Invitation Article

The Modes of Mean(ing)s in Cybercrime Theorising, Analysing, Modelling and More

*M.R. McGuire.**
Senior Lecturer
Department of Sociology, Surrey Centre for Cyber Security
University of Surrey

Abstract

Developing a more rounded understanding of cybercrime is key to enhancing the ways in which we respond to it. This task has often been associated with the process of definition, though options here remain far from satisfactory. But defining cybercrime is one thing, attaching meaning to these definitions is another. In this paper I review some possible ways forward for adding greater depth and substance to what we mean we talk about cybercrime. I consider the role of data collection, theory and analysis in this context and question how helpful these have been in furthering our understanding of digital offending. I then evaluate what seems to be a third, promising option – the modelling of cybercrime activity, whether formally or informally. I suggest this provides a useful synthesis of theory, analysis and available evidence, as well as providing the basis for a more dynamic sense of cybercrime 'in action'. I conclude by setting out details of a recent research project where an economic model of cybercrime was developed. Some implications of this model for our understanding of cybercrime are outlined and reflections offered on the extent to which modelling might provide a useful way forward.

Keywords

Cybercrime, Definition, Meaning, Modelling, Cybercrime Economy

* Direct correspondence to Dr. Michael McGuire; m.mcguire@surrey.ac.uk
* http://dx.doi.org/10.36889/IJCJ.2021.006
* Received 7 December 2021; Revised 8 December 2021; Accepted 8 December 2021
INTERNATIONAL JOURNAL OF CRIMINAL JUSTICE, Vol. 3 Issue 2, December 2021, 3-35

INTRODUCTION

We all know what we think we mean when we call an online crime a cybercrime. Or is it that we think we know what we mean? Or do we mean what it is we think we mean? Or is it somewhere in between? Confronted with these contrasting perceptions a tempting response has been to shrug one's shoulders and echo the words of the seminal K-Pop collective BTS, by saying, 'So what'? If some agree or some disagree with any particular interpretation of cybercrime why should this matter? For as BTS also argued, "if somebody call me right" and "somebody call me wrong" it may be best to just say "So what, let go".[1] Why, in other words should our interpretations of cybercrime have anything to do with framing responses to the problem? Shouldn't we just 'let go'?

To begin with it is obvious enough, as has been pointed out on several occasions (see McGuire 2019a), that there is nothing fixed about the act of calling a crime committed online a 'cybercrime'. It is not as if there haven't been plenty of other terminological options along the way. Why not 'online crime' for example? Or 'e-crime', 'computer crime' internet crime, 'techno-crime', 'digital crime' and so on? The fact that the term cybercrime is now sufficiently familiar and convenient for it to seem like a waste of energy in pursuing alternatives is not in itself a decisive reason to retain it. We may be "stuck with it" (Wall 2007, p.11) but force of habit does not constitute a final condition for assuming that it is any more meaningful (or serviceable) than the alternatives on offer. On the other hand – what's in a name and why would it be worth spending any more time in worrying about this? After all, surely it is the case that names have little bearing upon conceptualisations, or in establishing significance? There are perhaps two reasons why the terminological issue isn't entirely dead, even if it no longer seems very crucial. First is the conceptual baggage that comes with the term 'cybercrime'. That elusive prefix has often seemed like it 'adds something' extra to old fashioned crime – augmenting what has gone before with a frisson of the new or the mysterious. And we might (still) wonder whether this undermines effective understanding of it. Second, the term offers the tempting promise of universality - a rubric under which all the many and complex manifestations of human wrongdoing can be uniformly translated into the new space of the digital. The seeming ease with which the term has been imported across linguistic barriers so widely has reinforced this perception. For example, in Korea 'cyber' is saibeo

1) BTS-"So what" (2018)

(사이버), in Japan it is saiba, in Russia it is kiber (кибер), in Spanish ciber (netico), in Hindi saibar (साइबर) in Turkish siber and in Yoruba simply 'cyber' – and so on and so on.[2] Its presumed universality is even manifested within government circles where ministers often just say 'cyber' as their reference point to any kind of digital issue. But this seeming linguistic universality is at best a de facto one and may imply little more (as seems to be the case here) than a convenient replication of a familiar term.

Beyond the (ostensibly) minor issue of terminology lies the wider question of meaning. We may indeed think we know what we mean by the term 'cybercrime' but if its key criterion – the technology underpinning it – changes and mutates so quickly, can we be sure that our ideas are as stable as we imagine? For even if we could keep the technological element fixed across all its criminal manifestations this would still leave open the thorny question of how technology makes a crime a cybercrime, and what kind of level of causal dependency is at work here. I have dwelt at length on these questions elsewhere (McGuire 2007, 2019) but suffice to say here that they remain unanswered in any very satisfactory way.

At this point the question of redundancy raises its head. If its terminology is so questionable and its meaning so unsure, is a concept of cybercrime worth retaining at all? Why would we need it? After all, we know what crime is, irrespective of whether it is committed using a paper clip, a pocketknife or a PC. And isn't that enough? But whilst dispensing with the language of cybercrime has sometimes been an appealing option, it has never been seen through in any systematic way. The idea of cybercrime seems hard to relinquish, not just because this would seem to fly in face of popular wisdom but also because it ignores the facts on the ground. That crime using networked computers is happening seems indubitable. That it is significant, rising, causes harms to individual interests and may, on occasions, pose existential threats to society is hard to reject. And the fact that its modus operandi does seem to involve important variations on traditional criminal methods remains more than plausible. In what follows I will try to plot a way through this labyrinth of assumptions and find a way of accommodating them, whilst also suggesting a pragmatic way forward.

---

2) Two interesting exceptions here are Mandarin Chinese which has Wǎngluò fànzuì (网络犯罪) and Arabic which has aljarimat al'iiliktrunia (الجريمة الإلكترونية - 'electric referred') as their transcription of e-crimes. Note however that both still invoke the technology as central. For example, wǎngluò meaning "network (computing, telecommunications, transport etc)" and fanzui, crime (or committing one).

THREE RESPONSES

On the one hand then we have been landed with a seemingly indispensable criminological constant – one which has been regularly projected as amongst the greatest threats to the world today. At the same time, it appears to be something with conceptual foundations which lack clarity, depth or substance. Three ostensibly distinct ways of responding to this unsatisfactory state of affairs seem possible:

Sceptical Agnosticism: On this view, whilst the epistemic questions around the terms of meaning and reference of cybercrime may be interesting, they offer no real utility in dealing with cybercrime as an ongoing challenge. Thus, whilst there may be problems in how we think about digital/online/computer crime it is better to press on with gathering as much data as possible and not to worry too much about what this might all mean.

Cyber-Particularism: Conceptual/semantic questions about cybercrime may be problematic for developing a well-integrated approach towards it, but they do not prevent our understanding specific manifestations of online offending. The best response to any epistemic uncertainty is to therefore to keep a tight focus on *particular* cybercrimes, or elements of these – whether this involves the operation of online markets, online stalking or ticket fraud. By developing evidenced understanding of the particularities of online offending, the question of whether there are any useful connections or correlations between them can be postponed or ignored altogether.

Cyber-Universalism: In order to provide the most well-informed response to cybercrime, the epistemic challenges around meaning and conceptualisation are worth trying to overcome. This is best addressed by attempting to fix upon a universal conception of cybercrime. Such a framework is not just attainable but worth pursuing in its own right.

These responses need not be mutually exclusive or independent of each other. For example, one could easily be a cyber-particularist and maintain a focus upon more specific, empirically driven questions whilst retaining the belief that there is some

kind of unity behind the manifestations of online offending which are studied. Similarly, one could be a sceptical agnostic about the meaning of cybercrime or whether specific manifestations of online crime represent anything criminologically distinct whilst never ruling out that they might do. Finally, it is perfectly possible to hold, with the cyber-universalist, that there really is a clear and distinctive conceptual unity to the cybercrime construct whilst accepting that we can only ever find this in the particularities of its specific manifestations.

In other word, these three responses do not represent distinct decisions about the meaning of cybercrime, merely methods for managing best practice (whether as a researcher or a practitioner). What is clear though is that where there has been a decision to treat cybercrime as a real and unique evolution in crime and criminality the optimal response is going to conform with something like a cyber-universalist stance. This does not rule out a degree of agnosticism about what cybercrime actually entails, or that the best way to understand it is through the study of its specific manifestations. But, unlike the other responses, it *does* start with the assumption that cybercrime is something 'real' rather than ending with this. For this reason, it is this position I will assume in what follows, whilst also acknowledging the advantages of the greater caution represented by the first two positions.

Constructing a criterion for cybercrime

Cyber-universalism has tended to centre upon attempts to identify its most obvious and common characteristics. Since this has invariably involved the digital technologies upon which (it seems) to depend, providing a general definition of cybercrime has often resulted in formulations similar to what I will refer to as the 'C_{def}' Criterion:

$$C_{def} = \text{Cybercrime is (T-related) crime involving K}$$

Here T is the variable indicating the technological term to be inserted (digital; computer; network, or sometimes just technology); K refers to the *kind* of crime involved (i.e. stalking, fraud etc) and 'related' is a placeholder indicating whatever relation between T and the crime is considered to hold. This must clearly be some form of causal relation, though its level of determinism is variable and can be thought of in terms of necessary and sufficient conditions. Thus, at one end of the scale is causal *dependency* – indicating a necessary and sufficient relationship between the

crime and the technology whilst somewhere in the middle is causal *enablement* which indicates only a sufficient relationship (cf. Sloman et al 2009, McGuire and Dowling 2013, Salmon, 2020). That is, technology as non-necessary factor in the offending or, more simply still, that the crime could have been committed without it. Even weaker varieties of causal dependency involving the idea of a computer 'assisting' in the commission of a crime have also been invoked on occasions (Wall, 2014). Here computers are merely involved in some capacity (for example being used for a Google search), rather than as a tool central to the crime.

It is worth noting how the structure of C compares to formulations involving traditional crime. For example:

Rape is a crime involving sexual violence: R_{def} = (C, SV)
Fraud is a crime involving deception: F_{def} = (C, D)

The logical form of these criteria indicates a clear difference in that they involve a **two-place** predicate (C, *x*) whilst C_{def} requires a three-place predicate (Cdef = (C,T,K) to indicate that the relation between crime and victim is mediated. And what this suggests is that whilst standard conceptions or crime definitions are associated with a *direct* act of harm against another body or its interests, cybercrimes are not.

How necessary the technology place holder variable in definitions of cybercrime might be has been widely debated (cf. Wall 2007, McGuire 2018a). One reason for questioning this has been where T is substituted for N (referring to a network) as so:

$C2_{def}$ = Cybercrime is (N-related) crime involving X

Whilst it is true that contemporary networks are invariably seen as digital, this hasn't always been the case. Though traditional crime was a largely face to face business, it was also able to exploit certain network effects at times. Such networks might have been wholly socially centred - as in the explosion of new social connections made possible by 19th c urbanisation. Or they might have involved more constructed – though still physical – connections. As for example in the criminal exploitation of transport networks by the highwayman, the pirate and so on. I will return to considerations around connection shortly, but a more immediate question is whether *definitions* of cybercrime like the above also suffice to provide a *meaning* for cybercrime?

Constructing a meaning for cybercrime

The answer to this question appears to be no. A definition, though it can serve as a conceptual criterion, doesn't necessarily convey anything meaningful to us. That meaning and definition are not equivalent is easily shown in the way that a word like 'love' has no straightforward definition but carries a wealth of meanings. Conversely whilst it can be agreed that the following definition:

Copper = the name for the element with atomic number 29 represented by the symbol Cu

is true, it doesn't convey the many associations we attribute to copper (a shiny metal used in electrical wiring; a constituent of bronze; symbol for the 7th wedding anniversary – etc etc.). Thus, whilst definitions for cybercrime like C_{def} can be formulated, more is needed for them to say anything very substantive to us. Meaning used to be associated with reference – those objects or situations in the world to which a word refers. However, this was shown to be mistaken when it was realised that the *same* object can be referred to by words with *different* meanings (Frege, 1948). More generally, it is also clear that it is not possible to derive a semantics of cybercrime from purely syntactic considerations about definitions of terms or the rules governing their application (See McGuire, 2018a for an evaluation of the syntax/semantics distinction in relation to cybercrime). One suggestion for adding substance has been to acknowledge the role of context dependence and the contributions of both the social and the external world in determining meaning (Putnam, 1973). This certainly makes sense for our interpretations of cybercrime where contextual factors such as the techniques used by cybercriminal or the harms done by perpetrators against victims seem as essential to determining its meaning as any abstract definition.

A preliminary observation is that meaning constructions within cybercrime are consistent with at least two of the stances identified above. For example, cybercrime-particularists will look more towards the specific circumstances of what they have uncovered so that the meaning of cybercrime (for them) will tend to reside in their datasets and the observations made on this basis. By contrast, cybercrime-universalists will try to associate such observations within the more general pattern of cybercrime which they perceive. Not only does this emphasize that there is, as yet no general agreement about what is needed to make definitions of

cybercrime properly meaningful and that something additional is needed to plug into them. It also suggests that, as with the study of other social phenomena, other epistemic processes – most obviously *theory construction* are required for the pursuit of meaning. I will therefore begin here, before moving to the related process of *analysis* and finally my own suggestion for securing meaning – the process of modelling where both theory, data and analysis come together in fruitful ways.

Theory: Though the most obvious starting point for providing a meaning for cybercrime is to accommodate it within a theoretical framework of some kind, such frameworks have been far less developed than one might imagine. The application of *criminological* theories to cyber-criminality has been the most frequent strategy of this kind though, as suggested below, their use has sometimes been a little uneven. Far less common has been the development of new theory, tailored towards the novelty of cybercrime. This may be because it is still early days – cybercrime remains a relatively new phenomenon in the history of crime. Or it might just be that attention has been more preoccupied with empirical than with theoretical concerns.

Of the available theoretical positions which have seemed applicable to digital crime phenomena it is perhaps the routine activities approach (Cohen and Felson, 1979) which has found the widest favour. As far back as 2001 Peter Grabosky suggested this as one of the more promising theoretical directions (Grabosky, 2001) and there have been attempts to apply it to a range of cyber-offending contexts ever since (cf Reyns, 2017). For example, website defacement (Howell et al 2019); insider cybercrime victimisation (Williams et al 2018); spam distribution (Perkins et al. 2020) cyberstalking (Reyns et al., 2011); identity theft (Williams 2016); malware (Kigerl, 2021) and even cyberterrorism (Holt et al 2021). The appeal of routine activities as a way of providing meaning to cybercrime parallels its attractions in the context of traditional crime. By framing criminal acts in terms of their intersections between three key variables, the (suitable) target, an offender who is motivated in some way and the gaps provided by an absence of any effective guardian, a seemingly straightforward and flexible way is offered for understanding (and responding to) them. In turn, these 3 factors appear to translate across unproblematically into cybercrime contexts. For example, a motivated offender might be an advance fee phishing fraudster, a target the victims banking details and the failure to provide effective account security by the bank an absence of guardianship.

On the other hand, it is not clear that these often mechanical applications of a routine activities framework tell us very much about cybercrime that we don't already know. After all, it is trivially true that any crime involves a criminal or criminals. And irrespective of whether it is a digital or a terrestrial crime there is usually some kind of target or reward they are after - an objective made far easier where the means to stop them are lacking. Routine activities-based approaches have also been criticised for conflating the kinds of space available to criminals operating in physical contexts with those in digital contexts (Yar, 2005). The spatio-temporal compression (Harvey, 1990) which typifies online interaction means that time is not fixed (offending can be asynchronous) and the space between offender and target is usually not equivalent to what is feasible within traditional crime. In fact it is precisely these spatio-temporal differences that have led some to seek reasons for identifying meanings of cybercrime that transcend the resources of traditional criminological theory (see below).

Another theoretical approach which has often been invoked in trying to make sense of cybercrime is Social Control theory – the idea that offending results from low self-control (Hirschi, 1969, Gottfredson and Hirschi 1990). Poor self-control arises where there are few stakes in conformity, for example a lack of social attachments, limited ambitions/interests and minimal levels of belief in social institutions. Low self-control has been used to explain issues such as digital piracy (Moon et al 2010); cyber-victimisation (Nodeland, 2020) and hacking (Back et al 2018). There have also been attempts to show how control theory might apply beyond such frameworks (Donner et al 2014). Like routine activities-based approaches, there have been frequent claims of empirical corroboration for control theory when applied to cybercrime, though this has not always been borne out by studies which sometimes appear inconsistent with each other. For example Bossler and Holt (2010) took their use of the Grasmick et al. (1993) scale — (which measures low cognitive forms of self-control) — to suggest that low self-control could be associated with unauthorized password access and file tampering, But this conclusion was challenged by other researchers (Ngo and Paternoster, 2011) who found that low self-control had **no** significant effects on phishing or virus infection victimization when they used the same cognitive measure (see Louderback and Antonaccio 2021). It is also worth bearing in mind that if it were possible to show that control theory is able to cross the digital divide then this divide would cease to matter. Since Gottfredson and Hirschi's claim is that their theory provides a general approach to (all) crime, any search for the

meaning of cybercrime then becomes redundant, since there would be nothing ultimately very distinct about it.

Elsewhere, social learning approaches have also found some applications in the cybercrime context (cf Bowman & Freng, 2017), though examples are not extensive. Early studies looked especially at the way socialisation at college level sometimes persuaded young people to engage in cybercrime (Skinner & Fream 1997). And this theme has persisted, for example in the explanation of software piracy. Here the sharing of technical skills amongst young people and their gradual familiarisation with hacking communities was used to make sense of the spread of piracy and the perception that it is 'not real crime'. (Burruss et al., 2012). More widely, the use of social learning approaches to *predict* digital offending has also been proposed (Dearden and Pati, 2021).

Other applications of criminological frameworks to cybercrime have included Mertonian strain theory (Chism & Steinmetz, 2017); labelling theory (Turgeman-Goldschmidt, 2008, Payne et al 2019) and subcultural theory. The latter has found particular (though predictable) applications to hacking subcultures (Steinmetz, 2015, Collier et al 2021) and online forums (Bada et al 2021). However, surprisingly unexplored has the been the relations between subcultural formations and the impacts of online 'filter bubbles' – especially those implicated in the dissemination of crimes involving online hate or disinformation. Still less common have been the application of tested frameworks like white collar crime or youth gang crime to explain cyber offending characteristics (cf. Payne, 2018, Sela-Shayovitz 2012), and far more research is needed in such areas if more nuanced meanings of cyber criminality are to be drawn out.

By contrast more novel theoretical approaches to cybercrime have been few and far between. One more developed example is (so-called) space transition theory which suggests differences in behaviour where people move from physical to cyberspace – in particular the way that criminal tendencies which might be repressed within the physical domain are able to find expression within this extended digital medium (Jaishankar, 2008 Schmalleger & Pittaro, 2009). However, it is not clear whether this offers any more insights into cybercrime than what was identified with Suler's famous 'online disinhibition effect' (2004). Nor is it obvious whether the internet is always used for crime in the way the theory suggests (c.f Holt and Bossler p. 93) More radical uses of spatial concepts can be seen in the suggestion that what cybercrime 'is' - and

therefore what it ultimately means - is precisely to do with reorientations of spatial experience and the nature of social interaction that come with digital networks. The suggestion is that with these comes a wholly new kind of space - a 'hyperspace' - one that reflects the hyperconnected nature of contemporary life (McGuire 2007) and which produces *hypercrime* rather than cybercrime. However, these more radical interpretations of what cybercrime might mean have not yet been taken up very widely.

Whilst the examples cited here are certainly not only the theoretical frameworks which have been applied to cybercrime, they offer a fair representative selection of what has been tried. But a recurring problem in finding meanings for cybercrime in this way has been the rather fragmented applications of theory and the minimal agreement between scholars over which approach might be the most efficacious. And whilst theory is a useful tool, it can often seem a little remote from the facts on the ground. Perhaps more crucially, few of the theoretical frameworks which have been applied have had very much to say about the *technological* aspects of cybercrime. Aside from a few isolated examples, such as attempts to utilise actor network theory (Brown 2006, Van der Wagen & Pieters, 2015), serious engagement with what it is about digital technology which makes crime 'cybercrime' remains limited. Thus, in applying criminological theory it is unclear whether we understand the meaning of *cybercrime* any better or whether the outcome is, in the end, more about developing a better understanding of criminological theory.

Analysis – Another common way of providing a meaning for what we encounter in the social world is to break it down into component parts. This is the process of analysis, a process often contrasted with *synthesis* (where component parts are assembled into a kind of whole). Most physical science is analytic in this sense – physics finds meaning and understanding in the world by breaking down natural phenomena into elements and the forces acting upon them. Social science often aspires to the same thing but of course runs into the problem that its analytic components – human subjects – are not inert. Rather, they constitute a pre-existing intersubjectivity where meaning is indexical to individuals and therefore very hard to break down further into elements suitable for analysis. Within the cybercrime context, analysis has tended to take two forms – simple and complex. Its first, more simple application has usually involved straightforward <u>*descriptive*</u> analysis centred upon

quantities such as fraud prevalence, rises in DDos attacks and so on. More complex forms of analysis have included:

Mapping & logging analysis. Such approaches examine phenomena in the online crime world by gathering data about it and then attempting to break this down into indicative patterns and interrelationships. Since there is usually also a strong descriptive component to this approach - with an emphasis upon counting, accessing reliable datasets is essential. Some analyses of this kind have focussed upon causal correlations – for example the relationship between police interventions and the operations of dark markets (Décary-Hétu & Giommoni 2017); the effect of web takedowns on phishing (Moore and Clayton, 2007) or the impacts of education on cybercrime prevention (Bele et al 2014). Other studies have concentrated upon identifying and enumerating specific patterns of criminal activity such as the sale of drugs on social media (Moyle et al 2019); online image based abuse (Henry & Flynn, 2019); internet money laundering forums (Mikhaylov. and Frank, 2016) or the sale of personal information (Holt et al 2016). However, though such exercises are clearly valuable in establishing certain baseline indicators, it less obvious whether their greater focus upon finding the trees rather than the wood informs the meanings we draw from cybercrime very substantively.

Crime scripting analysis. Crime scripting involves a form of analysis which aims to break down crime events into their key stages to produce a kind of step by step 'script' of successful offending. The approach derives much from earlier precedents within the social sciences (see for example Abelson, 1976, Schank and Abelson, 1977) and was adapted for criminological analysis by Cornish (1994). It has been widely applied throughout the field since then (Dehghanniri & Borrion, 2019). Crime scripting has obvious appeal as a method for cybercrime analysis, with (at least) 24 scripting exercises recorded up to 2018 (Dehghanniri & Borrion ibid). For example, online data markets (Hutchings & Holt 2015) and internet trolling (Somer et al 2018). More recent applications have included online sex offending (van der Bruggan & Blokland 2020); online fraud (Junger et al 2020); SQL injection attacks (Leppänen, et al 2020) and sexual abuse via images (O'Hara et al 2020) amongst others. One problem is the degree of subjectivity in how the elements within a script (cast, props etc) are selected since this may compromise generalisation. And whilst crime scripting

contributes structure to our sense of 'what is happening' in specific cybercrime situations it is less clear that it provides the more nuanced interpretations or can demonstrate the wider significance of cybercrime events in terms preferred by a cyber-universalist.

Situational crime analysis Rather than focussing upon offenders or their motivations, situational crime approaches have concentrated more upon the background environment and how this might be doctored to reduce its appeal for criminal exploitation. Though this form of analysis has an overtly preventative rationale, its capacity to evaluate the cybercrime environment might also provide some resources for interpreting it. As with its applications to crime in general (see Clarke 1995), analysing cybercrime in situational terms essentially follows the routine activities approach by breaking crime events down into three key parameters – risk, opportunity and reward. For cyber criminality, environmental risks could include the strength of prevention processes like network security, where inadequacies then bring opportunities. For example, weak phishing controls or unpatched systems. Rewards might be purely financial – such as access to customer accounts, but could just as easily include, data, CEO emails, intellectual property and so on. Examples of situational crime analysis in the cybercrime context have included its application to online child pornography (Me & Spagnoletti 2005), information security (Hinduja & Kooi, 2013); the use of money mules (Kleemans & Leukfeldt, 2019); insider cybercrime (Willison & Siponen, 2009, Stockman, 2014), online piracy (Basamanowicz and Bouchard, 2011); cybercrime prevention (Brewer et al 2019) and cybersecurity in higher education (Back & LaPrade, 2020). Given its (relatively) long history a number of critiques have been raised against SCP-based analysis, any of which could also stand where it is applied in cybercrime contexts (cf. Wortley 2010). In particular, such analyses have often been charged with failing to consider displacement effects. Thus, an evaluation of a prevention measure as successful against cyber-attacks may overlook the fact that the hack or intrusion is then transferred or attempted elsewhere. There is also the problem that, since SCP analyses are more concerned with the circumstances of cybercrimes and how they unfold than with the offenders behind them, they are unable to detail the motivations behind any attack. This has some obvious drawbacks in the cybercrime context where one attack can often look very much like another from the outside. But suppose we have one

DDos attack mounted by a teenager seeking to demonstrate their skills, another by a cybercrime gang in search of 'Fullz' datasets and another still by a Nation state which aims to disrupt business activity. Being able to distinguish the intentions behind these Ddos attacks would seem to be an important factor in understanding them. Finding out who did it and why is likely to be just as valuable in determining meaning as identifying perimeter vulnerabilities. Certainly, it seems unlikely that providing for meanings for cybercrime can be wholly separated from acquiring a sense of the protagonists and their aims.

Social network analysis. Given that cybercrime can very plausibly be thought of *as* networked crime, (no network, no cybercrime), applying social network analyses appears to be a promising option. A wealth of potential insights and meanings seem likely to be drawn here by finding typical network structures or patterns within cybercrime activity. For example, better understanding of the ways in which illicit money is filtered through payment mechanism chains; clarifying who particular kingpins might be; finding distribution hubs and so on. Though SNA has not perhaps been applied as widely to cybercrime as might be expected, certain examples have pointed towards its potential going forward. Amongst these have been analyses illustrating the form and operation of hacker communities (Lu et al 2010); illicit activities on social media (Geetha et al, 2020); cyber-attacks on enterprise (Sarkar et al, 2019); cybercrime groups in China (Yip 2011); organised cybercrime (Leukfeldt 2015) and underground forums (Pastrana et al 2018) amongst others. However, an obvious concern with SNA based approaches is that whilst they are good on structure, they tell us far less about the *substance* of cyber-offending and this, as suggested above, seems to be an indispensable component of finding meaning in it. There is also a problem with potential triviality, in that almost any collection of elements can be interrelated to form a network Thus it is not always clear that SNA tells us anything particularly novel or surprising in more general terms about cyber criminality.

This catalogue of analytic approaches is by no means exhaustive. For example, there are also analytic tools available within other fields, most obviously psychology which look promising. Given the need to understand why cybercriminals think and act in the way that they do, psychological analyses of hackers (McAlaney et al 2019), of cybercrime victims (Van de Weijer & Leukfeldt, 2017), or the rationales of cybersecurity (Taylor-Jackson et al 2019) all seem likely to add to our understanding.

In isolation however analysis alone seems unlikely to deliver everything we need to develop effective interpretations of cybercrime. Taking something apart doesn't necessarily tell us how it works and certainly not what it signifies in wider social contexts. Combining analysis with theory might be a way of bridging this gap, though how remains uncertain. Overall, when evaluating the rather fragmented way in which both theory and analysis have been applied to cybercrime it is hard to resist the conclusion that these have been more like 'suck it and see' style exercises, than consistent or properly integrated programmes of study. For this reason, it may be that the third, modelling-based approach I will now consider, offers a more promising option for determining meaning in the longer term.

Modelling Cybercrime – an economic approach

Modelling aims to provide explanation in terms of models or simulations which create dynamical representations of clusters of activities at greater or lesser levels of detail and sophistication. I suggest it represents a more robust potential combination of theory and analysis in that the link between abstract (theoretical) frameworks and the way these are 'filled in' with data is far more transparent. Modelling in the social sciences have tended to pursue largely mathematical approaches, though there has been a shift towards agent based & game theoretic approaches more recently (Mershon & Shvetsova 2019). This has yet to find many applications within the cybercrime field, with some notable exceptions. For example, Onuchowska & Bernt (2019) utilised an agent-based approach to model malicious behaviour on social media whilst Basuchoudhary & Searle (2019) used a game theoretic model to highlight business responses to trade secret theft. Overall however, it has been within the cybersecurity field where we tend to see more of these kinds of models (see for example Rajivan et al 2013, Thompson & Morris-King, 2018 & Ashiku & Dagli, 2020).

More typically, modelling within cybercrime research has taken an informal 'heuristic' style approach. For example, Porcedda & Wall (2021) used an informal modelling approach to show how cyber-enabled data-crime influences cyber-enabled offending, whilst the use of non-mathematical modelling has also been seen in attempts to outline itemize the key features of a cybercrime 'ecosystem (cf. Broadhead 2018, Dupont 2019). Though these more informal approaches do not yet outline any consistent methodological approach, certain advantages can result where they are

conducted effectively. One benefit is to provide succinct yet dynamic snapshots of cybercrime 'in action', a useful counter to its often very static representations within many research approaches. Another is to provide a way of accommodating the various stances outlined earlier. For example, the fact that models can be applied directly to cybercrime scenarios without the need for a prior theoretical framework means that it is consistent with cyber-particularism. At the same time a cyber-universalist position can be supported by basing models upon theory and then testing to see how far data supports or refutes this.

To indicate some of the potential advantages of this approach to cybercrime and to conclude this discussion I will set out the contours of an informal modelling exercise conducted between 2018-21 (McGuire 2018b, 2019b, 2019c & 2021). This project had the initial aim of extracting some sense of how cybercriminals might spend their ill-gotten gains, but as it became apparent that other considerations needed to be built in to even pose this question it was soon obvious that something close to a model was under development – albeit one with uncertain boundaries and driven by a certain amount of educated guesswork. A first complication was that no estimate of the spending of cybercriminals could be made without knowing how *much* they have to spend. This in turn led straight to offending itself and the motivational backgrounds to this. Whilst motivations for cyber criminality may vary from revenge to sexual fulfilment, financial reward was the obvious motivation to explore in the context of understanding spending. When operationalised in terms of the pursuit of revenues, metrics could be derived from the key *methods* of generating revenues by cybercriminals which emerged. The research found a surprisingly wide range of activities here, from the more obvious varieties like fraud, through to more novel techniques such as selling advertising space on crimeware sites.

With agents directed towards various methods of revenue generation in place, other components of the model then began to emerge. For example, there are the targets and victims of such revenue generating schemes and in tandem with this the *quantity* of revenues cybercriminals are able to generate. Overlaid upon these variables were at least two further factors, both related to *where* these revenues go. Revenues may initially need to be moved around or concealed – so providing some sense of the connections between cybercrime activity and the wider field of (digital) money-laundering (Berghel, 2014. Albrecht et al. 2019). Finally, the ultimate point of disposal of the revenues need to be built in. This was found to take various forms,

from straightforward conversions into desirable commodities to more considered forms of disposal such as investment, or even their use in supporting further crime. Further complexity was added to the model by considering the kinds of *currencies* used to mediate the flow of revenue generation and transactions, with digital and crypto-currency the obvious tools driving these cycles. Some consideration was also paid to factors like production centres (where certain types of revenue generate activities are geographically focussed) and the size and type of criminal organisation involved in revenue generation.

One recognised advantage of models, especially in agent-based forms is that they are able to capture *emergent*, unexpected phenomena (cf. Bonabeau, 2002) – something not so easily accommodated within analytic or theoretical approaches. And what soon emerged from the model here was something close to an *economy* – a dynamic map of interactions amongst cybercrime (and other) actors based upon production, consumption and wealth generation. It also became apparent that this model of illicit digital relations conformed closely with economic patterns seen elsewhere within contemporary digital societies. For example, as traditional economic models based upon straightforward supply, demand and resource allocation have had to adapt to a more dynamic globalised world it is striking how the *movements* of wealth and the symbolic extensions of these (into data and so on) are now almost as important as the production of wealth itself. Thus, in the hyperconnected social world we inhabit the "power of *flows* takes precedence over the flows of *power*" (Castells, 1996, p. 469). Modelling cybercrime in terms of the very simple range of variables outlined above not only helped make this feature and its role as a wealth generator more obvious, but it was also able to illustrate the extent to which cybercriminality now feeds off the legitimate economy.

Understanding the meaning of crime through the lens of economics is not, in itself new of course. Becker's work in identifying seemingly useful correlations between the severity of punishment and a (rational) criminals' evaluation of how this compares to the benefits of violating the law represented an early foray into this kind of thinking (see Garoupa, 2014). Other applications of economic thinking have included attempts to apply theories of the firm and the dynamics of markets as a tool for understanding drug markets (Rottenberg, 1968; Moore, 1970; Fugii, 1975), or organized crime activity (Schelling. 1967; Rubin, 1973). Further studies have looked at the way economic theory in general might be useful in limited contexts (see for

example Orsagh, 1983). In a slightly different vein the Market Reduction Approach (MRA) (Sutton 1998, Sutton et al 2001) drew upon economic concepts around the market and market behaviours to develop a form of crime prevention based upon disrupting stolen goods markets.

Within cybercrime research itself economic thinking has most often tended to manifest itself within the 'cybercrime as a business' trope (Manky, 2013 NCSC 2017, Parise, 2019). However, the problem with this line is that it has tended to be more of an exercise in description than elucidation. We don't learn much, other than the fact that cybercrime activity sometimes resembles business activity by- for example – selling certain (illicit) commodities or being profit oriented. Worse, by simply seeing it as crime with economic *components* rather than as an integrated set of economic relations, a rather static portrait results. By contrast, modelling it more dynamically - as an integrated economy- more substantive insights related to the flows manifested within this economy and their interdependence become clearer. For example, by breaking down revenue generation into just 5 of the better evidenced modalities it was possible to build up a more connected sense of the key relationships in the flows connecting criminal profits, their destinations and what happens in between. In turn, this enabled some new insights into the modus operandi of cybercriminals and where cybercrime as a whole might be going.

Initial evaluation suggested that between 2018-19, activities in these five revenue categories were generating approximately:

Illicit/illegal online markets: $860bn per annum
Trade Secret/IP theft: $500bn per annum
Data Trading: $160bn per annum
Crimeware/CaaS: $1.6bn per annum
Ransomware: $1bn per annum

When totalled, these five categories implied that around $1.5 trillion in revenues is now available to cybercriminals annually.[3] And this, to be clear, was a fairly conservative estimate. Many other kinds of revenue generating activities were not considered and even within the five chosen categories estimates were always targeted

3) For details of how these and other estimates were arrived at, see McGuire (2018b, 2019b, 2019c, 2021)

towards the lower, rather than the higher revenue range. An obvious preliminary conclusion was that the size of the cybercrime economy is now very significant. Not only is it worth more than the total profits of the top 3 Fortune 500 companies, it also often matches or exceeds the GDP of many nation states (the annual GDP of Saudi Arabia is around $.75 as a comparison). Of course, some caution is necessary in interpreting agency here. There is no directed or collective synergy in the acquisition and disposal of these revenues, as there would be with an orthodox economic actor like a state or a company. Cybercrime actors tend not to share or jointly invest their profits. But the figures, no matter how undirected or provisional, provided several useful insights.

First, by indicating how much money is available to the cybercrime economy a firmer sense of the potential criminological significance of cybercrime was attained. Second by better understanding the relationships between cybercriminal activities and their revenues a more topographical, 3D picture emerged indicating where activity is most pronounced and what the key pulls of attraction for cybercriminals might be. And what was immediately striking here was that it was not so much the 'obvious' forms of cybercrime activity – such as ransomware attacks[4] - where the real money is being made, but in the more mundane activities associated with trading. Thus, the $860 bn in revenues being generated by illicit online sales clearly outstrips all others by a considerable amount. As a result, it might well be asked whether the sensible cybercriminal would be better off selling prescription drugs than trying to hack into a bank. The full implications of this imbalance are too complex to consider here[5] but there are clearly important questions about the focus of cybercrime activity to unravel as a result.

Third, by identifying this reservoir of illicit profits we can begin to draw

---

4) In 2020 it is estimated that known ransomware profits (i.e. those which got paid) came to around $370 million (Cimpanu, 2021). Though this represents an increase of over 300% increase over known 2019 earnings, it was below the estimated amount detailed in the Web of Profit research, probably because that also allowed for unreported payments. And it was still some way below the other revenue totals. Thus, whilst ransomware can be highly disruptive it is not necessarily the most profitable cybercrime activity. Nor any longer is it one of the safer ones. As ransomware attacks (especially the larger ones) have started to attract increasing attention from law enforcement and other agencies intervention and enforcement has begun to increase. See for example the recent arrest of members of the REvil ransomware group (DoJ 2021).

5) Though see my forthcoming (McGuire 2022) for some interpretations of what this might mean for cybercrime in the medium to long term.

inferences about where these are ending up and what that might imply. In particular, given these funds are illicitly generated, it is clear that a sizeable chunk of them will end up swilling around in the estimated 2 - 5% of global GDP currently circulating illegally around the world (around $800 billion - $2 trillion (UNODC 2011)). In this way, not only did the model help throw some additional light upon the murky world of money laundering, but insights into the contribution of digital deviance to this, most obviously in the use of bitcoin or other crypto currencies. Around $2.8 bn was estimated to have been laundered through cryptocurrency exchanges in 2019 (Chainanalysis 2020), so any additional steer on this is likely to prove beneficial in enhancing our understanding of the interweaving between the licit and illicit economies. Indeed, it raises many questions about how closely connected legitimate and criminal business activity now is – a point I will return to below. Finally, the modelling exercise also helped refine some of the questions about the modes of meaning around cybercrime which this paper is considering. For example, there have often been questions as to whether selling counterfeit or other goods through illicit markets should really be counted as 'cybercrime' in the truest sense. Yet if this contributes to the cybercrime economy in the way the model suggested, why wouldn't it?

Another way in which a modelling exercise like this can enhance our sense of what cybercrime might mean is by way of its flexibilities. Given the economic angle to the model, obvious sites for further analysis present themselves - not least other online contexts where trading activity can be discerned. One immediately interesting suggestion here was the challenge to assumptions that it is on the darknet where most economic cybercrime activity is conducted. Whilst there is clearly a substantial space for revenue generation provided by these 'hidden' markets, the so-called ''clear/open net" turned out have a far greater role in supporting the cybercrime economy. This was especially the case with social media platforms which appeared to be flourishing sites forcybercrime activity. Thus, it emerged that criminal revenues from fraud enabled by social media had increased by over 60% between 2017-2019 and certain activities - drug dealing most obviously - were being conducted within plain sight. One recent survey has suggested that 72% of young people have reported seeing illegal drugs advertised for sale on social media sites or apps every month (McCulloch & Furlong, 2019) and our research found that drugs were available for sale across a significant number of the platforms that were studied. And here too, received wisdom is not always reliable when such activity is modelled in more detail. For the research

again showed that it is in less spectacular activities where some of the real gains may lie. Thus, around $1.9bn was being generated through illegal pharmaceutical sales (i.e. prescription drugs) on social media – far in excess of the $290m or being made from the financial frauds enabled there. Nonetheless the fact that such frauds were being so openly conducted represents an obvious threat to social media users, as does the role of such platforms in generating around $138m from romance/dating fraud. Other categories of cybercrime revenue generation on social media were less predictable – for example around $250m being made from the distribution of Crypto mining malware. Also surprising was just how much common or garden cybercrime activity was going on, with 30-40% of the social media platforms inspected for the report having accounts offering some form of hacking service. The use of digital media for more traditional crime was also evident. For example, young people's readiness to use social media to communicate via provides an obvious angle for exploitation, so the 36% rise in the use of social media platforms between 2017-2018 to recruit money mules under the age of 21 was no surprise.

The value of an economically oriented model was also evident when extended to the more obvious site for cybercrime activity - the darknet. Credible estimations of revenues here have proved all but impossible to obtain given the numbers of active vendors and their reluctance to say very much about their operations. This means it is very hard to be sure how many transactions are successfully completed, let alone their total volume or value. However, since bitcoin or cryptocurrencies now represent an almost universal currency in dark market commerce, examining these transactions provides another method for obtaining a firmer grasp on how the darknet fits within the cybercrime economy as a whole. One study has suggested that the value of darknet trading had reached something like $1bn by 2019 (Chainanalysis, 2020). Whilst this doesn't tell us *what* is being traded, or what level of profit this represents, it does give us some insight into the revenues available through the darknet site for cyber criminality. And this in turn supports the conclusion alluded to above – the fact that it still lags behind revenues available from the clear net. Our analysis of the type of listings to be found suggested that around 25% of the total content involved items such as counterfeit goods - indicating again that it is old fashioned trading, rather than spectacular hacks which represent the bread-and-butter activities for cybercriminals. And this trade, fairly predictably, involves more familiar commodities rather than those which are overtly cybercrime related. Of the 70,000+ listings examined in the

research, 47% were related to drug or drug-related sales, while just under half (43%) were related to digital products like compromised bank accounts, malware, DDoS tools, or stolen card credentials. Six percent represented 'services' like hacking tutorials.

Also revealing was the fact that individual victims appeared to emerge as less of a target than enterprise and other social institutions within this trading environment. For example, where listings from drugs were excluded, we found that 60% of the digital products and services traded on the dark net represented direct opportunities to harm the enterprise. 15% of content could be associated with more indirect forms of harm to the enterprise (e.g. reputational damage). And of the vendors who were directly questioned at least 60% said they could offer access to more than 10 business networks; 30% offered access to between 5-10 and 10% were offering access to up to 5 networks. As might be expected - malware and DDoS/botnet tools represented the most frequent types of threat from the dark net in relation to network compromises; constituting an average of around 45% of listings examined (25% for malware and 20% for DDoS).

But perhaps the most telling indicator of the growing influence of the cybercrime economy is the way that nation states have become implicated within it. Whilst the threats posed by nation state attacks are now familiar enough, the role of the cybercrime economy in supporting and enabling their actions has been far less discussed. An analysis of nation state attacks between 2019-2021 was conducted suggesting that around 50% of them involved low budget, straightforward tools easily purchased on dark net, or other cybercrime markets. Around 20% involved more sophisticated custom-made weapons such as targeted malware or weaponised exploits, probably developed within dedicated state cybersecurity programmes. Crucially, many of these tools have themselves now been acquired and traded across darknet sites. For example, Eternal Blue - just one of the tools acquired from the US national security agency in the notorious 'Shadow brokers' hack has now helped compromise over 5 million computers worldwide; caused several billion dollars of losses to businesses and governments globally and generated in excess of $500 million in revenues for cybercriminals (Cf. Perloth & Shane, 2019) More recently, data stolen from multiple US government agencies during the SolarWinds hack has been reputedly advertised for sale on the dark net for over $1 million.

The interweaving of the cybercrime economy with the ongoing struggles in

cyberspace could be interpreted even more radically. Given the apparent dependence upon cybercrime activity on the part of some nation states (it could be argued that something like ‘cyberwar economies’ have emerged with nations profiting openly from the tools, services and revenues these illicit activities are now producing. One relatively well evidenced example here has been the case of North Korea (DPRK). Most experts believe that it has been able to combine methods of generating revenues from cybercrime with digital innovation. One approach has been bank robbery - albeit in contemporary forms like cryptocurrency theft coupled withransomware operations andmoney laundering. For example, a well evidenced set of cyberattacks on cryptocurrency exchanges in 2017 generated revenues equivalent to $571 million for the North Korean Lazarus APT group in that year alone. The group used phishing and other techniques to access the exchange, providing a useful way of supplementing the North Korean government’s limited access to foreign currency. Similarly, North Korean groups, probably government sponsored, were involved in a 2016 attack using SWIFT credentials from Bangladeshi Central Bank employees to engineer an $81 million transfer – one of a series of attempted heists from banks in South East Asia by the group. In 2018, the group switched their attention to ATM hacks, successfully engineering them into paying out millions of dollars on command using a specially adapted Trojan. A 2021 report by the UN has suggested that over $300 million generated by the DPRK in 2020 through cybertheft was used to fund its nuclear and ballistic missile programmes (Roth and Berlinger, 2021).

However, the benefits of the cybercrime economy are not restricted to smaller nations. For example, our analysis suggested that cybercrime related activities sponsored by China may now generate an equivalent of 10% of the value of its exports. Indeed, the increase in revenues for the Chinese economy is equivalent to total income from high profile exports like textiles (worth c$239bn to the Chinese economy in 2017). Similarly, the Russian economy now benefits from an additional $600m+ annually (at minimum) from carding operations alone, with cybercrime activities generating revenues around three times the value of arms/weapons exports for the Russian economy. And even where the economic activities are ostensibly legal, cybercrime is fuelling nation state GDP in significant ways. For example, Israel’s cyberwar economy benefitted by around $1.19 billion in 2017, with over 20% of global investment in cybersecurity being directed there.

Conclusions: Meanings in the modes of Cybercrime?

If the meaning of cybercrime amounts to nothing more than formulating a definition for cybercrime then, as this paper has suggested, not much can be concluded. Definition is not equivalent to meaning, so the standard way of characterising cybercrime as 'internet/digital/technology/etc crime', even if this were satisfactory (which I have argued it is not), doesn't begin to explain the depth and breadth of what (we think) it signifies. Gathering data, developing theoretical frameworks, or applying different forms of analysis seem like obvious ways of trying to bridge this gap between definition and meaning but each appears to be wanting in some way. In particular, simplistic exercises in applying established criminological theory or drawing upon recognised analytic tools has often seemed to be more about stamp collecting than providing genuine understanding. And the risk of intellectual noise arising from far too many attempts to apply far too many tools to find meaning is a real one confronting researchers.

If then cybercrime really is as novel or poses as much of a threat as is often held, the current situation represents a failure of the criminological imagination of the highest order. Too often the catastrophising of cybercrime has pushed researchers more towards finding 'interventions', 'disruptions' or 'solutions' than advancing explanation or finding meaning. But criminological understanding surely ought to be about more than providing a service industry for law enforcement or policy makers. At present, the best ways forward seem to be to attempt to carve out some form of synthesis between these options, perhaps in the form of models of greater or lesser rigour though even here reaching an optimal balance between the evidence and what we can say about this evidence remains uncertain.

Whilst this discussion has tried to pose some wider questions about the understanding of cybercrime it too remains very much within the confines of academic, rather than public discussion. This kind of insularity is of course a general problem for research, but we might wonder whether, in the context of what appears to a problem with such sweeping societal implications – extending from nation states down to teenage money mules – whether this is satisfactory. For what is never touched upon in questions of meaning is what cybercrime means to *others*? Here any duty of criminology to be 'public' (Loader & Sparks 2010) does not reside solely in making its findings palatable for policy makers, but accessible to everyone. Given current concerns about the way that public understanding of fact, truth and meaning is

being distorted in the mirror of digital mediation this challenge seems especially pressing. Finding a meaning for cybercrime surely also needs to properly represent its relevance to minority as well as to majority groups and to be far more culturally sensitive than it has been to date. But finding *that* kind of mode of meaning in cybercrime remains another story for another day at present.

References

Abelson R.P. (1976). Script Processing in Attitude Formation and Decision Making. In *Cognition and Social Behavior*. Edited by: Carroll JD, Payne J. Hillsdale NJ: Erlbaum.

Albrecht, C., Duffin, K.M., Hawkins, S. and Rocha, V.M.M. (2019). The use of cryptocurrencies in the money laundering process. *Journal of Money Laundering Control*.

Ashiku, L. and Dagli, C. (2020). Agent Based Cybersecurity Model for Business Entity Risk Assessment, *2020 IEEE International Symposium on Systems Engineering (ISSE)*, pp. 1-6,

Back, S., Soor, S & LaPrade, J. (2018). Juvenile Hackers: An Empirical Test of Self-Control Theory and Social Bonding Theory, *International Journal of Cybersecurity Intelligence & Cybercrime*,1(1), 40-55

Back, S. & LaPrade, J. (2020). Cyber-situational crime prevention and the breadth of cybercrimes among higher education institutions. *International Journal of Cybersecurity Intelligence and Cybercrime*, 3(2), 25-47.

Bada, M., Chua, Y. T., Collier, B., & Pete, I. (2021). Exploring masculinities and perceptions of gender in online cybercrime subcultures. In M. Weulen Kranenbarg, & R. Leukfeldt (Eds.), *Cybercrime in Context: The human factor in victimization, offending, and policing* (1 ed., pp. 237-257). Springer International

Basamanowicz, J. and Bouchard, M., (2011). Overcoming the Warez paradox: online piracy groups and situational crime prevention. *Policy & Internet*, *3*(2), pp.1-25.

Basuchoudhary, A., Searle, N. (2019). Snatched secrets: Cybercrime and trade secrets modelling a firm's decision to report a theft of trade secrets, *Computers & Security*, 87

Bele, J, Dimc, M. Rozman D & Jemec, A. (2014). Raising awareness of cybercrime - the use of education as a means of prevention and protection, *10th International Conference Mobile Learning*

Berghel, H., (2014). The future of digital money laundering. *Computer*, *47*(8), pp.70-75.

Bonabeau, E. (2002). Agent-based modelling: Methods and techniques for simulating human systems, *Proceedings of the National Academy of Sciences* May 2002, 99 (suppl 3) 7280-7287;

Bowman, J. and Freng, K. (2017). Differential Association Theory, Social Learning Theory and Cybercrime,in Steinmetz, K. & Nobles, M. (eds) *Technocrime and Criminological Theory*, London Taylor and Francis

Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A. and Maimon,

D., (2019). Situational Crime Prevention,in *Cybercrime Prevention* (pp. 17-33). Palgrave Pivot, Cham.

Broadhead, S. (2018) The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments, *Computer Law & Security Review*

Brown S. (2006). The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical Criminology*, 10(2):223-244.

Burruss, George W., Bossler, Adam M. And Holt, T. J. (2012). Assessing the mediation of a fuller social learning model on low self-control's influence on software piracy. *Crime and Delinquency*, 59(5), 1157-1184

Chainanalysis (2020). Crypto Crime Report. Available at: https://go.chainalysis.com/2020-crypto-crime-report

Chism, K. & Steinmetz, K (2017). Technocrime and Strain theory in Steinmetz, K. & Nobles, M. (eds) *Technocrime and Criminological Theory*, London: Taylor and Francis

Collier, B. Clayton, R.,Hutchings, A. & Thomas, D. (2021). Cybercrime is (often) boring: Infrastructure and alienation in a deviant subculture, *The British Journal of Criminology*, 61, 5, 1407–1423

Cornish, D.B. (1994). Crimes as scripts. In: Zahm, D, Cromwell, P (eds) *Proceedings of the International Seminar on Environmental Criminology and Crime Analysis*. Tallahassee, FL: Florida Statistical Analysis Center.

Donner, C., Marcum, C., Jennings, W., Higgins, G. & Banfield, J (2014). Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy, *Computers in Human Behavior*, 34,165-172

Clarke, R. V. (1995). Situational Crime Prevention. *Crime and Justice*, *19*, 91–150.

Dearden, T.E., Parti, K. (2021). Cybercrime, Differential Association, and Self-Control: Knowledge Transmission Through Online Social Learning. *Am J Crim Just*

Dehghanniri H, Borrion H. (2021). Crime scripting: A systematic review. *European Journal of Criminology*. 18(4):504-525.

Dupont, B. (2019). The ecology of cybercrime in Leukfeldt, R. & Holt, T.J. (eds) *The Human Factor in Cybercrime*, London: Routledge

Garoupa N. (2014). Economic Theory of Criminal Behavior. In: Bruinsma G., Weisburd D. (eds) *Encyclopedia of Criminology and Criminal Justice*, Springer, New York, NY.

Geetha,S. P. Dinesh Kumar, G. Senthil Velan, D. Ali, S & Kanya, N. (2020). Big Data Analysis - Cybercrime Detection in Social Network, *Journal of Advanced Research in Dynamical and Control Systems*, 12,04, 147-152

Harvey, D. (1990). *The Condition of Postmodernity: An Enquiry into the Origins of Cultural Change*. Cambridge, MA: Blackwell.

Henry N, Flynn A. (2019). Image-Based Sexual Abuse: Online Distribution Channels and Illicit Communities of Support. *Violence Against Women*. 25(16):1932-1955.

Hinduja, S. and Kooi, B. (2013). Curtailing cyber and information security vulnerabilities through situational crime prevention. *Security Journal*, 26(4), 383-402

Hirschi, T. (1969). *Causes of delinquency.* Berkeley, CA: University of California Press.

Fugii, E. T. (1975). Heroin addiction and public policy, *Journal of Urban Econ.* 2:181-198.

Gottfredson, M., & Hirschi, T. (1990). *A General Theory of Crime*. Stanford, CA: Stanford University Press.

Grabosky, P. (2001). "Virtual Criminality: Old Wine in New Bottles?" *Social and Legal Studies* 10(2):243–249

Howell, C. Burruss, G., Maimon, D. & Sahani, S. (2019). Website defacement and routine activities: considering the importance of hackers' valuations of potential targets, *Journal of Crime and Justice*, 42:5, 536-550,

Hutchings, A, Holt, T.J. (2015). A crime script analysis of the online stolen data market. *British Journal of Criminology* 55(3): 596–614.

Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). *Data thieves in action: Examining the international market for stolen personal information*. New York: Palgrave

Holt T.J., Turner N.D., Freilich J.D. &Chermak S.M. (2021). Examining the Characteristics That Differentiate Jihadi-Associated Cyberattacks Using Routine Activities Theory. *Social Science Computer Review*, 10

Jaishankar, K. (2008). Space Transition Theory of Cybercrime, in Schallmeger, F. & Pittaro, M. (eds) *Crimes of the Internet*, Upper Saddle River, N.J. : Prentice Hall, pp. 283-296

Junger, M., Wang, V. & Schlömer, M. (2020). Fraud against businesses both online and offline: crime scripts, business characteristics, efforts, and benefits. *Crime Science***9,** 13

Kigerl, A. (2021). Routine activity theory and malware, fraud, and spam at the national level. *Crime, Law and Social Change* 76:2, pages 109-130.

Kleemans, E. & Rutger, E (2019). Cybercrime, money mules and situational crime prevention in Hufnagel, S. & Moiseienko, A. (ed) *Criminal Networks and Law Enforcement*, pp.75-89

Leukfeldt, E. (2015). Organised Cybercrime and Social Opportunity Structures: A Proposal for Future Research Directions, *The European Review of Organised Crime* 2(2), 91-103

Leppänen, A., Toiviainen, T., & Kankaanranta, T. (2020). From a Vulnerability Search to a Criminal Case: Script Analysis of an SQL Injection Attack,

International Journal of Cyber Criminology, Vol. 14, 1**,** 63-80.

Louderback, E. & Antonaccio, O. (2021). New Applications of Self-Control Theory to Computer-Focused Cyber Deviance and Victimization: A Comparison of Cognitive and Behavioral Measures of Self-Control and Test of Peer Cyber Deviance and Gender as Moderators, *Crime and Delinquency*, 67, 3, 366-398

Lu, Y. Luo, X., Polgar, M & Cao, Y (2010). Social Network Analysis of a Criminal Hacker Community, *Journal of Computer Information Systems*, 51:2, 31-41

Manky, D. (2013). Cybercrime as a service: a very modern business, *Computer Fraud & Security*, Volume 2013, 6, 9-16

McAlaney, J., Kimpton, E. & Thackeray, H., (2019). Fifty shades of grey hat: A socio-psychological analysis of conversations on hacking forums, *CyPsy24: Annual CyberPsychology, CyberTherapy & Social Networking Conference,* 24-26 June 2019, Norfolk, VA, USA.

McCulloch, L. & Furlong, S. (2019). *DM for details: Selling Drugs in the Age of Social Media*, Volteface

McGuire, M. R. & Dowling, S. (2013). *Cybercrime - A Review of the Evidence*, HOS/11/047, Home Office

McGuire, M. R. (2007). *Hypercrime: the new geometry of harm*, London Routledge

McGuire, M. R. (2018a). Cons, Constructions and Misconceptions of Computer Related Crime: From a Digital Syntax to a Social Semantics. *Journal of Qualitative Criminal Justice & Criminology*, 6,2

McGuire, M. R. (2018b). *Into the Web of Profit: - Analysing the cybercrime economy* – Bromium: industry report

McGuire, M. R. (2019a). It ain't what they do, it's the way that they do it. Why we still don't understand Cybercrime' (in Leukfeldt, R. & Holt, T. *The Human factor in Cybercrime*, Routledge

McGuire, M. R.(2019b). *Social Media platforms and the Cybercrime Economy*, Bromium: industry report

McGuire, M. R., (2019c). *Behind the Darknet Black Mirror*, Bromium: industry report

McGuire, M. R., (2021). *Nation States, Cyberconflict and the Web of Profit*, Hewlett Packard: industry report

McGuire M. R. (forthcoming) *Platform Criminality and Post Crime*, London Routledge

Mershon, C and Shvetsova, O. (2019). *Formal Modelling in Social Science*. Ann Arbor MI: Michigan University Press

Mikhaylov, A. and Frank, R., (2016). Cards, money and two hacking forums: An analysis of online money laundering schemes. In *2016 European intelligence and security informatics conference (EISIC)* (pp. 80-83). IEEE.

Moon, B., McCluskey, J.D. and. McCluskey, C.P (2010). A general theory of crime and computer crime: An empirical test, *Journal of Criminal Justice*, 38 (4) pp.

767-772

Moore, M. H. (1970). *The Economics of heroin distribution.* Croton-on-Hudson, NY: Hudson Institute.

Moore, T. and Clayton, R., (2007). Examining the impact of website take-down on phishing. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*,pp. 1-13.

Moyle, L., Childs, A., Coomber, R., & Barratt, M. J. (2019). # Drugsforsale: An exploration of the use of social media and encrypted messaging apps to supply and access drugs. *International Journal of Drug Policy*, 63, 101-110

NCSC (2017). Cybercrime: understanding the online business model, *National cybersecurity centre*. June

Nodeland, B. (2020). The effects of self-control on the cybercrime victim-offender overlap. *International Journal of Cybersecurity Intelligence and Cybercrime*, 3(2), 4-2

O'Hara, A.C., Ko, R.K.L., & Mazerolle, L. (2020). Crime script analysis for adult image-based sexual abuse: a study of crime intervention points for retribution-style offenders. *Crime Science* 9**,** 26

Onuchowska, A. and Berndt., J. (2019). Using Agent-Based Modelling to Address Malicious Behavior on Social Media, *ICIS 2019 Proceedings*. 24

Orsagh, T. (1983). Is there a place for economics in Criminology and criminal justice? *Journal of Criminal Justice*, 11. pp. 391-401

Pastrana S., Hutchings A., Caines A., Buttery P. (2018). Characterizing Eve: Analysing Cybercrime Actors in a Large Underground Forum. In: Bailey M., Holz T., Stamatogiannakis M., Ioannidis S. (eds) *Research in Attacks, Intrusions, and Defenses*. RAID 2018. Lecture Notes in Computer Science, vol 11050. Springer, Cham.

Payne, B. (2018). White-Collar Cybercrime: White-Collar Crime, Cybercrime, or Both? *Criminology, Criminal Justice, Law & Society*, 19 (3), p.17

Payne, B.K., Hawkins, B. & Xin, C. (2019). Using Labeling Theory as a Guide to Examine the Patterns, Characteristics, and Sanctions Given to Cybercrimes. *Am J Crim Just* **44,** 230–247

Perkins, R., Jordan Howell, C. Dodge, C., Burruss, G. &Maimon, D.(2020). Malicious Spam Distribution: A Routine Activities Approach. *Deviant Behavior* 0:0, pages 1-17.

Parise, J. (2019). Heads Up: Cybercriminals Are Businesspeople, *CFO* 2/8/2019

Porcedda, M. and Wall, D. (2021). "Modelling the Cybercrime Cascade Effect in Data Crime," in *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Vienna, Austria, 2021 pp. 161-177.

Putnam, H. (1973). Meaning and Reference. *The Journal of Philosophy*, *70*(19), 699–711.

Rajivan P, Janssen MA, Cooke NJ. (2013). Agent-Based Model of a Cyber Security Defense Analyst Team. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 57(1):314-318.

Reyns, B.W., (2010). A situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers. *Crime Prevention and Community Safety*, *12*(2), pp.99-118.

Reyns, B. W., Henson, B., Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle-routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, 38, 1149-1169.

Reyns, B. (2017). Routine Activity Theory and Cybercrime in Steinmetz, K. & Nobles, M. (eds) *Technocrime and Criminological Theory* London: Routledge

Roth, R. and Berlinger, J. (2021). North Korean hackers stole more than $300 million to pay for nuclear weapons, says confidential UN report , *CNN*, 09/02/2021

Rottenberg, S. (1968). The clandestine distribution of heroin, its discovery and suppression. *J. of Poli. Econ*. 76: 78-90.

Rubin, P. H. (1973). The economic theory of the criminal firm, in Rottenberg, S. (ed) The *Economics of Crime and Punishment***,** Washington, DC: American Enterprise Institute for Public Policy Research.

Salmon, Wesley C.. "The Sufficiency/Necessity View". *Scientific Explanation and the Causal Structure of the World*, Princeton: Princeton University Press, (2020), pp. 185-190.

Sarkar, S., Almukaynizi, M., Shakarian, J., & Shakarian, P. (2019). Predicting enterprise cyber incidents using social network analysis on dark web hacker forums. *The Cyber Defense Review*, 87–102.

Schank R, Abelson R. (1977). *Scripts, Plans, Goals, and Understanding*. Hilladale NJ: Lawrence Erlbaum Associates

Schelling, T. (1967). Economics and criminal enterprise. *The Pub. interest* 7: 61-78**.**

Sela-Shayovitz R. (2012). Gangs and the Web: Gang Members' Online Behavior. *Journal of Contemporary Criminal Justice*.;28(4):389-405.

Skinner, W. & Fream, A. (1997). A Social Learning Theory Analysis of Computer Crime among College Students. *Journal of Research in Crime and Delinquency*. 34(4):495-518.

Sloman, S., Barbey, A. & Hotaling, J. (2009). A Causal Model Theory of the Meaning of Cause, Enable, and Prevent. *Cognitive science*. 33. 21-50.

Somer, T, Tiido, A, Sample, C, Mitchener-Nissen, T (2018). Application of journey mapping and crime scripting to the phenomenon of trolling. In: *ICCWS 2018 13th International Conference on Cyber Warfare and Security*. Academic Conferences and Publishing Limited, 465.

Stockman, M., (2014). Insider hacking: applying situational crime prevention to a new white-collar crime. In *Proceedings of the 3rd annual conference on Research in*

information technology,pp. 53-56.
Steinmetz, K.F. (2015). Craft(y)ness: An ethnographic study of hacking. *British Journal of Criminology*, 55, 125–145.
Sutton, M. (1998). Handling Stolen Goods and Theft: A Market Reduction Approach. Home Office Research Study 178. Home Office. London.
Sutton, M., Schneider, J.L. and Hetherington, S. (2001). Tackling theft with the market reduction approach. *Home Office Crime Reduction Research Series* Paper 8.
Suler, J. (2004). The Online Disinhibition Effect, *Cyberpsychology & Behavior* 7(3):321-6
Thompson B, Morris-King J. (2018). An agent-based modeling framework for cybersecurity in mobile tactical networks. *The Journal of Defense Modeling and Simulation*. 2018;15(2):205-218.
Turgeman-Goldschmidt, O. (2008). Meanings that Hackers Assign to their Being a Hacker, International *Journal of Cyber Criminology*,2 (2): 382–396
UNODC (2011). Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes, *United Nations Office on Drugs and Crime*, October
Van der Bruggen M, Blokland A. (2021). A Crime Script Analysis of Child Sexual Exploitation Material Fora on the Darkweb. *Sexual Abuse*. 33(8):950-974.
Van der Wagen, W. & Pieters, W. (2015). From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks, *The British Journal of Criminology*, 55, 3, 578–595,
Van de Weijer, S.G. and Leukfeldt, E.R., (2017). Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking*, *20*(7), pp.407-412.
Wall, D. (2007). *Cybercrime – The Transformation of Crime in the Information Age,* London :Polity
Wall, D. (2014). 'High risk' cyber-crime is really a mixed bag of threats, *The Conversation*, 14/11/2014
Williams, M., Levi, M., Burnap P. & Gundur, R.V. (2019). Under the Corporate Radar: Examining Insider Business Cybercrime Victimization through an Application of Routine Activities Theory, *Deviant Behaviour* 40:9, 1119-1131,
Willison, R. and Siponen, M., (2009). Overcoming the insider: reducing employee computer crime through Situational Crime Prevention. *Communications of the ACM*, *52*(9), pp.133-137.
Wortley, R. (1997). "Reconsidering the Role of Opportunity in Situational Crime Prevention." In: G. Newman, R.V. Clarke and S.G. Shohan (eds.), Rational Choice and Situational Crime Prevention. Aldershot, UK:Ashgate Publishing.

Wortley, R. (2010). Critiques of situational crime prevention. In B. Fisher & S. Lab (eds) Encyclopedia of Victimology and Crime Prevention. Thousand Oaks, CA: Sage.

Yar, M. (2005). The novelty of “cybercrime”: An assessment in light of routine activity theory. European Journal of Criminology, 2, 407–427.

Yip, Michael (2011). An investigation into Chinese cybercrime and the applicability of social network analysis. *ACM WebSci '11, , Koblenz, Germany. 13 - 16 Jun 2011.*