, with more than half of those killed by a current or former partner being previously subject to forms of coercive control.

What is Digitally Enabled Coercive Control (DECC)?

Digitally enabled coercive control sits under the umbrella term of 'technology-facilitated domestic abuse' which includes the use of, but not limited to, "surveillance, global positioning system (GPS), tracking, impersonation, doxing, computer hacking, restricting access to technology, and image-based sexual abuse" (Henry et al., 2023: 1206-1207). The use of technology to facilitate abuse and forms of domestic violence is common. Women's Aid (2014) identified that 48 percent of women reported experiencing online abuse within domestic abuse contexts. Refuge (2020) reported that 72 percent of its service users experienced technology-facilitated abuse, with interviewees experiencing emotional abuse (82%), harassment/stalking (82%), monitoring (71%), coercive control (59%), access/control of bank accounts (47%), location tracking (41%), threat of violence (41%), economic abuse (35%), impersonation (29%), intimate image abuse (29%), and doxxing (18%) (Refuge, 2022).

Whilst research focusing upon DECC remains limited, it is certain that, as with all forms of domestic abuse, coercive control has been fundamentally impacted by technological advancement, making coercive control more pervasive and easier to perpetrate. For example, increased connectivity removes the need for the victim and offender to occupy the same space, increasing the sense of abuser omnipresence (Powell et al., 2018) and leaving victim-survivors with no reprieve. Victim-survivors are now always contactable and can be subject to continuous monitoring. Technology has also changed some of the ways in which coercive control manifests itself. For example, although the Refuge (2020) report noted that Facebook, Instagram and WhatsApp are the most commonly used platforms to perpetrate abuse, DECC is now facilitated by a multitude of software and devices which are becoming increasingly complex and difficult for victim-survivors and police forces to identify.

Policing responses to modern forms of abuse need fundamental improvement if police forces are to adequately identify and respond to digital forms of victimisation (Harkin and Whelan, 2022; Horsman, 2017; Todd et al., 2021; Wilson-Kovacs, 2021). This includes being able to identify cases of DECC correctly, identify and undertake digital forms of evidence collection, and provide appropriate interpersonal responses to victim-survivors (Barlow et al., 2020; Horsman, 2017; Huber, 2022; Todd et al., 2021; Wilson-Kovacs, 2021). This report explores how police forces can better respond to the growing DECC problem, and for the purposes of the study, we define DECC as coercive and controlling behaviour which is facilitated by any form of digital technology.

UNIVERSITY OF LIVERPOOL
TACKLING DIGITALLY ENABLED COERCIVE CONTROL

Research Design

The research comprised statistical analysis of police data and interviews with stakeholders. Three northern police forces took part in the study, two of which provided data on reported incidents (see reported incidents data section for more information), and all forces participated interviews. A range of police officers and staff were interviewed across the forces (n=26) including call handers, response officers, detectives, and digital specialists. These interviews provided information on the challenges faced by police forces and by police officers at various career stages when responding to DECC, as well as areas of good practice and discussions about existing training provision.

Stakeholders from the Third Sector (n=6) were recruited via email and interviewed about their knowledge of victim-survivor experiences of DECC and policing responses. Inclusion of the third sector, specifically those who have supported multiple victim-survivors, allowed us to build a more generalized picture of policing responses. Victim survivors (n=13) were mainly recruited with the assistance of third sector agencies, and some responded to information provided on the University of Liverpool website. Inclusion of victim-survivors provided first-hand experience of policing responses[1], distinctive insights into what constitutes effective practice, and ensured the service recipients of the criminal justice system were given a voice.

1 We were not able to recruit victim-survivors from our partner forces, so experience of victim-survivors did not always reflect the experiences of the partner forces.

Reported Incidents Data

Police Force 1 supplied details of cases (n = 270) of domestic abuse (DA) with digital element(s) reported between 1st June 2023 and 30th August 2023. The data included details of the date of the incident; offence group; gender, ethnicity, age of suspect and victim; suspect and victim relationship status, Home Office outcome code, whether the suspect was known to police, whether the case had been reviewed by the Crime Management Support Unit, and a free text description of the incident. We analysed the data, recording frequencies, and created additional analytical variables using the free text description as data: Was there a digital element evident? Was there evidence of coercive and controlling behaviour? Was there evidence of digitally enabled coercive control? Was there more than one incident reported for that day for the people involved? Was there a sustained pattern of domestic abuse? Was violence used or threatened in the incident? Analysis of data supplied by Police Force 1 established that:

- A fifth of offenders were female and four-fifths were male. Eight out of ten victims were female; and a fifth of victims were male.
- Three-quarters (77%) of offenders self-defined as White British. It is likely that many of those whose ethnicity was not defined were also White British, as officer-defined ethnicity for offenders was 84%.
- The suspect/subject was recorded as known to police in approximately a quarter (26%) of incidents.
- The vast majority (84%) of cases were recorded as offences against the person; 6% were recorded as frauds; 3% as thefts. The remaining 6% included burglary and theft, public order, sex offences, and miscellaneous/other.
- Nearly half of cases involved the threat (31%) of or use of violence (16%).
- In approximately 30% of cases, there was only one incident, but in 70% of cases, there were more than one incident on the day of the occurrence. In over half (53.7%) the cases involved incidents that took place on more than one day.
- Approx a fifth (58) cases were identified as having a digital element which did not seem to merit the marker. For example, cases where the only offence was that the victim had been hit on the arm with a mobile phone for example, or where the suspect had "stolen the victim's bank card to withdraw money from an ATM". It may be that there was a digital element in these cases, but the text was not sufficiently detailed enough for us to identify it.
- There was no evidence of coercive and controlling behaviour in nearly 40% of recorded incidents, and it was not possible to state with certainty whether coercive control was present or not in 30% of incidents (as recorded in the officer notes).
- Incidents which involved both a digital device in the commissioning of the offence and evidence of coercive and controlling behaviour (DECC) constituted 29% of cases:

"The victim and suspect used to be in a relationship. They have briefly got back together and have ended the relationship again in May 2023. Since the 28th May 2023 the victim has been receiving numerous messages and calls from the suspect demanding money, and being generally unpleasant. The victim has replied back saying to leave her alone, which the suspect ignored. The victim has then blocked the suspect on the phone, and the suspect would then continue messaging using alternate messaging software. When the victim blocked him on those also, he has started to use other people's social media to contact the victim." It may be that this percentage should be higher as, in approximately a quarter of cases (27%) it may have been possible to identify DECC if the data had been higher quality.

- Seven per cent of cases were recorded as reviewed by the Crime Management Support Unit.
- By far the most common outcome for incidents (60%) was HO16 (the prosecution did not proceed because, although a suspect was identified, the victim did not support the prosecution). The second most common outcome was HO15 (where the suspect was identified, and the victim did support prosecution, but there were other evidential difficulties). These constituted 17% of all recorded cases. Approximately 7% of cases resulted in a charge/summons.

Police Force 2 provided data on all cases of coercive control in an intimate family relationship (stalking and harassment) reported between 1st September 2022 and 31st October 2022 (n=187). The data contained details of date and location of incident; whether it was domestic in character; whether drugs/alcohol were involved; the Home Office outcome code and free text which allowed us to run our analysis of whether there were elements present that indicated coercive and controlling behaviour or digitally enabled coercive control.

- The majority of incidents occurred within a dwelling (83%); one took place in a prison; and 14% of incident locations were unrecorded.
- 8% were recorded by police as non-domestic in character.
- 22% of incidents involved drug use; 13% alcohol misuse; and approximately 5% involved both drugs and alcohol.
- Of these 187 cases, 5 cases (3%) had been marked by police as digitally enabled. Our assessment of the data supplied by Police Force 2 was that there were 39 cases in this sample which contained a digital element (21%)
- Of the 187 cases we assessed that 9 (5%) did not contain a coercive and controlling element, and another 7 cases (4%) may or may not have but the free text data did not allow us to make a determination.
- We assessed that there were 39 DECC cases in the dataset including the following: "Victim is seeking to end her relationship and leave the home she shares with her husband. She does not have a source of income and feels socially isolated therefore planning to leave is understandably daunting and stressful. She has attempted to end her life on a number of occasions and has attended hospital as a result. She feels she does have reasons to live and has several children and grandchildren however her home life makes it difficult to keep going. She is restricted in her movements and says her activity is tracked. There is a tracker in her car which she cannot remove, and her husband checks her phone, if there is a number on her phone, he will call it to see who she has been communicating with, therefore victim communicates via email. Constantly monitors her phone and will always know where her car is due to the tracker that is installed."
- There were 21 cases where the offence could have been digitally enabled, but the free text data was not sufficient to decide for certain.
- 68% of the 187 cases resulted in HO16 outcomes (the prosecution did not proceed because, although a suspect was identified, the victim did not support the prosecution); and 22% in HO15 (where the suspect is identified, and the victim does support prosecution, but there are other evidential difficulties); 4% of incidents resulted in a charge/summons.

In analysing the data, it should be noted that some statistics may be artefacts of the compilation of data. For example, officers attending incidents may not have recorded sufficient detail to enable, coercive control to be identified, or stated whether a digital device was involved in the incident. They would therefore not be coded by us as DECC; however, they may well have been pursued and investigated as DECC by police. Ideally, we would have wished to analyse a large sample of cases of domestic abuse across time to examine which had been identified as having either an element of coercive control, a digital element, and/or both; follow cases through to conclusion and final criminal justice outcome; and to have interviewed a sample of officer/victims involved in various cases which were/were not identified as DECC. Future research of this kind would be invaluable.

UNIVERSITY OF LIVERPOOL
TACKLING DIGITALLY ENABLED COERCIVE CONTROL

Victim-survivor experiences

Interviews with police forces, third sector and victim-survivors identified range of technologies being used to facilitate coercive control. Whilst most participants identified use of smart phones as being the most common, other devices included iPads, AirPods, Apple AirTags and other tracking devices (including aftermarket AirTags with no warning functionality), iPads, Ring doorbells, digital watches, Amazon Alexa, and other smart devices in the home (such as Hive heating devices). In terms of software, social media (e.g. Facebook messenger), WhatsApp and text messages, were commonly identified as key facilitators as well mirroring apps and tracking apps (e.g. Find my Phone, car tracking apps or maps, and location settings in apps such as Snapchat). Some tracking apps can be downloaded onto victim-survivor phones disguised as everyday apps such as calculators so that they remain undetected. Participants also identified the use of cloud syncing as a means to monitor digital activities, whether that be hacking into the victim's Apple ID or the abuser setting up the victim-survivor's devices with their own Apple ID which they can then access anytime.

Although not an exhaustive list, using the digital devices and software listed above, DECC took the form of:

- Harassment (e.g. constant bombardment of electronic messages and phone calls, messages and phone calls from the perpetrator's family/friends, posting messages about or threatening the victim-survivor directly and indirectly on social media. Threats used to ensure victim-survivors stay in a relationship or behave in a particular way (i.e. threatening to share intimate images, including to the family courts), threats of violence and criminal damage, and threats of suicide by the perpetrator).
- Digital deprivation/restriction (e.g. not allowing the victim-survivor access to digital devices or software, such as social media, using smart devices in the home to restrict or control heating, lighting and other electronics in the home).
- Stalking/monitoring – (e.g. putting trackers on cars, use of live location information, hacking cameras in the home, placing tracking apps on the victim-survivors phones, checking the victim-survivors' phones, placing tracking apps on children's devices in shared custody situations, logging into victim-survivor accounts externally including Apple ID or other cloud storage, the use of parcel deliveries where perpetrators send parcels to addresses in the local area and use the photo taken by delivery companies for delivery confirmation to identify victim-survivors' correct addresses in post separation contexts, and tracking victim-survivor activities on apps such as Spotify and Discord which display activity information such as the music they are listening to and gaming time.
- Accessing the victim-survivor's data (e.g. Cloud syncing, hacking, changing passwords to lock victim-survivors out of their own accounts, generating search history results from Amazon Alexa).
- Image-based Abuse **–** (e.g. non-consensual taking, making and sharing or threatening to share intimate images).
- Financial abuse **–** (e.g. denial of access to money, denial of access to bank accounts, stealing money, removing money from joint accounts, signing victim-survivors up to subscription services).

All of the above can be used as a means to manipulate and control a victim-survivor either directly or indirectly. Whilst constant abuse via mobile phones and threats of violence are often direct attempts to control victim-survivors, perpetrators will also use information gathered through monitoring to manipulate the victim-survivor into feeling trapped. For example, a perpetrator may tell a victim-survivor that they know where they have been, what they have done, and who they have spoken to throughout the day. Often the victim-survivor will restrict their own behaviour, for example not visiting family and friends, to avoid confrontation, questions, or further abuse as response to behaviour deemed inappropriate by the perpetrator. It is also worth noting that some victim-survivors identified the use of devices being used by their abuser from prison demonstrating that imprisonment is not a protective barrier against coercive control for victim-survivors. Participants in the study also noted that digital and non-digital forms of abuse often combined together. Non-digital forms they mentioned included:

- Physical violence (i.e. assaults and threat of violence)
- Criminal damage to property
- Use of children (i.e. manipulating children to divulge information in post-separation contexts, preventing children from speaking with victim-survivors when they are in the custody of the abuser, coercively controlling the children themselves, including preventing them from learning or engaging with schoolwork)
- Restriction of access and/or choice (i.e. control over what the victim-survivor wears, where they can go, removing/hiding aids from disabled victim-survivors e.g. walking sticks)
- Harassment and stalking (i.e. turning up at the victim-survivor's address, following victim-survivors and their families)
- Isolation (i.e. isolating victims from family and friends)

UNIVERSITY OF LIVERPOOL
TACKLING DIGITALLY ENABLED COERCIVE CONTROL

Challenges

The use of digital devices in coercive control provides digital lines of inquiry for investigation. Digital lines of inquiry provide opportunities to contextualize interactions between victim-survivors and their abusers and can provide more objective evidence of perpetrator behaviour. For example, when abusers gain remote access to victim-survivor's accounts, an IP address can be used to help identify location (and subsequently the abuser), if an abuser attends a victim-survivors' home and their phone automatically connects to the WiFi, a download of the router can be used to prove their attendance at the address, and so on. However, the ability to take advantage of these lines of inquiry is significantly dependent on the knowledge and decision-making of the officer who first attends to the incident, the ability of officers to pursue digital lines of inquiry, and back-office support to continue the investigation.

UNIVERSITY OF LIVERPOOL
TACKLING DIGITALLY ENABLED COERCIVE CONTROL

Identifying DECC on first contact

There was a consensus amongst officers from all three police forces that coercive control legislation was difficult to apply in practice. It was not always understood by officers first attending an incident and there was a need to improve knowledge amongst officers of how coercive control can present to victim-survivors and to officers. Even when coercive control was suspected, officers could not easily distinguish it from behaviour that perpetrators presented as mundane non-abusive behaviour. For example, someone may put CCTV cameras up outside their home for security purposes or they may use them to ensure that their partner is not able to leave the household undetected; frequent messages sent throughout the day could indicate a loving and caring relationship, or it could be an indication of monitoring; smart devices may be set up for efficiency and convenience (e.g. smart heating) but they could also be used restrict the partners usage of utilities. Police officers therefore struggled to prove that the *intentions* behind the behaviours were abusive. One police officer stated that:

> *"Control and coercive is quite a blurry subject and in a way, it's a bit like defining fog. If you look in the middle, you can see that's fog but you're asked to draw a line of where the edges are, it's very hard to define."*

Consequently, police officers may be more likely to charge perpetrators in cases where there is clear evidence of harassment and stalking, or an assault that has resulted in physical injury, since these are more easily identified. They are also more likely to pass CPS threshold tests and result in conviction. The relatively easy identification of offences of violence or theft, compared to the harder-to-identify coercive control can also lead to misidentification of victims/perpetrators when more graspable offences could be (sometimes wrongly) identified, as the victim-survivor's story below illustrates:

> *A man made sexually explicit homemade videos of himself and his female partner. Whilst the woman consented to the creation of the videos, she did not consent to the man distributing the videos via a WhatsApp group which consisted of multiple people sharing sexual homemade videos. Because the woman suspects the man of cheating, she looked through his phone and found that the videos of her have been distributed to the WhatsApp group. The woman begins to try and collect evidence as quickly as possible by recording herself scrolling through the phone because she knew that she did not have time to examine the information in depth before her partner returned. The woman wanted to report the information to the police but was worried that evidence would be deleted from his phone. She hid the phone in the house. When her partner returned, the couple had an altercation in which the man aggressively took the woman's phone away from her. When the police arrived, the female tried to explain to the officers what she had found and why she had hidden the man's phone. She told them that she knew that image sharing is illegal and that there were sexual videos of her on his phone. The police officer responded "Yeah, it's a real grey area, this kind of topic, so we just need you to give him back his phone". The female continued to argue her point with the police officers, who replied, "we don't want to have to use force [in getting the phone returned]" and the woman was threatened with being arrested for theft. After the officers left, the man subsequently reported the woman to police for allegedly showing people the footage she had taken of her looking at the content on his phone. She was arrested and her devices were seized for investigation.*

It was generally acknowledged that response officers having the time to sit down and speak with victim-survivors was important in providing a good service but also to ask the right questions to fully understand the context, and to identify offences. This is particularly pertinent in DECC cases as a visit to the victim-survivors home allows officers to see which devices are present in the home and to speak with the victim-survivor properly about the devices and the abuser's behaviour. Whilst it was argued that over the years, police had got better at asking questions about the physical (i.e. how often you see your family and friends), it was highlighted that that this *"does not always [happen] for the digital side of things".*

> *"What we very rarely get is people thinking around the wider implications of coercive control and behaviour. So, if it's the victim's phone, does the victim have their bank cards linked to like their Apple Pay or the other Google Pay? Do they have logins for their online stuff for the banking? Are they shopping on Amazon, or have they not even got the app installed? These types of things are indicative of someone, who's basically living a life under duress. And I think that's the type of*

stuff that goes missing that doesn't get picked up".

By far, the biggest challenge faced by police forces in responding quickly to DECC is a lack of knowledge in identifying and understanding how to launch digital lines of inquiry. Senior officers (investigators/specialist officers) highlighted problems in the investigative process that stemmed from poor initial contact with the victim-survivor. Statements and case notes were of poor quality and frequently missing information - in instances of harassment via mobile phones or social media, response officers missed basic but essential information such as telephone numbers, profile names and IDs, and screenshots which could have been used as initial evidence or to identify the correct social media profile. This information was vital for investigators who took over the case at a later date, and often resulted in a second statement needing to be taken, undermining the victim-survivor's confidence in the process. One officer highlighted that, even if supervisors or digital/forensics teams subsequently identify missed lines of inquiries, by that time victim-survivors have already lost confidence in the police and are much less likely to cooperate.

To address these issues, Durham's safeguarding team developed their own force specific domestic abuse training which included a focus on coercive control, training all public facing officers (circa 1,400) in a face-to-face setting over the course of a year. The training included discussion of legislation, expectations in relation to force process and positive action, use of body cameras, the importance of recognizing the risks of post-separation abuse (including homicide), seeing children as victim-survivors in their own right, the impact of police officer attitudes on victim-survivors, special measures, signposting victim-survivors to information and resources as well as digital lines of inquiry. The training used case studies from within Durham Constabulary as well as input from victim-survivors. Durham police also utilise a 'digital bungalow' which is set up to replicate a house with common digital devices so that officers know what to look for and how to seize digital devices.

As part of their efforts to upskill officers on a large-scale Cumbria police have created 'The Academy' in which digital skills training is delivered online and is available to five forces (Cumbria, Merseyside, Greater Manchester, Lancashire and Cheshire). They deliver training at various times of the day and evening to account for police officer shift patterns and to deliver the training in 20-minute sessions following by questions and discussions. Each session is focused on a particular issue and includes training on what evidence can be gained through different digital inquires, how evidence can be obtained from social media, how victim-survivors can be advised on digital hygiene, and so on.

Nevertheless, despite training provision, there was a consensus amongst the three forces that a large proportion of response officers, investigating officers and supervisors did not feel comfortable identifying digital lines of inquiry or that they would not benefit the investigation, resulting in digital lines of inquiry being missed.

Pursuing digital lines of enquiry

The importance of collecting digital evidence during the 'golden hour' (the period immediately following the report) was consistently highlighted across forces, especially due to the risk of data loss (e.g. deleting incriminating evidence online or cloud syncing to externally delete data). It was also highlighted that a lack of knowledge around the different types of digital inquiry was causing an over-reliance on messages and call records, rather than thinking more broadly about how different lines of inquiry can be combined to identify wider patterns of abuse in coercive control cases. For example, one officer stated that investigators should consider:

"How frequently are they contacting their friends, what hours of the day is the phone used. Husband's saying to the wife, 'you're not allowed to use your phone when I'm in work. You're not allowed to go out'... you can say this phone is never used between 9am and 5pm Monday to Friday. Why? The only calls that [they've] made and received [are from him]... Are they going out to coffee shops? You know, these types of things. You build a pattern of behaviour through that because people live their lives on the phone. So, it's very easy when you start putting the timeline together of usage. These [are] the types of considerations that you'd make, and the review of a phone doesn't take long to put that together".

When investigating officers chose to pursue digital lines of inquiry, there was a lack of confidence and knowledge of the evidence collection process particularly how to preserve digital evidence at the scene or from perpetrator's devices. Some of the lack of confidence was due to the uncertainty as to which types of evidence the CPS will accept in DECC cases. For example, when evidencing digital communications or other forms of online abuse (e.g. image-based abuse) some officers stated that only live evidence (from the platform where the images/messages were available) was acceptable, whilst others stated with confidence that screenshots would suffice, and that sometimes victim-survivor phones were being unnecessarily taken when officers could record a screenshot at the time of the incident.

To increase confidence, and to increase efficiency in collecting digital evidence, Cumbria Police created a 'digital toolkit':

"Which has in it a digital investigation manual, if they really want to get into the depths of how to do digital live inquiry and what you can get and what you can do. And then there's, the way [they've] set it out is, victim, suspect, scene, and digital hygiene or digital prevention. And what you can then do with it is when you get to the victim, if you click on victim, it gives you a list of what you can do with your victim , so it gives you a bit of a form of these are the types of things you might want to ask the victim in relation to digital investigations."

Durham also makes use of a portable tool which detects the possibility of stalker-ware on victim-survivor phones.

"We have a a tool called the Guardian, which uses a piece of software, which we attach to the victim's device to it and run it through to see if there's any evidence of high volumes of traffic coming out. It might suggest that the suspect put stalker-ware onto victims' devices. It just means we don't have to take the victim's device and bring it to the police station, keeping it away from somebody who's vulnerable while we download, it which may be unnecessary anyway."

They also show victim-survivors how much of their personal data is available online using open-source searches and how they can better protect their information online.

"We act as the stalker, if that makes sense. And we say, 'this is this is what we found about you on the internet, this is how you need to now go in protect yourself further. Here's a report. This is what your Facebook shows, I know your address and where you work and the children's names and what school they go to'."

In order to progress cases with digital elements, and to support digital investigations, police forces have developed wider support structures. To reduce the backlog of devices in the digital forensics unit, Durham utilize digital kiosks at police stations. Merseyside have recently launched the Digital Kickstart Team, designed to address digitally enabled crime (as opposed to cyber-dependent or cybercrime). The team were formed to reduce the number of digital inquiries being missed, and to relieve pressure on investigating officers by undertaking the digital part of the inquiries. The team review cases within the police system to assist with creating digital strategies and undertaking digital lines of inquiries.

"Putting digital strategies on those crimes to help officers to say, you know, you've got this crime here, but have you considered ABC and D? And, actually, we won't just advise

you, but we'll do these enquiries for you, you know, because we know you've got a massive workload, will help you do in these inquiries to expedite the investigation."

Police officers can also contact the Digital Kickstart team about any investigations they are undertaking, and the team also provide drop-in-support.

"We've put in one officer per week into each of the four areas to basically act as like just a drop in. So, if staff have got any concerns or any investigations that they need advice on, they know that there's one officer there once a week who they can go to for advice and support."

Alongside existing domestic abuse training, including coercive control, the Digital Kickstart team deliver quarterly training as part of a 'digital skills week' to assist with upskilling detectives which includes practical elements and use of real-life cases. They also undertake specialist training courses themselves as part of their CPD.

Cumbria have recently increased their full-time Digital Media Investigators (DMIs) from one to five. These officers do not carry cases but support investigations that require specialist digital investigative assistance. They provide assistance and advice in support of live incidents, investigations, gathering intelligence and conducting proactive/reactive investigations where digital technology and data acquisition opportunities exist (College of Policing, 2024).

Durham police also utilize full time DMIs and have recently doubled their capacity from two to four. The DMI's role at Durham is to assist with rape and serious sexual assault cases, as well any high-risk or high-harm cases. Every morning, the DMIs review every crime that has taken place over the previous 24 hours to identify digital opportunities and guide the investigating officer on what to consider in relation suspect, location and the victim-survivor, as well as assisting with LIMA and CycComms applications. They make a note of these comments and suggested actions on the police system. DMIs are also used to visit victim-survivor's houses to collect some forms of evidence, for example downloading routers.

At both Cumbria and Durham forces, DMIs were also assisted officers with applications for digital evidence. For example, when it is necessary to obtain evidence by downloading the content of a device or request communications data from service providers, investigating officers are required to submit a Lima or a CycComms application. Whilst more senior officers stated that undertaking these applications "not rocket science, once you know how to do it', the importance of this assistance was highlighted when all of the response officers and many detectives we interviewed stated that the applications were complicated and difficult to complete ("The Lima form? Horrific. Absolutely horrific").

The two forces felt that DMIs were pivotal in reducing workloads for cyber and digital forensics units by providing intermediary support for cases which may be too complex for everyday officers but not complex enough to need a high level of support from cyber or digital forensics units. Officers who we interviewed and had made use of the DMIs found their advice and support helpful and senior managers identified them as playing an important upskilling role for investigating officers as working through cases with a DMI meant officers were learning digital inquiry on the job. However, some officers did not seem to know that the roles existed but when asked what would help them to become more confident with digital lines of inquiry, one essentially identified the DMI role.

"They would be there to look at crimes and answer questions. So, I could put an action on my crime, say I've got a digital element here, I'm a little bit out my depth here, this is what I've got, this is what I suspect, can you help me with this. And they will come back and put on a write up to say, 'these are your lines of inquiry, or saying 'you might want to consider this'…'these are your lines of inquiry and what you need to do for them'. Just your short, sharp, help."

Overall, there was consensus within Cumbria and Durham that DMIs were effective, but only if that was their only role. Prior to their recent employment of dedicated DMIs, both forces were using 'double hatted' DMIs (or an equivalent role) in which officers would advise on digital investigations alongside other policing roles. This was considered ineffective as double hatted DMIs do not have enough time to keep abreast of technological change and CPD (e.g what the latest software updates on devices means for evidence collection) leaving them unable to supply the latest guidance and advice to investigating officers:

"We need a dedicated digital media investigation team because the old process wasn't working. What we used to have was Digital Media Advisors, SPoCs [single point of contact] out in area in CID, intelligence [and] in neighbourhoods who had a little bit of training. Very little CPD though. People were getting de-skilled. There were certain guys who were good at it, and they'd become favourites, if you like. They would always be the go-to-guys, so they would get really upskilled. Across the force, maybe five who were really good and the other thirty-five just got forgotten about really, nobody was really managing the system."

However, whilst all three police forces had teams in place to advise and assist investigating officers with potential lines of inquiry, they were not always utilized. Some interviewees reported that a lack of confidence in their ability to carry out digital investigations meant that many officers did not always attempt to engage with the digital aspects of investigation.

Once digital evidence is obtained (via DMIs or otherwise), officers reported difficulties in analysing the volume of data. Data from a phone download or communications data can be sizable and investigators did not always know how to extract and interpret the information they need, as two officers noted.

"It was quite a lengthy case. It was three years of messages and such. When we get the information, it's just presented to us in an Excel spreadsheet. So, nobody kind of does anything with it. So as response officers, I think I came in on a day off, and it took me seven hours to work 3000 messages. And I then had to put them in a format that would be admissible in court as well."

"So, if you are submitting a comms data application and you're getting a month's worth of call data back, staff are overwhelmed with it because it's like I've got this Excel document and I don't know how to see how many times a suspect has called the victim, who her top call has been."

The increasing use of technology to commit criminal offences means that limited police resources are having to be stretched further to respond to the challenges of cyber and digitally facilitated offences. There are significant challenges in terms of keeping up with the emergence and changing nature of new technologies, the ability for data to be remotely deleted if it's not collected quickly and adequately protected (phones placed in Faraday bags or put on aeroplane mode, etc), technology companies increasingly providing more control over user data making access harder for the police, and overseas companies ignoring police requests for data.

All of these things mean that police forces ultimately do not have the resourcing power to deal with the increase in digital offences and the work that is involved in keeping abreast of the latest information and how to conduct increasingly complex investigations. Police officers frequently highlighted existing unmanageable workloads which resulted in lines of inquiry being missed and investigations being delayed (the length of time taken to get data back from perpetrators phone can take anything from 12 weeks to 12 months).

Police forces have made attempts to put some staffing resources in place to address the digital knowledge gap, however, overall, there are very few digital experts within the force. This combined an ever-increasing number of digital inquiries means that digital expert teams are consistently stretched and over-reliant on single members of expert staff.

There was a general consensus that more training was needed for police, both in relation to coercive control and for identifying and pursuing digital lines of inquiry. Stakeholders were asked about what they thought training around DECC should contain, who it should be aimed at, and how it should be delivered. Whilst there a general agreement on what the outcome of the training should be there was no overcall consensus on exactly what this should look like. One of the reasons for this is that there are nuances in the structure and processes within each police force. Thus, each police force was facing its own challenges not just responding to DECC but all digitally enabled forms of crime.

However, in order to effectively respond to coercive control in a digital society it is clear that coercive control training needs to coincide with more effective training around digital lines of inquiry. Generally, all police forces agreed that a complete upskilling of the police force was needed to ensure that digital lines of inquiry were not being missed and that officers felt confident dealing with digital lines of inquiry. However, due to limited resources, most participants also recognized that it was not realistic to be train every single officer in complex digital evidence collection methods. Therefore, it was argued that training should be tailored to the roles of specific officers play within their relevant force. There was also an agreement that training/upskilling needed to be force specific to effectively respond to the different structures, processes and challenges relevant to each force. It was identified by interviewers that any training provided by the College of Policing would be too slow to roll out, rendering the content consistently out of date. There should be further support for localised training which can respond to the immediate needs and knowledge gaps within forces. Therefore, below we lay out a series of recommendations, many of which relate to training content which build upon basic training as officers progress through the ranks or undertake new roles.

Recommendations

1 Call handlers and first responders need to establish possible offences as soon as possible in the process of dealing with incidents. Less experienced officers may run with the original crime label given by call handlers even if it is not correct, or if further offences become apparent during the opening of the investigation. This is particularly important with coercive control.

2 Call handlers should be trained to understand the key signs of coercive control, ask the right questions to identify possible coercive control, and to obtain initial digital information linked reports to assist police officers in identifying digital elements before attending the address/speaking with the victim-survivor. This should also be combined with an empathetic approach as these initial points of contact with the force can be make or break in terms of victim-survivors engagement with the police.

3 First responders should be equipped to identify key signs of coercive control and consider whether coercive control is present in addition to any physical assault, theft, fraud, and other more easily identifiable offences; if they identify elements of coercive control, they should feel confident to identify, investigate, and seize digital devices/evidence.

4 Given that coercive control can often involve multiple different forms of direct and indirect abuse, a victim-survivor may report many lower level and non-physical offences as this reflects the nature of the abuse. Therefore, it is imperative that first responders and investigators officers, understand the importance of context, and identify patterns of behaviour, as opposed to focusing upon individual incidents.

5 The data analysed showed that in a significant proportion of recorded incidents, DECC was mis-identified, or not identified at all (see recorded incidents section). This can lead to lines of investigation being missed, and misreporting of the scale of coercive control, and DECC.

6 Call handers, first response, and investigators must ensure that victim-survivors accounts are recorded correctly and that the victim-survivor understands how their accounts are being recorded (some victim-survivors described how when reading statements later down the line, or in family court, the statements did not adequately capture the bigger picture or had significant omissions with regards to patterns of behaviour).

7 When possible, investigators should conduct home visits so that they can see which digital devices are being used within the home and look out for other physical signs of coercive control (i.e. locks on the outside of doors, holes in the walls or if the perpetrator refuses to be separated from the victim-survivor).

8 All investigating officers should be able to identify the correct lines of inquiry, including what data can be collected from mobile phones, apps and other service providers and their windows of evidence collection, relevant digital evidence patterns (i.e. victim-survivors behaviour patterns as well as perpetrators), understand how to obtain the evidence they require (i.e LIMA and CycComms application forms and basic social media downloads), how to use software available to them, and how to review digital data.

9 Investigators should take an intersectional approach (i.e. to be aware of disabilities and how this can be taken advantage of in coercive control contexts (such as removal of aids) and ensure that children are not asked to translate for deaf victim-survivors as this may prevent them from disclosing.

10 Investigators should use police records of previous contact (including lower-level offences, incidents with different complainants, etc) to see if a pattern of abusive behaviour exists.

11 Ideally, all CID officers would be trained up to DMI level and have some level of open-source training, however this may not be possible, and forces may opt for the use of dedicated DMIs to assist investigating officers.

12 Supervisors were identified as potentially playing a key role in ensuring that digital lines of inquiry are not missed. Interviews identified that anyone with a supervisory capacity should be trained on digital inquiry to an extent in which they can identify lines of inquiry missed by investigators when reviewing cases. Data identified that not all supervisors have enough knowledge of digital inquiries to fulfil this role and therefore, lines of inquiry continue to be missed. Therefore, supervisors should also be trained, at minimum, to the same level as detectives and preferably hold a DMI certification.

UNIVERSITY OF LIVERPOOL
TACKLING DIGITALLY ENABLED COERCIVE CONTROL

13 Whilst DMIs were generally considered to be a worthwhile resource, this is not a long-term solution in addressing the need for force wide upskilling. This was highlighted in police interviews for two reasons; 1) the significant cost of the DMI training programme offered by the College of Policing and 2) reliance on DMIs to conduct digital lines on inquiry could result in an over-reliance on some officers whilst providing limited upskilling for non-DMI officers in a climate where 'digital policing' should be part of everyday practice. We found DMIs to be a critical resource, but one which was limited by resource pressures, and one that should be used to supplement an already high level of capability in response and investigative officers.

14 Specialist digital teams such as digital forensics teams, and DMIs should have access to regular CPD to ensue that they are able to keep abreast of changes and opportunities to digital lines of inquiry and how to execute these, include access to relevant software.

15 Whilst the NPCC and CPS do provide evidence gathering checklist which indicates what digital evidence might look like, it would be useful if more detailed guidance was provided in relation to the quality of evidence, especially within particular contexts. For example, in cases when intimate images have been non-consensually shared as part of a wider pattern of abuse. Waiting for police to collect live evidence can cause further harm to the victim-survivor by increasing the likelihood of further distribution and making it harder for images to be removed. Therefore, the necessity of live evidence needs to be balanced against the harm caused to the victim-survivor.

16 Risk assessment and safeguarding tools (currently DASH and DARA) should include questions about use of digital devices to control the behaviour of the victim-survivor.

17 Training should include contributions from the third sector to aid understanding of how coercive control can present to first responders; to understand trauma informed responses; to ask the right question (e.g. does he always know where you are, do you see family and friends, what was your life like before you met this person?).

18 Police forces should work with third sector to develop humancentric training which is focused on the needs and requirements of victim-survivors and counteracts desensitisation. However, this should be combined with regular police officer engagement with wellbeing support.

19 Digital training should be embedded within basic training for new recruits to ensure that digital lines of inquiry become a norm within policing. Over the years, police forces should aim for 'digital policing' to become standard policing practice.

20 Basic training should ensure that officers make the most out of the 'golden hour' evidentially and are able to collect evidence quickly from online spaces where evidence deletion is high risk (or quick removal is necessary e.g. cases of image-based abuse). Training should therefore include, at minimum identification of digital lines of inquiry, knowledge on collecting basic/initial evidence collection (e.g. device information, telephone numbers, correct social media profile information, how to effectively take screenshots of communication (i.e. ensuring overlap between text messages to demonstrate no evidence tampering), digital evidence preservation (including cloud storage), initial checks of victim-survivor's devices for potential evidence or risk (i.e. understanding location settings), LIMA and CycComms applications, and information on support teams (e.g. open source teams, DMIs, Digital Teams) to ensure rapid evidence collection when necessary.

21 If possible, local substantive training should be face-to-face to allow for police officers to obtain hands on practical experience.

22 Following local substantive training, it is necessary for training on digital lines of inquiry to be consistently rolled out to ensure that forces are up to date with the latest technological developments and changes, as well as latest information on what information service providers supply to law enforcement. For example, forces highlighted that officers still assumed that no information could be obtained from Snapchat, despite the fact that Snapchat now do engage with law enforcement. In these instances, face-to-face training is not likely to be feasible and therefore, it is more realistic for this training to be conducted online and consist of short updates on various topics relevant to forces, alongside on-demand refresher training.

23 Training should make use of real-life cases relevant to the specific forces should be responsive to feedback from police officers on upcoming challenges to prevent knowledge gaps (e.g. responding to an increase in the use of specific apps).

Conclusion

Whilst each of the forces we interviewed have made substantial attempts to improve knowledge and policing practice around digital lines of inquiry, it was found that more should be done to facilitate effective and long-lasting change. Almost every domestic abuse related incident contained digital lines of inquiry and therefore being able to collect digital forms of evidence, process them effectively, and investigate them fully should be part of everyday policing.

Acknowledgements

We would like to acknowledge and thank the participation of Merseyside, Cumbria, Durham and Cheshire police forces; Mankind Initiative, Revenge Porn Helpline, Welsh Women's Aid, and victim-survivors who kindly gave their time and expertise.

Research Team

Antoinette Raffaela Huber is Lecturer in Criminology at the University of Liverpool. Her research focuses upon gendered-based violence, image-based sexual abuse, misogynistic extremism, pornography, digital policing, and digital criminology. Antoinette works closely with domestic violence organisations, the Revenge Porn Helpline and Victims of Image Crime (VOIC). She has also worked with UK and EU commissions contributing to legislative and regulatory change around digital abuse.

Barry Godfrey is Professor of Social Justice at the University of Liverpool. Between 2021 and 2023, working with DA Leads at 23 police forces, a report on domestic abuse during covid was produced; recommendations were fully accepted by the NPCC Domestic Abuse Lead and subsequently used by the DA Commissioner to produce a new strategic plan in 2023. In 2022-23, funded by the N8 Police Research Partnership, he undertook research to examine strategies for reducing serious repeat DA offending. He continues to work with several police forces on strategies to identify and control 'high-harm high-frequency' domestic abuse perpetrators.

Bibliography

Barlow, C., Johnson, K., Walklate, S. and Humphreys, L. (2010) Putting Coercive Control into Practice: Problems and Possibilities, *British Journal of Criminology*, 60: 160-179.

Harkin, D. and Whelan, C. (2022) Perceptions of police training needs in cyber-crime, *International Journal of Police Science & Management*, 24(1): 66-76.

Henry, N., Gavey, N. and Johnson, K. (2023) Image-Based Sexual Abuse as a means of coercive control: Victim-survivor experiences, *Violence Against Women*, 29(6-7): 1206-1226.

Home office (2023) Controlling or Coercive Behaviour: Statutory Guidance Framework. Available at: https://www.gov.uk/government/publications/controlling-or-coercive-behaviour-statutory-guidance-framework/controlling-or-coercive-behaviour-statutory-guidance-framework-accessible

Horsman, G. (2017) Can we continue to effectively police digital crime?, *Science & Justice*, 57(6): 448-454.

Huber, A. R. (2023). Image-based sexual abuse: Legislative and policing responses, *Criminology & Criminal Justice*, *0*(0): 1-17.

Powell, A., Stratton, G. and Cameron, R. (2018), *Digital Criminology: Crime and Justice in Digital Society*. Abingdon: Routledge.

Refuge (2020) 72% of Refuge service users identify experiencing tech abuse. Available at: https://refuge.org.uk/news/72-of-refuge-service-users-identify-experiencing-tech-abuse/

Refuge (2022) Marked as Unsafe: How online platforms are failing domestic abuse survivors. *Report*. Available at: https://refuge.org.uk/wp-content/uploads/2022/11/Marked-as-Unsafe-FINAL-November-2022.pdf

Stark (2007) *Coercive Control: How Men Entrap Women in Everyday Life*. Oxford: Oxford University Press.

Todd, C., Bryce, J. and Franqueira, V.N. (2021) Technology, cyberstalking and domestic homicide: Informing prevention and response strategies, *Policing and Society*, 31(1): 82-99.

Women's Aid (2014) Virtual World, Real Fear: Women's Aid report into online abuse, harassment and stalking, *Report.* Available at: https://www.womensaid.org.uk/wp-content/uploads/2015/11/Women_s_Aid_Virtual_World_Real_Fear_Feb_2014-3.pdf

Women's Aid (2024) 'What is Coercive Control?'. Available at: https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/coercive-control/

Wilson-Kovacs, D. (2021) Digital media investigators: challenges and opportunities in the use of digital forensics in police investigations in England and Wales, *Policing: An International Journal*, 44(4): 669-682.

UNIVERSITY OF LIVERPOOL
TACKLING DIGITALLY ENABLED COERCIVE CONTROL

Find out more at
liverpool.ac.uk/law-and-social-justice/

We are the original red brick