A Framework to Investigate Cybergrooming Crimes

Natalie Fernandes
Cyberprotect Officer
City of London Police

Charles Edwards
Detective Inspector
Leicestershire Police

Dinesh Mothi, PhD
Course Leader
Ravensbourne University

ABSTRACT
Grooming is when an adult builds an emotional connection with a child with the intention of exploiting the child's trust by using them for their own sexual gratification. Groomers will first gain the trust of the child so that the child is less likely going to question their intentions. Groomers can do this by offering to buy gifts for the child, giving the child attention or pretending to be a child themselves therefore deceiving the child who may not know they are being groomed.

Thus leading to sexual abuse, and as the groomer would find ways to convince the child to meet up with them to then take sexual advantage of the child. After review, it was found that a method or framework was missing. To address that gap, in this paper, we propose a theoretical framework to investigate child cybergrooming offences in the jurisdiction of England and Wales. The data was gathered through interviews, and grounded theory was applied to create the framework which could then be applied at the operational or managerial level. Future work would also focus on applying digital policing skills to investigate how cybergrooming could be reduced and tackled in this day and age of the cyberworld.

Keywords
Cybergrooming; Digital Forensics; Investigation Framework.

1. INTRODUCTION
Cyber relates to the internet or cyberspace which is a means of communicating worldwide. This can be exploited because this enables a crime to be committed at a large scale. Grooming can be a cyber-enabled crime if facilitated through digital technology. One of the most common types of cyber- enabled crimes is sexual offending against a child one of which is cyber-grooming. With the growth of the internet today, groomers use it as a way of staying anonymous online while grooming. Most grooming is facilitated through online tools such as social media, chat rooms and gaming sites. Groomers exploit popular internet sites and applications with children such as chat rooms, gaming and social media. This allows an effective potential of private and unrestricted communication access to children (Inhope, 2018).

On 3 April 2017, section 67 of the Serious Crime Act 2015 inserted a new offence into the Sexual Offences Act 2003. Section 15A, criminalises a person aged 18 or over who intentionally communicates with a child under 16 for the purpose of sexual gratification. The adult does not have to reasonably believe that the child is 16 or over. The communication is sexual or intends to encourage the child to make a communication which is sexual. Sexual communication is if any part relates to sexual activity or a reasonable person were to regard any part of the communication as sexual. Also, it would carry a maximum two-year prison sentence (Sexual Offences Act, 2003). Republic of Ireland legislation for cyber-grooming is in Criminal Law (Sexual Offences) Act 2017 section 8 (Criminal Law (Sexual Offences) Act, 2017) and Scotland have sexual Offences (Scotland) Act 2009, part 4 section 24 under young children (Sexual Offences (Scotland) Act, 2009).

2. RELATED WORK
Grooming is the communicative part of luring theory, and even though the internet has broadened the grooming's scope, the frameworks are still grounded in offline grooming theory (Gauz, 2014). Child grooming involves a manipulative process wherein trust is first built with the victim and later desensitised by the perpetrator. The aim here is to acquire the victim's trust with the notion that they do not have the ability to identify deceptive communication strategies employed by the perpetrators (Davidson & Gottschalk, 2011; McGhee et al., 2011; Whittle et al., 2013).

Within (Olson et al., 2007) framework, grooming is defined as "the subtle communication strategies that child sexual abusers use to prepare their potential victims to accept the sexual contact" (p. 241). Craven et al. (2006) defines sexual grooming as "A process by which a person prepares a child, significant adults and the environment for the abuse of this child" (p. 297). The authors also have catergorised various phases of grooming which will be reviewed in the section 2.2. The internet has facilitated grooming and their characteristics to be carried out with ease with regards to maintaining anonymity online (Shannon, 2008; Briggs et al., 2011)

2.1 Online tools for facilitating cyber-grooming
According to ChildLine UK, a free 24-hour counselling service for children, the 6 places where grooming can happen are social networking websites, instant messaging apps, photo sharing apps, chat rooms, dating apps and online gaming sites (Childline, 2018). On social media, groomers may send out multiple 'friend requests', 'follow requests' or 'message requests' at random in the hope that a child will accept them. They also try to identify vulnerable children by looking at the things they post, pictures and profile information. In games and chat rooms they will try to start conversations with young people using similar interests such as gaming. They then may ask the child to move to a more private form of communication (Thinkuknow.co.uk, 2018). Peter Davies, chief executive of Child Exploitation and Online Protection Centre (CEOP), has stated that half of all child sexual exploitation takes place on social networks. The National Crime Agency (NCA) also has stated that many social networking sites and websites are used by groomers to target children and young people (Jordans Solicitors, 2017).

2.2 Grooming categories
2.2.1 Initiation
Grooming initiation can be differentiated between three categories. Designed by UK's leading children's rights organisation, End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes (ECPAT), the three categories include adult approaches child/children, child approaches the adult and 'loverboys' (ECPAT International,

2016). The first category, is when the adult approaches the child via online. From here they can choose two routes; either pretend to be a younger person or truly reveal they are an adult. The groomer nurtures a friendship with the child in order to gain their trust. Once the trust has been established, the perpetrator asks questions about the child's sexual experience thus leading to the sexual communication. The second category states that the initial contact is started by the child. Some children do it for fun or for monetary gain. For example, children can offer naked pictures, live broadcasts or a personal meeting for money. Contact details for potential 'customers' are shared within some grooming communities. The final category 'loverboys' is where the groomer establishes a friendship with the victim and then uses social engineering to gain the necessary information to build a relationship with the child. Information such as hobbies and interests will be available on the child's profile therefore this forms the basis of contact. The 'loverboy' then starts to ask for a bit more information, before taking their relationship further. This would subsequently mean the child sending naked pictures of themselves, which would lead to further blackmail and/or forced prostitution (Sulz, 2017). This research evidence suggests that offline grooming techniques appear to have been adapted for the virtual presence. The research is a good foundation for the preparation of a cyber-grooming investigation but lacks the facility to explore the cybercrime investigation or digital forensic element. This element is important when analysing chat logs.

2.2.2 Manipulation

Grooming involves some form of manipulation and victims are mostly pressurised o to behave uncharacteristically. As grooming can involve giving gifts, force, threats, giving bribes to name a few, and there are different variations in manipulation styles such as instilling fear in victims, overt manipulation, suffering, integrity protection employed by the perpetrators (Sullivan and Quayle, 2012). The manipulation style is dependent on the personality and circumstance of the offender, and their victim. The use of various manipulation techniques facilitates the perpetrator to have power and control over their victim and thus increasing their dependency on them (Ospina et al., 2010).

2.2.3 Access to Victims

Having access to victims is one of the crucial factors that determines whether a perpetrator is likely to get involved in grooming a victim or not. The internet is a good medium for perpetrators who have an interest to groom people safely and in confidence which would have not been possible a couple of years ago (Whittle et al., 2013). Whereas, in the past the perpetrators abused victims due to their acquaintance through family members, workplace, residential care, and other sources (Olson et al., 2007, Harkins and Dixon 2010). Nowadays, this has changed with the rise in young children and adults using the internet thus favouring perpetrators who can anonymously contact and communicate with their victims (Briggs et al., 2011).

2.2.4 Building Rapport

It is harder for a young victim such as a child to identify and recognise between online grooming phases and the genuine online relationships (Bryce, 2010). Perpetrators build rapport with victims by gaining their trust (Olson et al., 2007), and this is done through imitating the victims behaviour and their communication styles (Williams et al.,2013). The perpetrator learns about the victim's interests by stalking their online profiles to gain intelligence about similar interests or life experiences that they can relate to the victim (European Online Grooming Project, Webster et al., 2012). Grooming does not take place in a linear fashion but is cyclical in nature as stated by (William et al., 2013) which is further supported by (European Online Grooming Project, Webster et al., 2012).

2.2.5 Sexualisation

The key to the development of the grooming process is sexualising the communication with the victim (Whittle et al., 2013). This aspect of grooming is dependent on the type of the perpetrators. The three different types of online groomers as categorised by the (European Online Grooming Project et al., 2012) are intimacy seeking, adaptable, and hyper-sexualised. The perpetrators of the latter category are more likely to introduce sexual elements to the conversation. The form sexualisation can take are flirting, dirty talking, sending obscene pictures or even links to pornographic content (Ospina et al., 2010). Through sexualization the perpetrator establishes further control over the victim as they share sensitive information without anyone else's knowledge, and this is how the perpetrator has a leverage to blackmail their victim (Mc Alinden, 2006).

2.2.6 Deception

Perpetrators tend to use various tactics to deceit child victims online such as pretending to be of the victim's age. However, it is a misconception all perpetrators who groom their victims online lie about their age and intentions whilst conversing with their victims. In most cases victims are aware of their perpetrators age and their intentions (Wolak, 2007). Therefore, victims are aware that they are communications with adults online and continue to take risks by engaging with them which demonstrates the intensity of the grooming process and victim's vulnerability to a perpetrator (Whittle et al., 2013).

2.3 Theoretical Models

From the background research, there was no theoretical models pertaining to cyber-grooming investigation. Thus, three models were identified cybercrime investigation, digital forensic and cyber-grooming. The various stages will be compared and analysed for if they can be applicable to a cyber-grooming investigation.

2.3.1 Cybercrime investigation & Digital Forensic models

Ciardhuáin (2004) extended model of Cybercrime investigation incorporates the investigation process and cybercrime element. This model doesn't specify cyber-grooming, nevertheless it provides a comprehensive understanding of a cybercrime investigation. This can be applicable to cyber-grooming. However, for a cyber-grooming investigation this would need to be more specific to the crime of cyber-grooming. Authorisation for law enforcement agencies would usually be a formal legal authorisation setting out in precise detail what is permitted in an investigation, for example, a warrant. However, there is not enough detail on

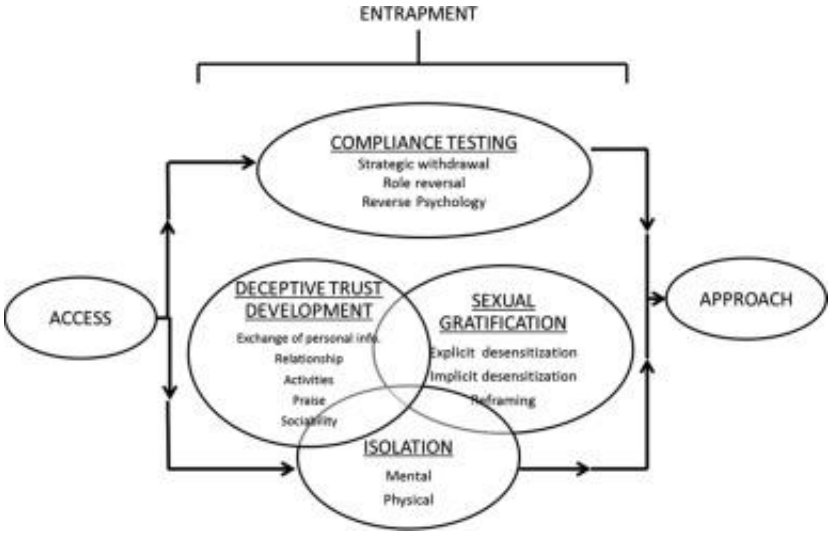


Figure 1 Lorenzo-Dus et al (2016) - A model of Online Grooming Discourse

the application of the warrant or the execution of it. This is an important part of an investigation because it places law enforcement with legal powers to seize digital.

evidence.

Kohn et al (2013) integrated digital forensic model is a current digital forensic model. The model compared to Ciardhuáin (2004) included the same 'activities' such as analysis but either referred to it as a different named activity. However, Kohn encourages the documentation process being continuous throughout the investigation which Ciardhuáin lacks of. Live forensic stage wasn't mentioned enough throughout these models. The Triage Process model proposed by Rogers et al (2006) demonstrates time constraints during triaging in an investigation. The more recent cyber-grooming model by Lorenzo-Dus et al (2016) was developed by analysing chat logs available from foundation, Perverted Justice that specialises in fighting online groomers. The model of online grooming communication compromises of three phases: access, approach and entrapment. Access entails groomers making initial online contact with potential victims. Approach refers to cues prompted by the groomer in order to take the online relationship offline. Compliance testing as an online grooming process that comprises three strategies: strategic withdrawal, role reversal and reverse psychology. Strategic withdrawal, is when the groomers gives the victim a bit of freedom to make decisions, so it appears to give the victim control over the relationship. In role reversal, groomers pretend to adopt low risk-taking attitude that may be expected of children when engaging with unknown adults. Reverse psychology entails groomers challenging their victims' intention or decisions. Figure1 provides an adequate foundation for a cyber-grooming investigation with the application of current digital forensic and cyber-grooming models. This understanding compensates for there not being one model pertaining to cyber-grooming Investigations if all three were to be applied. Considering that some of the theoretical models were created for law enforcement use, they do not specify any digital evidence guidelines.

2.4 Digital evidence guidelines

The Association of Chief Police Officers (ACPO) developed a good practice and advice guide containing forensic regulator's codes of practice and conduct of digital evidence in the UK.
The ACPO guidelines does not state that there is any specific ACPO guidelines for the investigation of cyber-grooming cases. Similarly, the legislations mentioned in section 7.5 in

ACPO fail to mention any legislations pertaining to cyber-grooming however warrants and sexual offences act. The reason for this, is that the latest ACPO guidelines was written in 2012, 6 years ago therefore wouldn't have any new key legislations that have passed post 2012. However, the four ACPO principles, which if adhered to display objectivity in court, as well as the continuity and integrity of evidence (ACPO 2012). The National Institute of Justice (NIJ) is the research, development, and evaluation agency of the U.S. Department of Justice. They have established a guide for first responders for electronic crime scene investigation. These guidelines lack population validity as it is based on the American justice system and also because it does not contain any specific guidelines when conducting a cyber-grooming investigation therefore isn't up for adaptation to a UK law enforcement system. The guidelines were published in 2008 which is outdated however some concepts the U.S include the UK haven't acknowledged therefore can be adapted to today in terms of emerging technologies that wouldn't have been mentioned or existed in 2008 (NIJ 2008).In terms of both sets of guidelines, ACPO and NIJ advise a set of equipment to bring. They are overlaps but NIJ include gloves which ACPO fail to mention and ACPO include a torch whereas NIJ assume this is a general tool but this should alsobe included in digital

evidence collection preparation. Both mention the use of equipment such as anti-static bags and faraday bags to prevent signal interference altering the evidence and the use of a camera to record crime scene, evidence and on-screen display. Also both give clear procedures for devices whether switched on or off. NIJ gave a better set of confirmation guidelines for checking the device compared to ACPO's vague outline.

3. METHOD

After reviewing the literature, the research questions were answered to a certain extent that addresses the research problem and the gap: a cyber-grooming framework specific to a law enforcement investigation was absent from the literature. Therefore, the primary data was gathered from interviews, and secondary data was gathered using document analysis. Both data would be analysed using grounded theory to progress into a new identification and integration of categories/phases to produce a framework. The framework would guide law

enforcement when investigating a cyber grooming case. Grounded theory as a method enabled help this study to identify categories and establish relationships between them. The identified categories were refined using constant comparative analysis, leading to the development of Cyber Grooming Investigation Framework.

3.1 Categories

The first categories are formed by grouping together the secondary data that share a central feature with one another. The categories are not mutually exclusive and will evolve throughout the data analysis.

3.2 Refining Categories

Reviewing the initial categories created, the data gathered can be further distributed into categories and sub categories using document analysis. The significant phases found from my review of digital forensic and cyber-crime investigation models can be divided into their own category. Awareness would be covered by the cyber-grooming category. Evidence collection, preservation, analysis and presentation will have their own category to further elaborate on these phases. Planning phases includes authorisation and search warrants. This is also mentioned briefly in the ACPO guidelines. A further category 'Legislations' will explore what are the key cyber-grooming legislations that ACPO fail to mention and what legislations are adhered to whilst performing digital forensic investigations. From the data gathered a new category 'future scope' was added to answer the research question, "what support and protection is offered to victims of cyber Grooming by protection agencies?" Therefore, the new categories are now cyber-grooming, legislations, planning, evidence collection, preservation, analysis, presentation, case studies, organisations and future scope. This formed four

new research questions that would explore how to identify, preserve, evidence pertaining to cybergrooming offences, the key legislations adhered to when investigation cybergrooming cases, and the collection and presentation of evidence.

3.3 Theoretical sampling

Theoretical sampling means checking emerging theory against reality by sampling incidents that may challenge or elaborate its developing claims. Semi-structured interviews were chosen because it would help in asking predetermined questions and, being present to be able to deviate from the question structure to explore whatever appears relevant and elicit a more detailed response. After reviewing the research questions, new research questions and new categories, interview questions were crafted to give the researcher a better insight on how a cyber-grooming case is dealt with.

3.3 Comparative analysis of categories

The new derived categories are Cyber Grooming, legislations, planning, crime scene, evidence collection, preservation, analysis, presentation, case studies, organisations and future scope. It was decided to group these categories together into main phases and have within sub-phases. This will be done by comparing both my primary and secondary data. The phases should demonstrate each stage of a Cyber Grooming investigation then lead to the development of a framework.

The first phase should be planning for a Cyber Grooming investigation. As data was gathered on obtaining a search warrant and different types of warrants, this phase turned into 'warrants'. This would include all of the legal authorisations that would need upon entering the crime scene.

As well as obtaining a search warrant, preparation before entering a crime scene is necessary. The second phase will be called Preparation in relation to entering the crime scene. This would be a continuation of the warrant phase, where the warrant is executed therefore giving legal authority to be on the premises and conduct a search and seize.

3.4 Theoretical saturation

After analysing the data it has been decided that Cyber grooming should be included but not as its own category/phase. A cyber Grooming Investigation would be needed when the awareness that the investigation relates to Cyber Grooming. The first phase 'warrants' has been refined to include the category Cyber Grooming as a sub phase. By refining warrants to legal authorisation, this would include sub phases: Awareness (Cyber Grooming); and Warrants (Application). Preparation (for crime scene) phase includes sub phases; 'organisations' to group all of the preparations for digital investigators and warrant (execution). When analysing the third phase, the analysis showed 'secure' would be more of an appropriate name with sub phases; crime scene, warrant (seizure) and transporting and storing. As I've already included the application and executed of warrants, it felt applicable to include warrants to seize the evidence thus securing it. The sub-phase transporting and storing entails recommendations and factors to maintain the integrity of the digital evidence. Analysis phase includes both analysing the evidence subsequent to imaging it. The interpretation of 'analysis' didn't define both of these sub phases, so an appropriate name for the phase would be 'examination' (of the evidence). An addition sub-phase 'prove communication' was included. Presentation phase was altered however a sub phase 'expert witness' was fitting to emphasise the digital forensics expert's duty to the court. This lead to the achievement of theoretical saturation as there was a lack of responses from other law enforcement officials and no new secondary data emerging. The phases, sub-phases and further sub-phases where identified. A block diagram of this is in appendix 1. Grounded theory has enable me to identify categories, collect further data, refine categories, compare all data to lead to theoretical saturation of the key phases. It was used as a method which lead to the identification of the phases. Hence, the theory of a Cyber Grooming investigation is grounded from the data gathered. The end-product of grounded theory was an explanatory framework for law enforcement of these phases.

4. RESULTS (FRAMEWORK)

This section will comprise of defining the only key categories/themes (due to space restrictions) identified from the data analysis. Defining each theme and further dividing each theme into sub-themes, will set about the data gathered, contextualising it in relation to existing literature. The five themes and their individual sub-themes are presented in section appendix 1. As you can see the warrant sub-theme is across three main themes. This emphasises the importance of legal powers in accordance with search and seizure. Acquiring digital evidence is a predominant element in a conviction for a cyber-grooming crime. Therefore, the key UK legislations, legal documentation and handling of digital forensic evidence have been identified and implemented within the framework to prevent the digital evidence being inadmissible in court.

The following guidelines are advised to be used alongside:

- Authorised Professional Practice (APP) investigation Process - from the college of policing (College of Policing, 2013).

- The Association of Chief Police Officers (ACPO) good practice guide for digital evidence (2012). The principles of digital forensics issued by ACPO, can be used as guidelines in handling digital evidence when which it being admissible in court. These will be referred to within framework.

4.1 Legal authorisation

Legal authorisation consists of the initial responsiveness to a cyber-grooming case. To collect evidence from a premise (crime scene) authorisations need to be made. This is done by applying for a warrant under Police and Criminal Evidence Act (PACE) 1984. This gives the investigatory team the legal power to search and seize with or without a warrant. Also applying for a requesting a Mutual Legal Assistance (MLA) can aid when there are cross boarder issues when gathering evidence. This phase authorises the investigatory team the legal power or sanction to search a premise(s). The following stages are applied to law enforcement in England, Wales and Northern Ireland. In Scotland, officers should ensure they are acting within the terms of the search warrant. This document can be a guide for law enforcement in Scotland applying for a warrant (Brodies LLP, 2017).

4.2 Awareness

From the identification of the case pertaining to is confirmed as a cyber-grooming case, the approach to the digital evidence is pertinent to the case. The awareness can be created from a reactive approach. A reactive approach, for example can start with a report from victim, intelligence links to other crimes or re-investigation because of new information (College of Policing, 2013). Investigators should be familiar with the investigative strategies relating to the victim(s) and suspect(s) within cyber-grooming. Within the framework a cyber-grooming investigation keyword search consisting of words relating to cyber-grooming will be included. The purpose of this is to enable a faster investigatory process. Recommended Lorenzo Dus's (2016) - A model of Online Grooming Discourse.

4.2.1 Warrant

The correct preparation of a warrant needs to be applied. Entry to the premises will not be granted unless a warrant is produced. The purpose of the search may be prevented unless a constable arriving at the premises can secure immediate entry.(Police and Criminal Evidence Act, 1984a).

4.3 International – Mutual Legal Assistance

Police to police enquires allow police officers in different states to exchange information, intelligence and evidence to aid the requesting state investigation. This can be useful for the exchange of information which is in a different states domain, that the UK doesn't have the legal grounds to obtain but is crucial for use as evidence in a UK investigation. This is the quicker and less complicated route if the foreign state has no objections. The UK law and the law of the foreign state should be adhered to. Also, this can be useful when requesting a Mutual Legal Assistance (MLA) as you can clearly specify your request and gather the necessary information (NPIA, 2012). MLA is a mutual legal aid treaty between States for obtaining assistance in the investigation or prosecution of criminal offences. Requests are made by an international formal letter of request (ILOR or LOR) to a country asking for help. It is the responsibility of the prosecutor to draft the LOR. For example, if Facebook have evidence that is pertaining to the cyber-grooming investigation, the international letter of request is given to the crown prosecution. This letter is sent over to the FBI in America as Facebook Headquarters is based there. The FBI would apply for a subpoena (equivalent to a warrant), who would of behalf on the UK acquire the necessary evidence needed for their investigation (Edwards, C. 2017). Investigators should seek advice from the prosecutor which route is best if obtain evidence from an oversea territory if deemed a challenge. Also, the ACPO (2012) Practice Advice on European Cross-Border Investigations should be used as guidelines for police officers who need to acquire an overseas warrant. Organisations such as NCA, CEOP and Europol have can help UK police officers with cross-border investigations as they will act as an authorised covert human intelligence source (NPIA, 2012).

4.4 Preparation (for crime scene)

Preparing for the collection of digital evidence, can only happen once the correct legal authorisation has been approved. Preparations include the organisation of seizure equipment to take. Also, potential electronic devices to seize that contain information of evidentiary value to a cyber-grooming investigation. Confidently, investigators then can execute the warrant to the occupier of the premise. To comply with ACPO principle 3, full records must be kept of all actions taken in relation to digital evidence. A chain of custody record; of the handling of evidence and contemporaneous notes; of all action taken by the digital forensic examiner.

4.5 Organisation

Organisation before entering a premise enables the investigatory team to deal with a cyber-grooming case effectively and efficiently. Investigators therefore need to prepare the correct equipment, anticipate evidence and interview questions. Legal documentation, although it is as a continuous process throughout the entire investigation, preparation for it is needed so the investigator knows good practice for compiling coherent documentation to be able to withstand legal scrutiny. A forensic examiner must prepare certain equipment items to be taken to the crime scene. The tools and materials are advised in digital evidence collection. The suggested items have been taken from ACPO and NIJ guidelines (ACPO, 2012) (NIJ, 2008).

4.6 Potential digital evidence

These items are advised when seizing items from the suspect and/or victim's premises. All personal electronic devices or devices that the suspect has access to if it is a shared device. It is essential to show a link between that evidence and the suspect. It would be a device(s) that can be used to communicate and save potential evidence.

Computers, mobile communication devices, calendars or journals, Internet activity records, printed e-mail, notes, and letters and maps, notes or records of chat sessions, microphones, computer games and consoles, printer, scanners, copiers, removable media, Information regarding steganography and External data storage devices. As a lot of cyber-grooming can lead to further child exploitation, these suggested items may be of interest when gathering evidence. Camera, digital camera software, photo editing and viewing software, printed images or pictures, web cameras, videotapes/DVD'S/CD-roms (NIJ, 2008).

4.7 Secure

Collection of evidence will consequently be easy if the correct preparation has been followed. Once lawfully on the premise (crime scene) securing the crime scene should be the first response for the forensic examiner. To secure the digital evidence precautions need to be made if the digital device is

switched on or off. Improper handling of evidence can result in loss of vital digital evidence. Furthermore, this should be regarded to when transporting and storing the collected evidence.

4.8 Crime scene

The first and most important step in any cyber-grooming investigation is to secure and take control of the area containing the digital evidence. Securing the scene includes keeping unauthorised personnel from interacting with any digital devices or power supplies. Do not allow any interaction with digital devices by suspect. Ensure that the condition of the digital device has not been altered. Allow any processes to continue such as printing before seizing. Photograph or video the scene and all the components including the leads/cables. Photograph and make a written record of the content of the screen. Label all connections on devices, ports, cables and power supplies for reconstruction purposes (ACPO, 2012). The digital forensic examiner should consider components such as keyboard, mouse, removable storage media, etc if they have value of any other type of evidence such fingerprints or DNA that should be preserved(Forensic Science Regulator, 2014).

4.9 Transporting and storing evidence

The forensic examiner should ensure that devices containing potential digital evidence are packaged, sealed and transported correctly in order to maintain the

integrity of the digital evidence. The security of the device and digital evidence to ensure that access to it is correctly supervised when moving it from the scene to

the laboratory or other location, and protection of the device and digital evidence to ensure that it is not affected by physical shock or electromagnetic interference, extremes of heat and humidity or other environmental hazard (Forensic Science Regulator, 2014).

4.10 Disclosure

Through the means of disclosure, each party is entitled to see the evidence of the other party. The exchange of evidence between the prosecution and defence is to avoid an ambush of evidence at trial. After disclosure of documents and witness statements, the expert might alter their report. This should be communicated with the prosecutor. A further report may be needed if new digital evidence emerges. If more than one party wants to introduce expert evidence, then a pre-hearing discussion of expert evidence is permitted by the court. This encourages the experts to meet before trail to settle any disputes and come to an agreement. If an agreement is made, their reports may be read at trial without the need of the expert to attend court. However, if an agreement cannot be met, at trial a cross-examination will focus of these discrepancies (Bond et al., 2007).

4.11 Expert witness in court

Part 33 of the Criminal Procedure Rules (CPR) deals with criminal expert evidence (Ministry of Justice 2014). An expert witness for a cyber-grooming case gives evidence of both fact and opinion. Experts must be able to identify the origin of their facts which their opinion, as an expert is based on. Digital forensic experts should only give their opinion of the digital evidence as this is the expert's qualified and experienced area. Therefore, the expert's role is to educate, prepare a report and sometimes give oral evidence at trial (Bond et al., 2007). A forensic expert should prepare for a court hearing as soon as they have been asked to prepare a report. The expert. When the evidence is finished being presented the expert is 'released' from court. The findings of the data analysis, presents a coherent flow which creates a cyber-grooming framework. It should provide law enforcement officers guidance and assistance to investigate a cyber-grooming case efficiently. It will be updated according to legislative and policy changes.

5. DISCUSSION

To contribute to the digital forensic and policing field, this cyber-grooming investigation framework will aid officers and digital forensic experts not familiar with either field and cyber-grooming as a concept. This gives a coherent set of guidelines for experts to follow. Overall, the cyber-grooming investigation framework was a fascinating, innovative and current topic to research. Cybercrime is increasing exponentially today thus a framework that can aid prosecution of more groomers will be a good contribution to policing and digital forensic fields. Unfortunately, due to lack of responses and not knowing a direct contact to law enforcement that deal with cyber-grooming crimes, only one law enforcement officer was interviewed. Because of the lack of exposure to the actual investigations and the vast differences between different Police Forces capabilities and capacities it is key that this will not solve every aspect of process but will provide a well-researched and developed basis to work from in developing their own local protocols and processes'.

The cyber-grooming investigation framework is a unique contribution to knowledge in the field of digital forensics. As this provides one consistent pathway for law enforcement to follow when investigating a case pertaining to cyber-grooming. From the data gathered it appears that there is no individual framework or guidelines that pertain to cyber-grooming. However, there are generic digital evidnce guidelines that law enforcement already uses, such as ACPO. Also, there are digital frameworks/cybercrime investigation models but again, these are generic. However, they still provide a model and basis of a cyber-related/digital investigation. In addition, cyber-grooming models are primarily from a psychological perspective of the groomer and victim. They fail to include the digital forensic perspective, which with the aid of forensic linguistics can advise a direction to cyber-grooming investigation. This is what has been delivered in the cyber-grooming investigation framework; combination of all frameworks, guidelines and viewpoints of law enforcement into one law abiding framework.

The significance of this framework is that it would serve as a guide or good practice guideline for law enforcement agencies when investigating cyber-grooming cases. The limitation of this framework is that it would be best suited for the law enforcement agencies that are based in England and Wales; however, in the future its scope would be expanded to national and international jurisdictions.

6. FUTURE SCOPE AND CONCLUSION

Future search will be a continuation and further scope into this current hybrid project. As this framework focuses on digital forensics, working alongside other digital forensic experts, linguistic experts, legal experts and cyber-crime psychologist hopefully will expand the scope of the framework to other domains, to gain a better understanding of a cyber-grooming investigation. Refining the framework with perspectives from more law enforcement agencies both national and international will enable the cyber-grooming investigation framework to be applied anywhere in the world with respect to the country's cyber-grooming investigation legislations. The system design of a cyber-grooming keyword search is the basis for further

development into an algorithm that can analyse chat logs for cyber-grooming content.

7. REFERENCES

[1] ACPO (2012). ACPO Good Practice Guide for Digital Evidence. 5th ed. [ebook] Available at: http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

[2] Aqib Riaz. (2014). Belkasoft RAM Capturer and Evidence center. [Online Video]. 6 December 2014. Available from: https://www.youtube.com/watch?v=kPA9bEJsar0.

[3] BBC Inside Out - the hidden scandal of sexual grooming of young Sikh girls by Muslim men. (2013). [video] Available at: https://www.youtube.com/watch?v=7hXTM7ehvtk

[4] BBC News (2018). Children could get online grooming 'alerts' - NSPCC. [online] Available at: http://www.bbc.co.uk/news/uk-42855172 [Accessed 22 Apr. 2018].

[5] Belkasoft. (2018a). Belkasoft Evidence Center 2017. [online] Available at: https://belkasoft.com/ec [Accessed 22 Apr. 2018].

[6] Belkasoft. (2018b). Belkasoft RAM Capturer: Volatile Memory Acquisition Tool. [online] Available at: https://belkasoft.com/ram-capturer [Accessed 22 Apr. 2018].

[7] Belkasoft. (2018c). Belkasoft Acquisition Tool. [online] Available at: https://belkasoft.com/bat [Accessed 22 Apr. 2018].

[8] Bond Solon (2010). Excellence in Written Evidence. pp.11-16.

[9] Bond, C., Solon, M., Harper, P. and Davies, G. (2007). The expert witness. 3rd ed. Kent: Shaw & Sons Limited, pp.47-76.

[10] Bowcott, O. (2018). Police should need warrants to search mobile phones, say campaigners. The Guardian. [online] Available at: https://www.theguardian.com/uk-news/2017/jan/13/police-warrant-search-mobile-phones-campaigners-privacy-international.

[11] Brodies LLP (2017). Search warrants - responding to search warrants in Scotland. [ebook] brodies, pp.1-4. Available at: http://www.brodies.com/sites/default/files/search_warrants_in_scotland.pdf

[12] Cellebrite. (2018). UFED Cloud Analyzer. [online] Available at: https://www.cellebrite.com/en/products/ufed-cloud-analyzer

[13] Cellebrite. (2018a). UFED Ultimate / PA. [online] Available at: https://www.cellebrite.com/en/products/ufed-ultimate/ [Accessed 22 Apr. 2018].

[14] Cellebrite. (2018b). Field Series. [online] Available at: https://www.cellebrite.com/en/solutions/field-series/ [Accessed 22 Apr. 2018].

[15] Cellebrite. (2018c). UFED Cloud Analyzer. [online] Available at: https://www.cellebrite.com/en/products/ufed-cloud-analyzer/ [Accessed 22 Apr. 2018].

[16] Childline. (2018). Online grooming | Childline. [online] Available at: https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/online-grooming/ [Accessed 22 Apr. 2018].

[17] Ciardhuáin, S.Ó., 2004. An extended model of cybercrime investigations. International Journal of Digital Evidence, 3(1), pp.1-22.

[18] College of Policing (2013). Investigation process. [online] App.college.police.uk. Available at: https://www.app.college.police.uk/app-content/investigations/investigation-process

[19] Criminal Law (Sexual Offenses) Act 2017 part 2, ss.8. Available at: http://www.irishstatutebook.ie/eli/2017/act/2/section/8/enacted/en/html ECPAT International. (2016). ECPAT International. [online] Available at: http://www.ecpat.org/

[20] Edwards, C. (2017) Interviewed by Natalie Fernandes, 29 November.

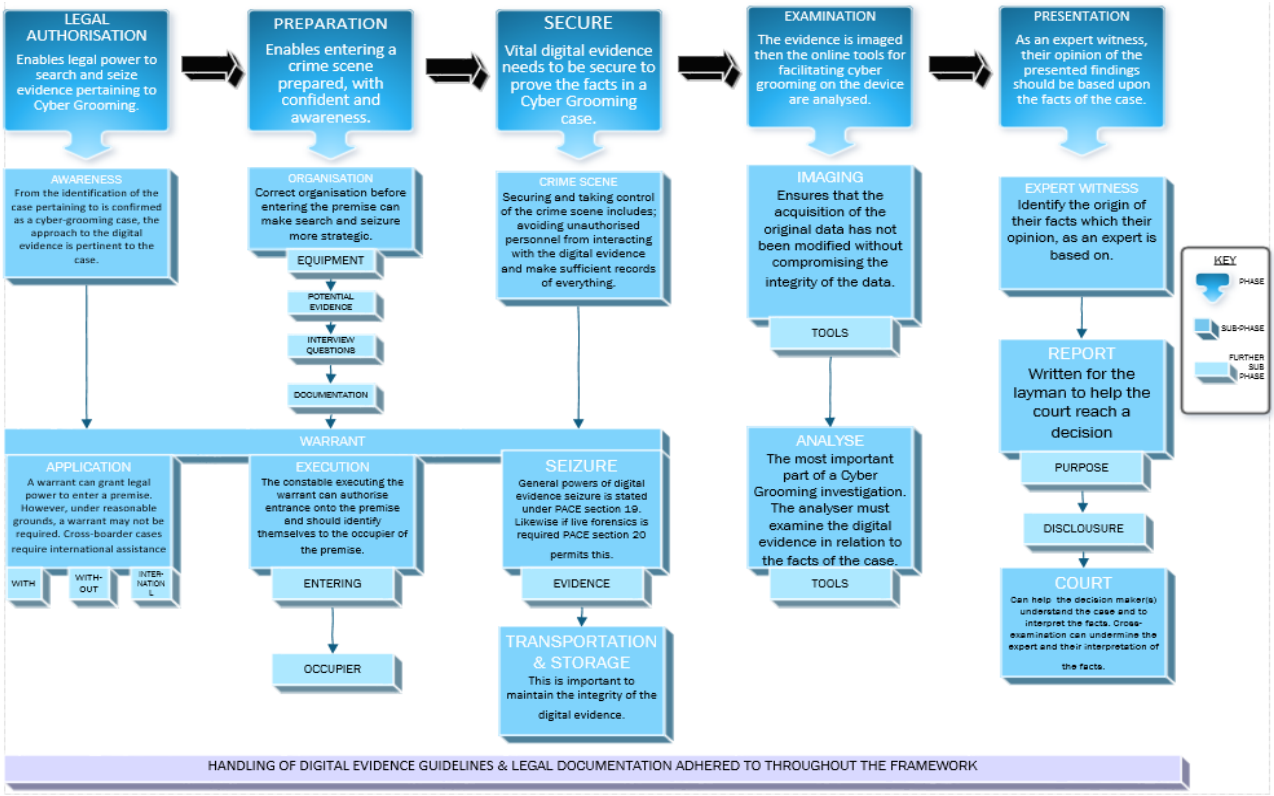
[21] Forensic Science Regulator (2014). Digital forensic services: codes of practice for forensic service providers. 1st ed. [ebook] p.7. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/351220/2014.08.28_FSR-C-107_Digital_forensics.pdf.

[22] Forensic Science Regulator (2014a). Digital forensic services: codes of practice for forensic service providers. 1st ed. [ebook] Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/351220/2014.08.28_FSR-C-107_Digital_forensics.pdf.

[23] Halliday, J. (2015). Teenager who killed Breck Bednar in 'sadistic' attack jailed for life. The Guardian. [online] Available at: https://www.theguardian.com/uk-news/2015/jan/12/lewis-daynes-stabbed-breck-bednar-essex-sentenced-chelmsford-crown-court [Accessed 22 Apr. 2018].

[24] Home Office (2014). Guidance – Evidence in criminal investigations. 3rd ed. [ebook] pp.33-34. Available at:

Appendix1: Cyber-Grooming Investigation Framework Block Diagram


LEGAL AUTHORISATION
Enables legal power to search and seize evidence pertaining to Cyber Grooming.
PREPARATION
Enables entering a crime scene prepared, with confident and awareness.
SECURE
Vital digital evidence needs to be secure to prove the facts in a Cyber Grooming case.
EXAMINATION
The evidence is imaged then the online tools for facilitating cyber grooming on the device are analysed.
PRESENTATION
As an expert witness, their opinion of the presented findings should be based upon the facts of the case.
AWARENESS
From the identification of the case pertaining to is confirmed as a cyber-grooming case, the approach to the digital evidence is pertinent to the case.
ORGANISATION
Correct organisation before entering the premise can make search and seizure more strategic.
EQUIPMENT
POTENTIAL EVIDENCE
INTERVIEW QUESTIONS
DOCUMENTATION
CRIME SCENE
Securing and taking control of the crime scene includes; avoiding unauthorised personnel from interacting with the digital evidence and make sufficient records of everything.
IMAGING
Ensures that the acquisition of the original data has not been modified without compromising the integrity of the data.
TOOLS
EXPERT WITNESS
Identify the origin of their facts which their opinion, as an expert is based on.
KEY
PHASE
SUB-PHASE
FURTHER SUB PHASE
WARRANT
APPLICATION
A warrant can grant legal power to enter a premise. However, under reasonable grounds, a warrant may not be required. Cross-boarder cases require international assistance
WITH
WITH-OUT
INTER-NATION L
EXECUTION
The constable executing the warrant can authorise entrance onto the premise and should identify themselves to the occupier of the premise.
ENTERING
OCCUPIER
SEIZURE
General powers of digital evidence seizure is stated under PACE section 19. Likewise if live forensics is required PACE section 20 permits this.
EVIDENCE
TRANSPORTATION & STORAGE
This is important to maintain the integrity of the digital evidence.
ANALYSE
The most important part of a Cyber Grooming investigation. The analyser must examine the digital evidence in relation to the facts of the case.
TOOLS
REPORT
Written for the layman to help the court reach a decision
PURPOSE
DISCLOUSURE
COURT
Can help the decision maker(s) understand the case and to interpret the facts. Cross-examination can undermine the expert and their interpretation of the facts.
HANDLING OF DIGITAL EVIDENCE GUIDELINES & LEGAL DOCUMENTATION ADHERED TO THROUGHOUT THE FRAMEWORK