How might Crime-Scripts be used to Support the Understanding and Policing of Cloud Crime?

Steve Warren[1], Gavin Oxburgh[2], Pam Briggs[3], and David Wall[4]

[1] School of Psychology, Newcastle University, UK (steve.warren@ncl.ac.uk)
[2] School of Psychology, Newcastle University, UK (gavin.oxburgh@ncl.ac.uk)
[3]Department of Psychology, Northumbria University, Newcastle, UK (p.briggs@northumbria.ac.uk)
[4] Centre for Criminal Justice Studies, School of Law, University of Leeds, Leeds, UK (d.s.wall@leeds.ac.uk)

Abstract. Crime scripts are becoming an increasingly popular method for understanding crime by turning a crime from a static event into a process, whereby every phase of the crime is scripted. It is based on the work relating to cognitive scripts and rational-choice theory. With the exponential growth of cyber-crime, and more specifically cloud-crime, policing/law enforcement agencies are struggling with the amount of reported cyber-crime. This paper argues that crime scripts are the most effective way forward in terms of helping understand the behaviour of the criminal during the crime itself. They act as a common language between different stakeholders, focusing attention and resources on the key phases of a crime. More importantly, they shine a light on the psychological element of a crime over the more technical cyber-related elements. The paper concludes with an example of what a cloud-crime script might look like, asking future research to better understand: (i) cloud criminal fantasy development; (ii) the online cultures around cloud crime; (iii) how the idea of digital-drift affects crime scripts, and; (iv) to improve on the work by Ekblom and Gill in improving crime scripts.

Keywords. Crime scripts, cloud-crime, cyber-crime

1. Introduction

Cloud computing is a relatively new term – estimated to be first used in the mid-2000s [6] - with the first cloud-type services offered as early as the late 1990s [14]. Since then, cloud computing has grown exponentially and continues to become a central part of consumer and business computing. Seventy-six percent of businesses make use cloud computing [24] with a prediction that by 2020, over half of mobile devices will rely on the cloud. The National Institute of Standards and Technology [32] have defined cloud computing as:

'A model for enabling convenient, on-demand network access to a shared pool

of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.'

They continue to state that cloud computing is composed of five essential elements: (i) *on-demand self-service* (an individual can alter the computing capabilities in an instant); (ii) *broad access network* (access via a network and standard mechanisms); (iii) *resource pooling* (multiple resources – physical and virtual - and multi-tenant design); (iv) *rapid elasticity* (resources can instantly scale up or down), and; (v) *measured service* (automatic control and optimization of resources).

The exponential growth of cloud computing has brought with it a steep rise in crime involving the cloud. The reasons are obvious, especially when considering the five elements listed above which allow criminals to commit crimes in a multitude of ways to both improve the effectiveness of the crime itself and lessen their chance of getting caught. Some examples of cloud crime include criminals who buy cloud computing resources (with stolen credit cards) to host computational resources to break passwords on databases (brute force), or use these cloud resources to launch a Distributed Denial of Service (DDoS) attack (in this case using the cloud-virtual machines as a botnet – see appendix for definitions of computer science terms). The fact that many businesses and individuals use the cloud to store private information allows criminals easier access to that data. Criminals may even use the cloud to store illegal data, such as child exploitation material. In one example of fraud, criminals used phishing emails (created on the cloud) which installed malware that mimicked a bank website, meaning that when an individual went to transfer money (using what they thought was their bank's website), it went direct to the criminals. The interesting facet of this was the malware was located on a cloud server.

The complexities of these cloud crimes are such that it is important for policing/law enforcement agencies to better understand both the crime event and the criminal in one easy to understand, yet complete, framework. One of the ways academia has put forth is a systematic framework called *crime scripts*. Crime scripts were first put forward by Cornish [13] as a way to understand a crime with a more psychological edge. Crime scripts essentially turn a crime from an *event* into a *process*. This means that rather than a crime being a confusing and singular episode, we are now able to see every step the criminal takes leading up to the crime, followed by the crime itself, then after the crime. This includes any resources, locations, actors, activities, and even motivations (if known). Once constructed, a crime script forms a cognitive script – an organised and structured pattern of thought presented as a script where every element has a relationship with each other - that includes any decision a criminal will make, therefore creating a sequence of the pragmatic knowledge about their *modus operandi.*

Whilst the growth of cloud computing is undoubtedly useful in many positive ways, it brings with it an extra and potent dimension to cybercrime. Already, policing/law-enforcement agencies are struggling to keep up with all the crimes committed using

digital and networked technologies [27]. The authors of this current paper believe that the creation of crime scripts is an essential element in understanding, and therefore tackling, cloud crime.

2. Cyber-crime and Cloud-crime

Cybercrime is continuing to grow at a high rate because of the potential that new digital and networking technologies affords criminals. For example, real world drug dealers are taking to the dark net to sell their goods because of the lack of face-to-face interactions (thereby decreasing the chances of getting caught), increase in security around selling (*PGP encryption* and the *TOR network* – see appendix) and increase in potential buyers' market share. The ever-increasing growth in crime-as-a-service is another issue, where a select few programmers create the viruses/spam/Trojans/DDoS (see appendix) capabilities and sell them to a layperson online, thereby distancing themselves from a 'crime scene'.

Westlake and Bouchard [47] believe that the Internet has affected crime on websites in three main ways. First, in terms of sexual exploitation, social networking sites have been used to groom victims [49, 50, 51] and have also been used for phishing [2], for the spread of malware [53] and spam [54], and financial institutions' websites are used to acquire private financial information of customers [30]. Second, both the Internet and the dark net (see appendix) are all used as a platform to buy and sell illegal goods/services [38]. Third, the Internet, deep web, and dark net are also used as a communal space to exchange ideas and provide social support to other criminals [52].

Wall [44] simplifies even further what the advent of digital and networked technologies has meant for criminals. It now allow criminals to commit over 50 million, £1 thefts (at a lower risk) rather than a single £50 million theft at an obviously far higher risk. Wall [45] believes that this transformation means that, in theory, the average person can now commit many crimes simultaneously on a global level. This is an entirely new, and somewhat terrifying, concept to deal with for policing/law-enforcement agencies. Thus, there is an urgent need for digital and networking forensic experts to better understand the process by which these crimes take place. Without this understanding, international policing/law-enforcement agencies have little hope of successfully making an impact. The UK has a strategy for impact through their 'Four Ps Strategy' - Protect, Prevent, Pursue, and Prepare:

> *'Existing [UK] Government strategy… has four components (the 'Four Ps Model') and involves a multiplicity of national and transnational organisations intervening both before ('Protect' and 'Prevent') and after ('Pursue' and 'Prepare') criminal activity.' (p.11 Implications of Economic Cybercrime for Police)*

However, despite these defined strategies and the growth of cybercrime, the definition of cybercrime itself is still under debate because whilst everybody agrees that it exists, not everybody agrees what it is [44]. Wall [44] argues that there are three main types of cybercrime based on his transformation test. A transformation test in this case

means removing the impact of the Internet is removed from the equation. First, there are *cyber-assisted crimes* – crimes that would, and could, still take place without digital or networking technologies (Wall uses an example of 'Googling' how to dispose of a dead body). Second, is *cyber-enabled crimes* which are crimes previously committed on a local level but now can take place on a much larger scale through the Internet (e.g., fraud). Third, and the purest form of cybercrime, is *cyber-dependent crimes*. These are crimes that if you took away the Internet, the crime itself disappears completely. This type of crime is completely dependent on the digital and networking technology – an example would be DDoS (distributed denial-of-service) attacks or spam e-mails. This paper will lean on the work of Wall and concentrate not only on *cyber-dependent* crimes, but what is now a subsection of that definition - *cloud-dependent* crimes.

Cloud-crime brings with it its own set of issues that differ from cyber-crime. Cloud crime can be defined as any crime committed with the assistance of the cloud, with this paper particularly focusing on cloud-dependent crimes. Traditional cybercrime forensic investigations involve collection of data or evidence from the location of the computer or device, followed by validation, analysis, interpretation, documentation, and presentation of results to a Court. Cloud-computing distorts this process as investigators must deal with multi-tenant hosting (same server serves multiple tenants), synchronisation problems, non-localised data, and jurisdiction issues (amongst others). Finding where the data is kept and retrieving it can be very problematic - in most cases, the user may not even know. With the exponential growth of cloud-computing, it is therefore essential to better understand the *behaviours* and *procedures* involved in cloud-dependent crime. This means understanding the criminal and their actions, something crime scripts do in a systematic way.

3. The Importance of Crime Scripts

It is well known that members of the public, in general, struggle to understand the science behind cybercrime and cybersecurity and this problem is exacerbated by the different regulatory frameworks associated with cybercrime, thereby resulting in a confusing array of issues for the average citizen [41]. One key issue in setting-up an effective and robust evidence-chain that might lead to successful prosecution in the cloud crime arena concerns the way in which the underlying crimes may be communicated to key stakeholders and to the general public. At present, there are real challenges in communicating effectively across stakeholders with an interest in cybercrime, where, for example, understanding the use of advanced machine learning and AI techniques – which will help automate the identifying and remedying of a cyber-crime – demand a level of computational expertise that is well beyond the non-expert. How much more difficult, then, will the task of convincing a court that such techniques have demonstrated criminal culpability beyond reasonable doubt. To address such issues, we take inspiration from literature around science communication [34, 15] where recently, the more traditional approaches to information delivery has given ground to participatory methods that actively seek the involvement of various communities in the science pro-

cess. In other words, this problem is not simply one of, "How shall we simplify a message", but becomes one of, "How can we collectively construct a common language with which to discuss key issues". Such a 'common language' would bring benefits, not only to the research process (facilitating the ability of researchers to involve key stakeholders more directly), but would also allow the different stakeholders throughout the criminal justice process to talk to each other more meaningfully. It would also help to raise public awareness and allow public input to the process more directly (e.g., by facilitating the rapid identification and reporting of cloud-crime as it happens).

The use of scenarios to understand the complexities of a particular situation (or set of tasks) have been in evidence for a long time, although their context of use has changed considerably in recent years. For example, scenarios were introduced as design tools to aid disaster planning where they were found to be powerful tools to support the visualisation of a range of possible outcomes [10]. Go and Carroll [23] described two kinds of scenarios: (i) 'problem scenarios' that could illustrate the complexities and difficulties with known systems, and; (ii) 'activity scenarios' that facilitate the process of reasoning about uncertainties and supported the creation of sets of alternative realities that could stimulate the design process. It is now recognised that one of the principal contributions of scenarios in the design process is the creation of a common language that can span different communities. The construction and use of scenarios evolved, however, and came to be more widely recognised as 'stories' with settings, actors and plots, capable of describing existing situations, but also of describing future and emerging situations. Not surprisingly, scenarios started to be played out in a form of a design theatre, where particular situations could be dramatised with actors and props in order to understand just how innovative tools and systems could be effectively introduced [5]. In addition to the script-based scenarios and a variety of techniques for describing the actors or personas involved in the script [12], some researchers have argued that good personal development is essential for the generation of a rich and credible script [35]. More recently, new tools for the scripting of highly ambiguous scenarios have been developed that allow the interpersonal elements of a scenario to be fore-grounded and allow the audience more flexibility in considering a range of possible variants or outcomes [9].

Consequently, one important technique in overcoming these issues is the creation of crime scripts [7, 14]. Crime scripts are schemata that guide our understanding of a criminal's behaviour and routines. Once this logical and cognitive sequence of events are known, policing/law enforcement agencies know where to focus their resources to investigate and prevent crime, with both researchers and practitioners adopting this method as an analytic tool for looking at rational and goal-orientated behaviour [37]. Levi [31] suggests that crime scripts can be important in improving understanding of complex crimes, such as *cloud-dependent* crime.

4. Crime Script Analysis

Cornish [13] was the first person to create a systematic approach to creating these scripts – the work based on the concept of rational choice and cognitive scripts [1, 37]. The rational choice perspective examines a crime from the perspective of the offender [14] and takes a present-centred look at the interaction between the offender and their environment. The cognitive script approach is used extensively in psychology whereby a sequence of behaviours or decisions are 'scripted' for a specific situation.

In order to create a crime script, a crime script analysis must be undertaken. This is a systematic methodology [7, 13, 24] that generally relies on qualitative data and behavioural decision-making. It classically involves breaking down the actions of the criminal into four main stages - *preparation*, *pre-activity*, *activity*, and *post activity* [7]. However, crime scripts have been further broken down by other researchers into *preparation*, *pre-condition*, *instrumental pre-condition*, *instrumental initiation*, *instrumental actualisation*, *post-condition*, and *exit* [13, 18] – different types of crime developing different sequences. These stages are created by concentrating on the main elements of a crime (e.g., who, what, when, where, why, and how). Classically, the most important information gathered is how the offender goes about the crime and what decisions s/he makes along the way. This includes how *'they accessed the crime scene, the skills they required, the effort involved, information about the crime opportunity, the financing required to carry out the crime, facilitators (tools, transport, weapons, communication), and technical expertise'* [43, p.7]. This information will be almost impossible to gather from a single source, thus, drawing on multiple sources is a salient point to remember when undertaking a crime script analysis. The information needed can be gained from various sources such as interviews with criminals, police notes, police investigative interviews/interrogations, CCTV footage, or from anyone intimate with the crime, etc.

In order to create these scripts, some form of qualitative or quantitative analysis must take place on the data. Qualitative analysis, particularly content analysis, is a popular choice [11] with a process of data categorisation allowing the researchers to develop the scripts. The exact type of analysis conducted seems less important than making sure the chosen analysis (whether it be content, conceptual, thematic, or a mix) allows for categories of themes to emerge, thereby lending understanding to the process and sequence of the crime. Script analysis can create high-order scripts - more generalised, over-arching scripts - or individual tracks - where every decision a criminal makes (or could make) is mapped. Crime scripts highlight the procedural nature of crime [7, 13] and should be able to reveal an overall picture of the sequence of actions a criminal undertakes before, during, and after a crime has occurred.

Table 1. An example crime script of a robbery given by Cornish in his original paper [13].

Script Scenes	***Script Actions***

Preparation	Meet and agree on hunting ground
Entry	Entry to underground system
Pre-condition	Travel to hunting ground
Pre-condition	Circulating/waiting at ground
Instrumental Pre-condition	Selecting victim and circumstances
Instrumental Initiation	Closing-in/preparation
Instrumental Actualisation	Striking at victim
Instrumental Actualisation	Pressing home attack
Doing	Take money, etc
Post-condition	Escape from scene
Exit	Exit system

The script outlined in table 1 highlights the process of how a robbery takes place, mapping out the sequence in which the event occurs, giving policing/law enforcement agencies multiple phases to explore in regard to either preventing the crime taking place or apprehending the offender - this is a salient point often forgotten in the creation of crime scripts. Surely the purpose must be for such agencies to carry out their job more efficiently, therefore ensuring crime scripts are more driven towards practitioners is important [22]. One paper that creates a crime script with possible interventions at every stage is on the activities involved in drug manufacturing in clandestine laboratories [11]. This paper divided up potential interventions into three categories: (i) *manager-place*; (ii) *guardian-target*, and, (iii) *handler-offender*. For every stage, they had potential interventions for policing/law enforcement agencies that apply to these categories.

Despite a diversity of papers employing crime scripts for real world crimes [18, 20, 22, 33, 43], the literature contains almost no cyber-crime scripts, with specific cloud-crime scripts an, as of yet, unresearched area. One paper that explores the creation of cyber-crime scripts relates to the online stolen data market [30]. In it, the authors found six universal stages, with each stage containing a mix of behaviours and events:

> ***Stage 1: Preparation*** (setting up the necessary client software and creating accounts, steps towards anonymity and security, marketplace location, and learning specialist knowledge);
>
> ***Stage 2: Entry*** (learning marketplace language and rules);
>
> ***Stage 3: Pre-condition*** (obtaining and manufacturing products to sell, instrumental pre-condition, advertising products and services, instrumental initiation,

exchanging law enforcement information, negotiating and communicating, instrumental actualisation, sending and receiving payment);

Stage 4: Doing (packaging goods, transporting goods);

Stage 5: Post-condition (reputation management, exchanging currency);

Stage 6: Exit (laundering proceeds).

One of the biggest challenges in creating cyber-crime scripts will be to understand how different they are to real-world crime scripts. The Internet is a fluid space – something we discuss in detail in the next section - so do we expect cyber-crime scripts to be so fluid, so lacking in concrete stages, as to be worthless? Hutchings and Holt argue that human behaviour is *human behaviour*, thus, wherever a human is involved, we are able to understand and map their behaviour and decisions.

5. What Elements Might We See in a Cloud-crime Script?

The inherent nature of the cloud means that committing a crime can be committed from any location in the world, with preparation and pre-activity phases now a more complex and expansive phase due to increased elasticity and access. The activity itself is, by definition, a far more elusive crime, and the traditional post-crime period can now involve a more active monitoring period - where the criminal can monitor the effect of the crime at a more intense frequency (be it participating in forums, contacting the victim for ransom, sharing the data multiple times over a long-time period, etc.). Disengagement and exit from a crime scene is also now more fluid and less concrete, which means that the process of a cloud-crime may be less formal and concrete than a real-world crime.

An important element that should appear throughout most cloud-crime scripts should be the role of the online community. Research in both the psychological and sociological literature has shown that online communities are very powerful and effective spaces, just as much as real world communities and even real world social interactions. The breaking-down of communication barriers by the Internet [36] have allowed communities to transform into global social networks [49] rather than local ones. Hillman, Procyk, and Neustaedter [26] argue that these online communities allow the easier conduct and targeting of illegal activities and potential victims. The Internet, they argue, brings crime from a solitary business into a globally communal business, where anyone with an Internet connection can take part, or indeed be a victim.

Holt [28] explored online criminal communities and found that crimes that would normally be categorised as solitary crimes (e.g., hacking) are in fact a communal effort, where the tools, resources and knowledge required are shared within these communities. The growth of cybercrime has made it a necessity to further explore these communities – through both quantitative, but more importantly, qualitative methodologies such as ethnography - that play a major role in facilitating these cybercrimes.

One of the most important elements, or stages, of a cyber-crime is the criminals' access to a like-minded online community. Westlake, Bouchard, and Frank [48] looked at how child exploitation communities are built and found that these websites play a crucial role in facilitating criminal activities. Henson, Swartz, and Ryns [25] decided to better understand the relationship between offline and online, and looked at the concept of street-orientated beliefs [3, 4] in the context of online culture. Anderson [3, 4] examined an inner-city community (in Philadelphia, USA), and found that the widespread feeling of isolation and mistrust in 'the system' stemmed from the endemic poverty, unemployment, and perceived discrimination. Because of this, some people in that community created their own notions of success, a more achievable notion than the 'white, middle class version'; in other words, respect through toughness. Anderson called this the "*code of the street"*, which is an informal set of violence-orientated rules as a means to achieve and maintain respect.

These findings show that, as hypothesized by Henson et al [25], codes of the street exist and play out in online settings. The second finding is an equally important one. It was found that individuals who were off-line criminals were more likely to commit a cybercrime than those who were not. These findings suggest that there is a strong relationship between the off-line and on-line criminal world, that real world strategies and known criminal psychology can be applied with potential success. Henson et al. [25] called for a greater exploration of these relationships to confirm the findings in their study. They believe that these online street codes might be the single greatest factor in driving cybercrime participation. This tends to indicate that *cloud-dependent* crime scripts will fundamentally be the same as a *normal* crime script. They will be more similar in behaviours, emotions, learning curves, planning, amount of trial and error etc, than the complexity of cloud-crime hints. This means, and corroborates the work of Ekblom and Gill [20], that cloud-crime scripts will be more psychological than event-driven. Therefore, cloud-crime scripts will be, and should be, just as much as a journey into the mind of the offender as other non-technical crime scripts.

One important facet of this new type of crime, especially cloud crime, is the concept of *digital drift*. This is defined in the work of Goldsmith and Brewer as *"individuals [who] can gain access to criminal associations, networks and resources in ways that see them drift in (and out) of related illicit activities facilitated by the medium of the Internet itself"*. They argue that the increasing ubiquitousness of technology, along with the increasing networking power of technology, means technology now acts as cognitive extensions - things that augment not only our cognition but our lived experience. They argue that the networking technologies can substitute for other interaction partners, making a crime potentially easier. What Goldsmith and Brewer warn of is a new form of 'bad guy', not one that is unambiguously a criminal, but those that move in and out of doing bad things. This fluidity of criminal is something we must understand better, according to Goldsmith and Brewer, if we are to tackle cyber-crime.

6. Limitations of Current Crime Scripts

One major criticism of using a rational choice perspective in crime scripts is that it fails to explain irrational behaviour – examples including when the offender is drunk, is unaware of how his/her actions will affect the situation, having to change plans on the spot, etc. Cornish and Clarke [14] have argued that the rational choice perspective is only to create a focused framework in which to assess criminal decision-making. If we are to make crime scripts a more systematic and successful tool, the work of Ekblom and Gill [20] is of paramount importance. They argue that with the rise in the use of crime scripts, *"…rather than tinkering with the concept [of crime scripts], a fundamental rewrite was indicated" (p.321).* They list some grievances they have with the current crime-script analysis, including:

- The universal script (with its preparation stage, pre-activity stage, etc.) can be difficult to apply, with more work than may be rewarded required to assign actions to the universal stages;
- There is a dilemma in how scripts can be generalised and yet accommodate variation;
- There is confusion between declaratory and procedural knowledge;
- It is unclear whether scripts describe behaviour or events.

Ekblom and Gill want to scrutinise the underlying concepts of crime-scripts to help develop more accurate scripts. One of the major issues they see with the current crime-scripts in use is the conceptual foundation on which they are based - the 'cognitive script' from Abelson [1], and Schank and Abelson [37]. Ekblom and Gill found this approach to be unclear and too narrow for what is needed in this situation. In general, they felt crime scripts were too loose, with a definition dependent upon who was creating it. They see differentiating *behaviours* and *events* as key to a crime script. For them, behaviour focuses on the perpetrator, while the event focuses on the interaction between perpetrator and their environment. They view scripts as, *"Abstracted descriptions of a particular kind of behavioural process, namely, structured sequences of behaviour extended over time and perhaps space, which could be considered functionally self-contained units or subunits of longer sequences" [p.323]*. They clarify that the behaviour they speak of may be individual or group. By concentrating on the behaviour, and then its consequence on events, we get to see a more consistent script.

Two of the example crime scripts they present in their paper offer some interesting thoughts, the first being *empirical scripts*. These, *"…are simple descriptions of recurrent sequences of behaviour in situ" [p324]*. In these, goals must be evidenced and never should an assumption be made about the inner thoughts of a possible offender. The second is called an *explanatory script*. They borrow from Tinbergen [42] four stages of explanation for animal/human behaviour: (i) function; (ii) causation; (iii) development, and; (iv) evolutionary history. Because crime scripts deal with agents' perception, knowledge, and experience, Ekblom and Gill [20] added a fifth stage - phenomenology (the subjective experience of the offender). All stages need to be taken

into account when creating explanatory scripts; a salient point we take from the paper - that crime scripts should be vital for understanding the offender in a broader way. Specifically, crime-scripts need to include goals, emotions, planning, learning, and errors. This is something we find vitally important, and have applied it to the cloud/crime script found in the final section of the current paper.

7. Potential Universal Cloud-Crime Script

Whilst Ekblom and Gill [20] question the usefulness of universal scripts, here we use one as an example to allow discussion on some potential stages in committing a cloud-crime. Using a crime script analysis (involving thematic analysis) on information found in online articles, including clippings in the UK (found on LexisNexis, a search engine for newspaper articles) relevant to cloud crime, a universal crime script was created (see below). Themes were then categorised using a mix of the classic universal stages (preparation, pre-initiation, instrumental initiation, exit), with the induction stage and monitoring stage newly created through the thematic analysis. This should not be seen as a fully completed cloud crime script due to the lack of hardened data, such as transcripts of police investigative interviews, interviews with cloud criminals, Court proceedings, etc. Rather, it should be viewed as a starting point for future discussions.

Our crime-script analysis found two main types of cloud criminal based on two skillsets: (i) **creators** and (ii) **purchasers**. The *creators* are those that actually create and distribute the malicious content - they are the individuals with the programming skillset needed to either be actively involved from day one, or just create the content for personal reasons and have no more to do with an actual crime. The *purchasers* are the mainly everyday individuals who primarily purchase the malicious content – malware, etc – for profit or for chaos. They may have the skillset needed, but instead decide to purchase for sake of ease. They can also be (and this is common) an average person with no programming skillset who can only operate via instructions. We also found three main types of cloud criminal based on motivations: (i) **profiteers**; (ii) **jokers**, and; (iii) **hacktivists**.

In terms of motivations, we found those who would take part in a cloud crime for moral or ethical reasons, a *hacktivist* - an example being the group Anonymous. which is a collective of moral or ethical hackers, joined under the umbrella term Anonymous, often working separately but with no set goals. The *jokers* are those that like nothing more than to cause chaos for self-interests, and take part just for their own personal enjoyment. The most common motivation for cloud crime (it appears) is for profit with the majority of purchasers of malicious cloud malware using it for ransomware purposes (*profiteers*). As Wall [45] argued, the cloud now allows many small crimes to take place instead of one large crime – and this extends to average individuals holding one person ransom via purchased, cloud-based content. Turning now to what sort of social 'being' a cloud criminal is, we found that there were unsurprisingly three types: (i) **collectivists**, (ii) **lurkers**, and; (iii) **lone-wolfs**. A *collectivist* is someone who relies on, and participates in, the community, learning, teaching, boasting, etc. The *lurker* is

the individual who is a member of a community but does not actively participate. They watch and read, and if it is an online community, are never seen. The *lone-wolf* is the criminal who acts outside of any community but does not enter any communities and acts completely alone.

The recent development, and alarming growth, of cyber/cloud crime-as-a-service makes for a very different type of crime-script. Those criminals that purchase malicious malware (or otherwise) with criminal intent, but are not actively involved in the creation of it, will have a different overall process to their crime. They may have the same fantasies, but lack some psychological element (e.g., determination, motivation, intelligence) or situational element (e.g., time, age) to create their own content. A criminal fantasy is the psychological growth of ideas and wants that to take place before any action, and have been linked with deviant behaviour in offenders. The induction phase (and subsequent phases) for these will involve less community involvement, etc. It is for these reasons that the current crime script is based on those who are actively engaged in the creation and distribution of cloud-crime. It is imperative that further work focuses on each type of cloud-crime and criminal - the more accurate a script, the more successful an investigation.

7.1 Example Crime Script

The following example cloud/cyber-crime script was created using a crime script analysis on newspaper articles, and based in the previous work on crime scripts. It differs in parts from pervious crime scripts due the analysis gleaning different phases due to the cyber-cloud factor.

Preparation

Phase 1 - Induction

This includes the development of cybercrime fantasies – those psychological ideas and wants that grow over time - learning about technical aspects, feelings of a political nature (whether experienced by oneself, or learnt in a community – see 'The Silk Road', the first Dark Net market place for selling illegal goods and services. The apparent creator and moderator, Ross Ulbrict, painted the project as a political act, fighting the increasingly oppressing nature of governments). These will include how they interact in online communities dedicated to passing-on knowledge – the formation of a criminal identity. The creators will be technically aware, who will mostly engage with each other online about technology-related matters. There are many communities specifically for cyber-crime available via the Internet, the dark net or some IRC chat group (a text-based communications software) or 4chan thread (an online forum that is infamous for its anonymity of use and therefore darker subjects discussed). This phase holds two areas of high importance to the current paper in: (i) the development of criminal fantasies, and; (ii) the involvement in online communities – such participation could come before, during, or after the development of

criminal fantasies. These are two main areas in which psychology can add a strong understanding, so that less cybercrime occurs, and cyber crime reports to policing/law enforcement agencies are reduced, meaning that valuable resources can be devoted to other areas.

Phase 2 - Pre-conditions

It could be that an opportunity arises due to a system update or a weakness is discovered via some newly created content. It could also be participation in a community where an opening will appear (someone might mention hacking a business cloud, and the community, as a collective whole, take it upon themselves to figure out how to do that). What seems to be the most common is a member of a community will succeed in discovering an opportunity, and will post about it (e.g., to show off), thereby opening the door for others to continue. In terms of a *lone wolf*, this phase will revolve around ideas in their head based on the induction phase. We suggest that a true *lone wolf* requires their own crime script, as their behaviours, emotions, thoughts and experiences will be very different to someone involved in a community.

Pre-activity

Phase 3 - Instrumental initiation

This phase relates to the planning of the crime, the learning of exact knowledge, the finding of weaknesses in a similar system, testing what they have - an iterative phase of 'getting ready' for their planned cyber-crime. The practicing of the crime may be conducted in legal or illegal ways in the first instance. For some cloud-crimes, the instrumental initiation and crime initiation are one and the same, but usually, one would expect to see a testing period, no matter how small, using maybe sqlmap to test for SQL (Structured Query Language) flaws. An sqlmap is a testing tool that automates the process of exploiting SQL flaws and taking over of database servers. Cloud-criminals were found to prey on a number of poorly written content management systems, poorly thought out authentication management processes, and even plain poor passwords that were found during this 'testing' period. While cloud crime can be complex, at times we found better public understanding is vital.

Entry to crime setting

Phase 4 - Crime initiation

This phase is the enactment of the planned crime. Given the wide differences in cloud crimes, this stage will be different in detail on each occasion. For example, differences exist between hacking the iCloud and infecting users with malware for ransom via cloud resources. This phase should be split into the main types of cybercrime based on the role of the cloud (e.g., target, tool, distributor) but should also be based on Wall's (2007) crimes against, crimes with, and crimes using the computer

categorisation. Phases 3 and 4 can be iterative as they plan and test (and re-plan and re-test) while attempting hacks. Whilst it is important to define this phase in terms of the technology, it is vital for any successful crime script to contain as much information about the psychology of the suspect as possible. It is, therefore, essential to describe this phase in terms of the person undertaking the crime.

Phase 5 - Monitoring

This phase will depend on the type of cloud crime that has been committed. For example, an attack like the iCloud hack may be carried out once, then disengaged from the server for good with a monitoring of the result via community or other online means. In contrast, a ransom by malware might be monitored for responses, etc. Thus, there are subtle differences in the type of monitoring conducted before and after disengagement, but what is clear is that cyber-criminals will monitor the crime in all its different meanings. The monitoring stage is important as digital and networked technologies allow crime to happen easier than crime in the non-digital world, with some of the crimes requiring constant engagement and monitoring before disengagement (e.g., ransom). This, potentially, means it is easier to uncover evidence, and therefore the suspect, involved. This is, of course, offset by the Internet's ability to hide the 'footprints' of an offender – it does, however, open-up avenues of investigation.

Post-crime

Phase 6 - Disengagement

This relates to 'leaving' the scene of the crime. Dependent on the type of cloud-crime committed, this may mean different things. However, a 'behaviour' will take place (the crime) and then the 'behaviour' will cease thereby ending the role of the perpetrator in the crime (disengagement).

We believe that because crime scenes can be very fluid and fast-moving, it is not as simple as having definitive phases one after another. We believe our phases outlined above are capable of 'blending' and 'being fluid'. This is something that academic researchers and policing/law enforcement agencies need to be aware of - with flexibility of the Internet comes flexibility and potential erratic criminal behaviour.

8. Discussion

It is hoped we can now start to see how crime scripts can potentially be an essential element in tackling cloud-crime. They act as a common language between different stakeholders, focusing attention and resources on the key phases of a crime. Perhaps, more importantly, they shed light on the psychological elements of a crime as opposed to the more technical elements. The offender's mind seems to be of the greatest importance in the creation of crime scripts - to better understand the behaviours, motives,

feelings, decisions within the process of a crime. The most pressing questions going forward, in our opinion, are those brought up by Ekblom and Gill [20] on the accuracy and fundamental makeup of crime scripts. Are crime scripts event driven or behaviour driven (Ekblom and Gill believing it should be behaviour driven)? How do we define and describe the behaviours? What type of crime script is best and in what situation? These are all fundamental questions and although the current crime scripts are focused enough to guide our thinking, we agree with Ekblom and Gill that it is now time to create a better (more accurate) definition of a crime script.

One of the big questions that cloud/cyber-crime scripts may help with is within the criminal justice system when decisions are being made about the correct policing strategy to tackle cyber-criminals. Should the law be strictly enforced with hackers given harsh prison sentences, or will sending them to prison make the situation worse, by allowing the criminals to socialise with one another, with the potential to develop links with other hackers? Conversely, perhaps they have all the connections they need from their own online communities, given the scope of these communities? What about young hackers that are harder to prosecute because they do not show full criminal intent? One of the major advantages of accurate crime scripts is that they guide intervention policy by policing/law enforcement agencies. A good crime script should not only describe the behaviour and psychology behind the crime/criminal, but also have anchor points for clear interventions to tackle the crime.

Finally, if we look at the example cloud-crime script we presented above, we can see similarities to the Darknet crime script created by Hutchings and Holt [30], as well as the more classic crime-scripts depicted by Cornish and Clarke [14]. The example crime script also has some key differences - mainly in how iterative and flexible the phases look to be, with the addition of a monitoring phase. While the Darknet actors tend to follow a tried and tested formula, the crime script presented here is more fluid. Future, more specific, cloud crime scripts created should continue to show that, this is especially so when we take into account the effect of *digital drift*. Our crime script analysis found many categories of cloud-crime offenders, all of them widely different both psychologically and situationally. It will be interesting to see how these types of cyber/cloud criminal both hold up in future research and how they relate to each other in terms of behaviour during the crime and interactions beforehand through online channels, as well as the influence of digital drift.

8.1 Future Research

We feel that there are four main areas for academic researchers to focus on to give better structure to policing/law enforcement agencies in their investigation of cloud-crime:

1. The role of ‘fantasy’

Understanding not just the individual who fantasizes about a criminal life or a crime, but the fantasies themself. There is a dearth of research in this area but is an area that is central to understanding the potential profile of a cyber-criminal, or at the very least, how agencies can stop a potential criminal before they act. For example, why does a certain teenager fantasize about being a Ross Ulbricht (Silk Road creator) over a Paul Thomas Anderson (a filmmaker)? We all evolve different fantasies and motivations, and understanding why individuals are drawn to cyber-crime over other popular pastimes is vitally important in tackling it. In this example, there may well be a simpler reason, as Ulbricht painted himself as a political rebel. But in other cases, it will not be as easy to understand the qualitative elements that create a potential criminal's mind. There have been many papers exploring this idea of criminal fantasy, but the vast majority relate to sexual predators [15] or homicide [7], with more quantitative rather than qualitative research methodologies employed. We need to understand the subjective qualities of these cybercrime fantasies and their formation during adolescence, and so we call on future work to qualitatively explore these issues.

2. The role of 'communities'

It is clear from the literature [25, 26, 27, 28, 30, 36, 47, 48, 49, 50] that online communities play a major role in inspiring, organising, and implementing online crime. Future research needs to focus on how cloud criminals (and/or potential criminals) are able to access the resources they need to undertake a cloud-crime – this will more than likely mean entering spaces of ethical divisiveness, such as the Dark Net or 4chan (or whatever new installment they have access to [e.g., 8chan]). Both qualitative and quantitative research methodologies must be employed to provide a richer understanding of all the elements Ekblom and Gill discuss.

3. Understanding digital 'drift'

We need to advance the previous work of Goldsmith and Brewer relating to digital drift and in understanding the creation of cloud/cyber crime-scripts. They *"...propose the concept of digital drift to capture some of the mediated effects of the Internet upon criminal commitments, particularly his [Matza, 1964] idea that drift into and out of criminal pathways can often be 'accidental or unpredictable' [p.113]*. In short, the Internet has now allowed what we would consider everyday citizens to either drift (or drift deeper) into criminal spaces, much more easier than before. However, what does this fluid nature of cybercrime now mean for a crime script?

4. Creation of crime-scripts

Precise crime scripts need to be created for all types of cloud (or cyber-crime) that can take place. All types of cloud criminal behaviour needs to be mapped out

which will allow policing/law enforcement agencies the opportunity to be ahead of the game, rather than falling behind.

8.3 Conclusion

We believe that the creation of cloud-crime scripts is an essential activity to be undertaken in the battle against cyber-crime. The exponential growth of cyber (and cloud) crime means policing/law enforcement agencies are struggling to have an effect, and while computer science works on machine learning and data collection automation, psychology and criminology can help policing agencies better understand the mind of a cloud criminal – and not just a static picture, but the process and evolution of behaviours before, during and after a cloud crime.

9. Acknowledgments

This work is part of the CRITiCal project (Combatting cRiminals In The Cloud - funded by the Engineering and Physical Sciences Research Council (EPSRC; EP/M020576/1).

10. Appendix

Term	Meaning
Botnet	A number of geographically separate networked computers controlled by some master (for nefarious purposes)
Cloud-crime	Crime undertaken using the cloud (see below)
Cyber-crime	Crime undertaken using a computer and network
Dark net	A series of networks that can be only accessed using specific software and configurations
DDoS	Distributed Denial of Service – making a network service unavailable by flooding the server with requests
Deep web	The un-indexed, or hidden, parts of the Internet
Malware	**Mal**icious soft**ware**
PGP encryption	PGP (Pretty Good Privacy) encryption allows messages to be sent so only the sender and receiver have the 'keys' to read it
The cloud	A network of networked computers or servers used to store, manage, and process data instead of local computers
TOR network	Free software used to connect to the dark net
Trojans	Malicious software that misleads a user into using it

References

1. Abelson, R. P. (1981). Psychological status of the script concept. *American psychologist*, *36*(7), 715.

2. Aggarwal, A., Rajadesingan, A., & Kumaraguru, P. (2012, October). Phishari: automatic realtime phishing detection on twitter. In eCrime Researchers Summit (eCrime), 2012 (pp. 1-12). IEEE.

3. Anderson, E. (1994). The code of the streets. Atlantic monthly, 273(5), 81-94.

4. Anderson, E. (1999). Code of the Street (pp. 107-141). New York: Norton.

5. Aoki P. M. and Woodruff. A. (2005) Making space for stories: Ambiguity in the design of personal communication systems. In: Proc. CHI '05, ACM, 181-190.

6. Bogatin, D. (2006). Google CEO's new paradigm:'cloud computing and advertising go hand-in-hand'. ZDNet. Aug, 23.

7. Borrion, H. (2013). Quality assurance in crime scripting. Crime Science, 2(1), 6.

8. Burgess, A. W., Hartman, C. R., Ressler, R. K., Douglas, J. E., & McCormack, A. (1986). Sexual homicide a motivational model. *Journal of Interpersonal Violence*, *1*(3), 251-272.

9. Briggs, P., Olivier, P., Blythe, M., Vines, J., Lindsay, S., Dunphy, P., Nicholson, J., Green, D., Kitson, J., and Monk, A. (2012). Invisible design: exploring insights and ideas through ambiguous film scenarios. In: Designing Interactive Systems Conference (DIS 2012), 11-15 June 2012, Newcastle-upon Tyne.

10. Carroll, J. (1995). Scenario-based design: Envisioning work and technology in system development. Wiley, New York, 11.

11. Chiu, Y. N., Leclerc, B., & Townsley, M. (2011). Crime script analysis of drug manufacturing in clandestine laboratories implications for prevention. British journal of criminology, 51(2), 355-374.

12. Cooper, A. (1999) The Inmates Are Running the Asylum. SAMS Publishing, Indianapolis.

13. Cornish, D. B. (1994). The procedural analysis of offending and its relevance for situational prevention. Crime prevention studies, 3, 151-196.

14. Cornish, D. B., & Clarke, R. V. (2008). The rational choice perspective. Environmental criminology and crime analysis, 21.

15. Cormick. C. (2012). Ten Big Questions on Public Engagement on Science and

Technology," Int. Journal of Delibera-tive Mechanisms in Science, vol. 1, no. 1, p. 3550.

16. Daleiden, E. L., Kaufman, K. L., Hilliker, D. R., & O'neil, J. N. (1998). The sexual histories and fantasies of youthful males: A comparison of sexual offending, nonsexual offending, and nonoffending groups. *Sexual Abuse: A Journal of Research and Treatment*, *10*(3), 195-209.

17. Desisto, R. P., Plummer, D. C., & Smith, D. M. (2008). Tutorial for understanding the relationship between cloud computing and SaaS. Analysis, 2(2).

18. Deslauriers-Varin, N., & Beauregard, E. (2010). Victims' routine activities and sex offenders' target selection scripts: A latent class analysis. Sexual Abuse, 22(3), 315-342.

19. Ekblom, P. (1991). Talking to offenders: Practical lessons for local crime prevention. In Urban crime Statistical approaches and analyses. International seminar held under the auspices of Ajuntament de Barcelona Forum des Collectives Territoriales Europeenes pour la Securit6 Urbaine. Barcelona: Institut d'Estudis Metropolitans de Barcelona.

20. Ekblom, P., & Gill, M. (2016). Rewriting the script: Cross-disciplinary exploration and conceptual consolidation of the procedural analysis of crime. European Journal on Criminal Policy and Research, 22(2), 319-339.

21. Ekblom, P., & Tilley, N. (2000). Going equipped: Criminology, situational crime prevention and the resourceful offender. The British Journal of Criminology, 376-398.

22. Gavin, H., & Hockey, D. (2010). Criminal careers and cognitive scripts: An investigation into criminal versatility. The Qualitative Report, 15(2), 389.

23. Go, K. and Carroll, J. (2004). The blind men and the elephant: Views of scenario-based system design. Interactions, 11 (6), ACM, 44-53.

24. Haelterman, H. (2016). Crime Script Analysis: Preventing Crimes Against Business. Springer.

25. Henson, B., Swartz, K., & Reyns, B. W. (2016). # Respect: Applying Anderson's Code of the Street to the Online Context. Deviant Behavior, 1-13.

26. Hillman, S., Procyk, J., & Neustaedter, C. (2014, February). Tumblr fandoms, community & culture. In *Proceedings of the companion publication of the 17th ACM conference on Computer supported cooperative work & social computing* (pp. 285-288). ACM.

27. HMIC Report. (2015). Real lives, real crimes: A study of digital crime and policing

28. Holt, A. (2009). (En) Gendering responsibilities: experiences of parenting a 'young offender'. The Howard Journal of Criminal Justice, 48(4), 344-356.

29. Holt, T. J., & Turner, M. G. (2012). Examining risks and protective factors of online identity theft. Deviant Behavior, 33(4), 308-323.

30. Hutchings, A., & Holt, T. J. (2016). The online stolen data market: disruption and intervention approaches. Global Crime, 1-20.

31. Levi, M. (2008). Organized fraud and organizing frauds Unpacking research on networks and organization. Criminology and Criminal Justice, 8(4), 389-419.

32. Mell, P., & Grance, T. (2009). The NIST definition of cloud computing. National Institute of Standards and Technology, 53(6), 50.

33. Morselli, C., & Roy, J. (2008). Brokerage qualifications in ringing operations. Criminology, 46(1), 71-98.

34. Powell, M., and Collin. M,. (2008). Meaningful Citizen Engagement in Science and Technology. What Would it Really Take?," Science Communications, vol. 30, no. 1, pp. 26-36.

35. Pruitt, J., and Grudin, J. (2003) Personas: Practice and theory. In: Proc. DUX '03, ACM Press, 1-15.

36. Rheingold, H. (2006). Social networks and the nature of communities. In *Networked Neighbourhoods* (pp. 47-75). Springer London.

37. Schank, R. C., & Abelson, R. (1977). Scripts, goals, plans, and understanding.

38. Scotford and Yeung (eds) The Oxford Handbook on the Law and Regulation of Technology, Oxford: Oxford University Press.

39. Somer, T., Hallaq, B., & Watson, T. (2016). Utilising journey mapping and crime scripting to combat cyber crime and cyber warfare attacks. Journal of Information Warfare.

40. Steinmetz, K. F., & Tunnell, K. D. (2013). Under the pixelated jolly roger: A study of on-line pirates. Deviant Behavior, 34(1), 53-67.

41. Sanquist, T., Morris, F., and Mahy, H. (2008) An Exploratory Risk Perception Study of Attitudes Toward Homeland Security Systems, Risk Analysis, vol. 28, no. 4, pp. 1125-1133.

42. Tinbergen, N. (1963). On aims and methods of ethology. Zeitschrift für Tierpsychologie, 20, 410–433

43. Tompson, L., & Chainey, S. (2011). Profiling illegal waste activity: using crime scripts as a data collection and analytical strategy. European Journal on Criminal Policy and Research, 17(3), 179.

44. Wall, D. (2007). Cybercrime: The transformation of crime in the information age (Vol. 4). Polity.

45. Wall, D.S. (2017) 'Crime, security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing', in R. Brownsword, E.

46. Wellman, B., Boase, J., & Chen, W. (2002). The networked nature of community: Online and offline. *It & Society*, *1*(1), 151-165.

47. Westlake, B., & Bouchard, M. (2016). Criminal Careers in Cyberspace: Examining Website Failure within Child Exploitation Networks. Justice Quarterly, 33(7), 1154-1181.

48. Westlake, B. G., Bouchard, M., & Frank, R. (2011). Finding the key players in online child exploitation networks. Policy & Internet, 3(2), 1-32.

49. Whittle, H. C., Hamilton-Giachritsis, C. E., & Beech, A. R. (2014). "Under His Spell": Victims' Perspectives of being Groomed Online. Social Sciences, 3(3), 404-426.

50. Whittle, H. C., Hamilton-Giachritsis, C. E., & Beech, A. R. (2014). In their own words: young peoples' vulnerabilities to being groomed and sexually abused online. Psychology, 2014.

51. Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013). A review of online grooming: Characteristics and concerns. Aggression and violent behavior, 18(1), 62-70.

52. Wortley, R., & Smallbone, S. (2012). Internet child pornography: Causes, investigation, and prevention. ABC-CLIO.

53. Yang, C., Harkreader, R., Zhang, J., Shin, S., & Gu, G. (2012, April). Analyzing spammers' social networks for fun and profit: a case study of cyber criminal ecosystem on twitter. In Proceedings of the 21st international conference on World Wide Web (pp. 71-80). ACM.

54. Yardi, S., Romero, D., & Schoenebeck, G. (2009). Detecting spam in a twitter network. First Monday, 15(1).