European Journal of Criminology

http://euc.sagepub.com

The Novelty of ‘Cybercrime’: An Assessment in Light of Routine Activity Theory

Majid Yar

European Journal of Criminology 2005; 2; 407
DOI: 10.1177/147737080556056

Volume 2 (4): 407–427: 1477-3708
DOI: 101177/147737080556056
Copyright © 2005 European Society of
Criminology and SAGE Publications
London, Thousand Oaks CA, and New Delhi
www.sagepublications.com

European
Journal of
Criminology

The Novelty of 'Cybercrime'

An Assessment in Light of Routine Activity Theory

Majid Yar
University of Kent, UK

ABSTRACT

Recent discussions of 'cybercrime' focus upon the apparent novelty or otherwise of the phenomenon. Some authors claim that such crime is not qualitatively different from 'terrestrial crime', and can be analysed and explained using established theories of crime causation. One such approach, oft cited, is the 'routine activity theory' developed by Marcus Felson and others. This article explores the extent to which the theory's concepts and aetiological schema can be transposed to crimes committed in a 'virtual' environment. Substantively, the examination concludes that, although some of the theory's core concepts can indeed be applied to cybercrime, there remain important differences between 'virtual' and 'terrestrial' worlds that limit the theory's usefulness. These differences, it is claimed, give qualified support to the suggestion that 'cybercrime' does indeed represent the emergence of a new and distinctive form of crime.

KEY WORDS

Cyberspace / Ecology / Internet / Virtual Crimes.

Introduction

It has become more or less obligatory to begin any discussion of 'cybercrime' by referring to the most dramatic criminological quandary it raises, namely, does it denote the emergence of a 'new' form of crime and/or criminality? Would such novelty require us to dispense with (or at least modify, supplement or extend) the existing array of theories and explanatory concepts that criminologists have at their disposal? Unsurprisingly, answers to such questions appear in positive, negative and indeterminate registers. Some commentators have suggested that the advent of 'virtual crimes' marks the establishment of a new and distinctive social environment (often dubbed 'cyberspace', in contrast to 'real space') with its own ontological and epistemological structures, interactional forms, roles and rules, limits and possibilities. In this alternate social space, new and distinctive forms of criminal endeavour emerge, necessitating the development of a correspondingly innovative criminological vocabulary (see, for example, Capeller 2001 and Snyder 2001). Sceptics, in contrast, see 'cybercrime' at best as a case of familiar criminal activities pursued with some new tools and techniques – in Peter Grabosky's metaphor, largely a case of 'old wine in new bottles' (Grabosky 2001). If this were the case, then 'cybercrime' could still be fruitfully explained, analysed and understood in terms of established criminological classifications and aetiological schema. Grabosky (2001: 248) nominates in particular Cohen and Felson's 'routine activity theory' (RAT) as one such criminological approach, thereby seeking to demonstrate 'that "virtual criminality" is basically the same as the terrestrial crime with which we are familiar' (2001: 243; also Grabosky and Smith 2001). Others, such as Pease (2001: 23), have also remarked in passing upon the helpfulness of the RAT approach in discerning what might be different about 'cybercrime', and how any such differences (perhaps ones of degree, rather than kind) present new challenges for governance, crime control and crime prevention. Indeed, crime prevention strategies derived in part from RAT, such as situational crime prevention, have been proposed as viable responses to Internet crime (Newman and Clarke 2002, 2003). Nevertheless there has yet to appear any sustained *theoretical* reflection on whether, and to what extent, RAT might serve to illuminate 'cybercrimes' in their continuity or discontinuity with those 'terrestrial crimes' that occur in what Pease (2001: 23) memorably dubs 'meatspace'. The present article aims to do just that, in the hope of shedding some further light on whether or not some of our received, 'terrestrially grounded' criminology can in fact give us adequate service in coming to grips with an array of ostensibly 'new' crimes.

The article is structured as follows. I begin by briefly addressing some of the definitional and classificatory issues raised by attempts to delimit cybercrime as a distinctive form of criminal endeavour. I then explicate the formulation of routine activity theory that is utilized in the article, and offer some general reflections on some of the pressing issues typically raised vis-à-vis the theory's explanatory ambit (in particular its relation to dispositional or motivational criminologies, and the vexed problem of the 'rationality' or otherwise of offenders' choices to engage in law-breaking behaviour). In the third section, I examine cybercrime in relation to the general ecological presuppositions of RAT, focusing specifically on whether or not the theory's explanatory dependence on *spatial and temporal* *convergence* is transposable to crimes commissioned in online or 'virtual' environments. After considering in a more detailed manner the viability of Felson et al.'s conceptualization of 'target suitability' in relation to the presence of persons and property in virtual environments, I engage in a similar examination of issues related to 'capable guardianship'. In conclusion, I offer some comments on the extent to which cybercrimes might be deemed continuous with 'terrestrial crimes'. Substantively, I suggest that, although the core concepts of RAT are in significant degree transposable (or at least adaptable) to crimes in virtual environments, there remain some qualitative differences between virtual and terrestrial worlds that make a simple, wholesale application of its analytical framework problematic.

Cybercrime: Definitions and classifications

A primary problem for the analysis of cybercrime is the absence of a consistent current definition, even amongst those law enforcement agencies charged with tackling it (NHTCU/NOP 2002: 3). As Wall (2001: 2) notes, the term 'has no specific referent in law', yet it has come to enjoy considerable currency in political, criminal justice, media, public and academic discourse. Consequently, the term might best be seen to signify a *range* of illicit activities whose common denominator is the central role played by networks of information and communication technology (ICT) in their commission. A working definition along these lines is offered by Thomas and Loader (2000: 3), who conceptualize cybercrime as those 'computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks'. The specificity of cybercrime is therefore held to reside in the newly instituted interactional environment in which it takes place, namely the 'virtual space' (often dubbed 'cyberspace') generated by the interconnection of computers into a worldwide network of information exchange, primarily the Internet (Castells 2002: 177).

Within the above definition it is possible to further classify cybercrime along a number of different lines. One commonplace approach is to distinguish between 'computer-assisted crimes' (those crimes that pre-date the Internet but take on a new life in cyberspace, e.g. fraud, theft, money laundering, sexual harassment, hate speech, pornography) and 'computer-focused crimes' (those crimes that have emerged in tandem with the establishment of the Internet and could not exist apart from it, e.g. hacking, viral attacks, website defacement) (Furnell 2002: 22). On this classification, the primary dimension along which cybercrime can be subdivided is the manner in which the technology plays a role, i.e. whether it is a contingent ('computer-assisted') or necessary ('computer-focused') element in the commission of the offence.

Although the above distinction may be socio-technically helpful, it has a limited criminological utility. Hence, one alternative is to mobilize existing categories derived from criminal law into which their cyber-counterparts can be transposed. Thus Wall (2001: 3–7) subdivides cybercrime into four established legal categories:

1. Cyber-*trespass* – crossing boundaries into other people's property and/or causing damage, e.g. hacking, defacement, viruses.
2. Cyber-*deceptions* and *thefts* – stealing (money, property), e.g. credit card fraud, intellectual property violations (a.k.a. 'piracy').
3. Cyber-*pornography* – activities that breach laws on obscenity and decency.
4. Cyber-*violence* – doing psychological harm to, or inciting physical harm against others, thereby breaching laws pertaining to the protection of the person, e.g. hate speech, stalking.

This classification is certainly helpful in relating cybercrime to existing conceptions of proscribed and harmful acts, but it does little in the way of isolating what might be qualitatively *different* or *new* about such offences and their commission when considered from a perspective that looks beyond a limited legalistic framework. Consequently, most criminological commentators (especially those of a sociological bent) focus their search for novelty upon the socio-structural features of the environment ('cyberspace') in which such crimes occur. It is widely held that this environment has a profound impact upon the structural properties and limits that govern interactions (both licit and illicit), thereby transforming the potential scope and scale of offending, inexorably altering the relationships between offenders and victims and the potential for criminal justice systems to offer satisfactory solutions or resolutions (Capeller 2001). Particular attention is given to the ways in which the establishment of cyberspace variously 'transcends', 'explodes', 'compresses' or 'collapses' the constraints of space and time that limit interactions in the 'real world'. Borrowing from sociological accounts of globalization as 'time–space compression' (Harvey 1989), theorists of the new informational networks suggest that cyberspace makes possible near-instantaneous encounters and interactions between spatially distant actors, creating possibilities for ever-new forms of association and exchange (Shields 1996). Criminologically, this seemingly renders us vulnerable to an array of potentially predatory others who have us within instantaneous reach, unconstrained by the normal barriers of physical distance.

Moreover, the ability of the potential offender to target individuals and property is seemingly amplified by the inherent features of the new communication medium itself – computer-mediated communication

(CMC) enables a single individual to reach, interact with and affect thousands of individuals simultaneously. Thus the technology acts as a 'force multiplier', enabling individuals with minimal resources (so-called 'empowered small agents') to generate potentially huge negative effects (mass distribution of email 'scams' and distribution of viral codes being two examples). Further, great emphasis is placed upon the ways in which the Internet enables the manipulation and reinvention of social identity – cyberspace interactions afford individuals the capacity to reinvent themselves, adopting new virtual personae potentially far-removed from their 'real world' identities (Poster 1995; Turkle 1995). From a criminological perspective, this is viewed as a powerful tool for the unscrupulous to perpetrate offences while maintaining anonymity through disguise (Snyder 2001: 252; Joseph 2003: 116–18) and a formidable challenge to those seeking to track down offenders.

From the above, we can surmise that it is the supposedly novel socio-interactional features of the cyberspace environment (primarily the collapse of spatial–temporal barriers, many-to-many connectivity, and the anonymity and plasticity of online identity) that make possible new forms and patterns of illicit activity. It is in this alleged discontinuity from the socio-interactional organization of 'terrestrial crimes' that the criminological challenge of cybercrime is held to reside. I will now turn to consider whether and to what extent the routine activity approach, as a purported general theory of crime causation (Felson 2000), can embrace such novelties within its conceptual apparatus and explanatory ambit.

Delimiting the routine activity approach: Situational explanation, rationality and the motivated actor

Birkbeck and LaFree (1993: 113–14) suggest that the criminological specificity of routine activity theory (RAT) can be located via Sutherland's (1947) distinction between 'dispositional' and 'situational' explanations of crime and deviance. Dispositional theories aim to answer the question of 'criminality', seeking some causal mechanism (variously social, economic, cultural, psychological or biological) that might account for why *some* individuals or groups come to possess an inclination toward law- and rule-breaking behaviour. Dispositional theories comprise the standard reference points of criminological discourse – Lombroso, Durkheim, Merton, the Chicago School, Bonger, Chambliss, and so on being 'textbook' examples.

In contrast, situational theories (including various 'opportunity' and 'social control' approaches) eschew dispositional explanations, largely on the grounds of their apparent explanatory failures – they appear recurrently unsuccessful in adequately accounting for trends and patterns of offending in terms of their nominated causes (Cohen and Felson 1979: 592, 604). Routine activity theorists 'take criminal inclination as given' (Cohen and Felson 1979: 589), supposing that there is no shortage of motivations available to all social actors for committing law-breaking acts. They do not deny that motivations can be incited by social, economic and other structural factors, but they insist that any such incitements do not furnish a *sufficient* condition for actually following through inclinations into law-breaking activity (Cohen and Felson 1979: 589, 604–5; Birkbeck and LaFree 1993: 114). Rather, the *social situations* in which actors find themselves crucially mediate decisions about whether or not they will act on their inclinations (whatever their origins). Consequently, routine activity theorists choose to 'examine the manner in which the spatio-temporal organization of social activities helps people translate their criminal inclinations into action' (Cohen and Felson 1979: 592). Social situations in which offending becomes a viable option are created by the routine activities of other social actors; in other words, the routine organizational features of everyday life create the conditions in which persons and property become available as targets for successful predation at the hands of those so motivated. For routine activity theorists, the changing organization of social activities is best placed to account for patterns, distributions, levels and trends in criminal activity. If this is the case, then the emergence of cybercrime invites us to enquire into the routine organization of *online* activities, with the aim of discerning whether and how this 'helps people translate their criminal inclinations into action'. More broadly, it invites us to enquire whether or not the analytical schema developed by RAT – in which are postulated key variables that make up the criminogenic social situation; what Felson (1998) calls 'the chemistry for crime' – can be successfully transposed to cyber-spatial contexts, given the apparent discontinuities of such spaces vis-à-vis 'real world' settings.

Before such questions can be addressed, however, a number of extant issues relating to RAT must be tackled. The first relates to the specific formulation of the theory that is to be mobilized for present purposes. As with many other theoretical approaches RAT does not comprise a single, self-subsistent set of explanatory concepts. Rather, it can take a number of different forms, utilizing a variable conceptual apparatus and levels of analysis, depending upon the specific orientations of the criminologists who develop and mobilize it (Bennett 1991: 148). Moreover, the work of a single contributor does not remain static over time, but typically undergoes revision and development. Thus, for example, Felson has elaborated and refined his original 'chemistry for crime' over a 25-year period by introducing additional mediating variables into what is an ever-more complex framework. Here I discuss RAT in something like its 'original' formulation. This statement of the theory hypothesizes that 'criminal acts require the convergence in space and time of *likely offenders*, *suitable targets* and the *absence of capable guardians*' (Cohen and Felson 1979: 588, emphasis in the original). This definition has the virtue of including the 'central core of three concepts' (Bennett 1991: 148) which appear as constant features of all routine activity models.

A second issue relates to the theory's controversial attachment to presuppositions about the 'rational' character of actors' choices to engage in (or desist from) illegal activity. Routine activity approaches are generally held to be consistent with the view that actors are free to choose their courses of action, and do so on the basis of anticipatory calculation of the utility or rewards they can expect to flow from the chosen course. Felson, for example, has made explicit this presupposition (Felson 1998: 23–4; Felson 1986: 119–20), and his work has been marked by a clear convergence with 'rational choice theory' (Clarke and Felson 1993). One common objection raised in light of this commitment is the theory's potential inability to encompass crimes emanating from non-instrumental motives. Thus, for example, Miethe et al. (1987) and Bennett (1991) conclude that, although routine activity theory exhibits considerable explanatory power in relation to property offences (those oriented to material and economic gain), it is considerably weaker in respect of 'expressive' crimes, such as interpersonal violence. Similar objections can be raised from outside routine activity analysis, for example by proponents of 'cultural criminology' who highlight the neglect of emotional and affective 'seductions' that individuals experience when engaged in criminal and deviant activity (Katz 1988). I would suggest, however, that the basic difficulty here arises not so much from the attribution to actors of 'rationality' per se, but from taking such rationality to be necessarily of a limited, economic kind (Hollis 1987). It may be a mistake to view affective dispositions as inherently devoid of rationality; rather, as Archer (2000) argues, emotions can better be seen as responses to, and commentaries upon, situations that we encounter as part of our practical engagements with real-world situations. Particular emotional dispositions (such as fear, anger, boredom, excitement) are not simply random but 'reasonable' responses to the situations in which we as actors find ourselves. My point here is that, by adopting a more capacious conception of rationality (which includes aesthetic and affective dimensions), the apparent dualism between 'instrumental' and 'expressive' motivations can be significantly overcome. For the remainder of this piece I shall follow routine activity theorists in taking motivations 'as given', without, however, conceding that such motivations must necessarily be reducible to instrumental calculations of economic or material utility.

Convergence in space and time: The ecology and topology of cyberspace

At heart, routine activity theory is an *ecological* approach to crime causation, and as such the spatial (and temporal) localization of persons, objects and activities is a core presupposition of its explanatory schema. The ability of its aetiological formula (offender + target − guardian = crime) to explain and/or anticipate patterns of offending depends upon these elements converging in space and time. Routine activities, which create variable opportunity structures for successful predation, always occur in particular locations at particular times, and the spatio-temporal accessibility of targets for potential offenders is crucial in determining the possibility and likelihood of an offence being committed. As Felson (1998: 147) puts it: 'The organization of time and space is central. It . . . helps explain how crime occurs and what to do about it.' Thus, for example, Cohen and Felson (1979) suggest that the postwar increases in property crime rates in the United States are explicable in terms of changing routine activities such as growing female labour force participation, which takes people increasingly out of the home for regularized periods of the day, thereby increasing 'the probability that motivated offenders will converge in space and time with suitable targets in the absence of capable guardians' (1979: 593). Similarly, they argue that 'proximity to high concentrations of potential offenders' is critical in determining the likelihood of becoming a target for predation (1979: 596; see also Lynch 1987, Cohen et al. 1981 and Miethe and Meier 1990 on the positive correlation between proximity and predation). Thus, at a general level, the theory requires that targets, offenders and guardians be located in particular places, that measurable relations of spatial proximity and distance pertain between those targets and potential offenders, and that social activities be temporally ordered according to rhythms such that each of these agents is either typically present or absent at particular times. Consequently, the transposability of RAT to virtual environments requires that cyberspace exhibit a *spatio-temporal ontology* congruent with that of the 'physical world', i.e. that place, proximity, distance and temporal order be identifiable features of cyberspace. I will reflect on the spatial and temporal ontology of cyberspace in turn.

Spatiality

Discourses of cyberspace and online activity are replete with references to space and place. There are purported to exist 'portals', 'sites' complete with 'back doors', 'chat rooms', 'lobbies', 'classrooms', 'cafes', all linked together via 'superhighways', with 'mail' carrying communications between one location and another (Adams 1998: 88–9). Such talk suggests that cyberspace possesses a recognizable geography more-or-less continuous with the familiar spatial organization of the physical world to which we are accustomed. However, it has been suggested that such ways of talking are little more than handy metaphors that provide a convenient way for us to conceptualize an environment that in reality is inherently discontinuous with the non-virtual world of physical objects, locations and coordinates (Dodge and Kitchin 2001: 63). Numerous theorists and analysts of cyberspace suggest instead that received notions of place location and spatial separation are obsolete in an environment that is 'anti-spatial' (Mitchell 1995: 8). The virtual environment is seen as one in which there is 'zero distance' between its points (Stalder 1998), such that entities and events cannot be meaningfully located in terms of spatial contiguity, proximity and separation. Everyone, everywhere and everything are always and eternally 'just a click way'. Consequently, geographical rules that act as a 'friction' or barrier to social action and interaction are broken (Dodge and Kitchin 2001: 62). If this is true, then the viability of RAT as an aetiological model for virtual crimes begins to look decidedly shaky, given the model's aforementioned dependence on spatial convergence and separation, proximity and distance, to explain the probability of offending. To take one case in point, if all places, people and objects are at 'zero distance' from all others, then how is it possible meaningfully to operationalize a criterion such as 'proximity to a pool of motivated offenders'? Despite these apparent difficulties, I would suggest that all is not lost – that we can in fact identify spatial properties in virtual environments *that at least in part* converge with those of the familiar physical environment.

Positions that claim there is no recognizable spatial topology in cyberspace may be seen to draw upon an absolute and untenable separation of virtual and non-virtual environments – they see these as two ontologically distinct orders or experiential universes. However, there are good reasons to believe that such a separation is overdrawn, and that the relationships between these domains are characterized by both similarity and dissimilarity, convergence and divergence. I shall elaborate two distinctive ways in which cyberspace may be seen to retain a spatial geometry that remains connected to that of the 'real world'.

First, cyberspace may be best conceived not so much as a 'virtual reality', but rather as a 'real virtuality', a socio-technically generated interactional environment rooted in the 'real world' of political, economic, social and cultural relations (Castells 2002: 203). Cyberspace stands with one foot firmly planted in the 'real world', and as a consequence carries non-virtual spatialities over into its organization. This connection between virtual and non-virtual spatialities is apparent along a number of dimensions. For instance, the virtual environments (websites, chat rooms, portals, mail systems, etc.) that comprise the virtual environment are themselves physically rooted and produced in 'real space'. The distribution of capacity to generate such environments follows the geography of existing economic relations and hierarchies. Thus, for example, 50 percent of Internet domains originate in the United States, which also accounts for 83 percent of the total web pages viewed by Internet users (Castells 2002: 214, 219). Moreover, access to the virtual environment follows existing lines of social inclusion and exclusion, with Internet use being closely correlated to existing cleavages of income, education, gender, ethnicity, age and disability (Castells 2002: 247–56). Consequently, presence and absence in the virtual world translate 'real world' marginalities, which themselves are profoundly spatialized ('first world' and 'third world', 'urban' and 'rural', 'middle-class suburb' and 'urban ghetto', 'gated community' and 'high-rise estate'). In short, the online density of both potential offenders and potential targets is not neutral with respect to existing social ecologies, but translates them via the differential distribution of the resources and skills needed to be present and active in cyberspace.

A second way in which cyberspace may exhibit a spatial topology refers to the purely internal organization of the information networks that it comprises. It was noted above that many commentators see the Internet and related technologically generated environments as heralding 'the death of distance' and the collapse of spatial orderings, such that all points are equally accessible from any starting point (Dodge and Kitchin 2001: 63). However, reflection on network organization reveals that *not* all 'places' are equidistant – proximity and distance have meaning when negotiating cyberspace. This will be familiar to all students and scholars who attempt to locate information, organizations and individuals via the Internet. Just because one knows, suspects or is told that a particular entity has a virtual presence on the Net, finding that entity may require widely varying expenditures of time and effort. Those domains (e.g. websites) with a higher density of connections to other domains (e.g. via 'hyperlinks') are more easily arrived at than those with relatively few. The algorithms that organize search engines prioritize sites having the highest number of links to others, thereby rendering them more proximate to the online actor. Arriving at a particular location may require one to traverse a large number of intermediate sites, thereby rendering that location relatively distant from one's point of departure; conversely, the destination may be 'only a click away'. Thus the distribution of entities in terms of the axis 'proximity–distance', and the possibility of both convergence and divergence of such entities, can be seen to have at least some purchase in cyberspace.

Despite these continuities, it should also become clear that there exist qualitative differences between the spatial organization of non-virtual and virtual worlds. Most significantly, they exhibit significantly different degrees of stability and instability in their geometries. Non-virtual spatialities are relatively stable and perdurable. Granted, they can undergo significant shifts over time: patterns of land use can and do change (as, for example, when the former industrial cores of cities are redeveloped for residential use – Zukin 1988); the sociodemographic configuration of locales is also subject to change (as with processes of 'gentrification' and 'ghettoization' – Davis 1990); the proximity of places is elastic in light of developing transport infrastructures; and so on. However, given that non-virtual spatial orderings are materialized in durable physical artefacts (buildings, roads, bridges, walls), and their social occupation and uses are patterned and institutionalized, change in their organization is likely to be incremental rather than wholesale. It is this very stability in socio-spatial orderings that permits ecological perspectives such as RAT to correlate factors such as residential propinquity with predation rates and patterns. In contrast, virtual spatialities are characterized by extreme volatility and plasticity in their configurations. It was noted above that virtual proximity and distance may be seen as the product of variable network geometries and connection densities. Yet these connections are volatile and easily transmuted – little resistance is offered by virtual architectures and topologies. Thus the distance or separation between two sites or locales can shift instantly by virtue of the simple addition of a hyperlink that provides a direct and instant path from one to the other. Similarly, virtual places and entities appear and disappear in the cyber environment with startling regularity – the average lifespan for a web page is just a couple of months (Johnston 2003); actors instantaneously appear and disappear from the environment as they log in or out of the network. Consequently, the socio-spatial organization of the virtual world is built on 'shifting sands'. This quality presents considerable difficulty for the application of routine activity analysis to cyberspace, given its presuppositions that (a) places have a relatively fixed presence and location, and (b) the presence of actors in locations is amenable to anticipation in light of regularized patterns of activity.

Temporality

The ability to locate actors and entities in particular spaces/places *at particular times* is a basic presupposition of RAT. The explanatory power of the theory depends upon routine activities exhibiting a clear temporal sequence and order (a *rhythm*, or 'regular periodicity with which events occur', and a *timing*, in which different activities are coordinated 'such as the coordination of an offender's rhythms with those of a victim' – Cohen and Felson 1979: 590). It is this temporal ordering of activities that enables potential offenders to anticipate when and where a target may be converged upon; without such anticipation, the preconditions for the commission of an offence cannot be fulfilled, nor can criminogenic situations be identified by the analyst (Felson 1998: 147–8).

The temporal structures of cyberspace, I would argue, are largely devoid of the clear temporal ordering of real-world routine activities. Cyberspace, as a *global* interactional environment, is populated by actors living in different real-world time zones, and so is populated '24/7'. Moreover, online activities span workplace and home, labour and leisure, and cannot be confined to particular, clearly delimited temporal windows (although there may be peaks and troughs in gross levels of network activity, as relatively more people in the most heavily connected time zones make use of the Internet – Dodge and Kitchin 2001: 105). Consequently, there are no *particular* points in time at which actors can be anticipated to be *generally* present or absent from the environment. From an RAT perspective, this means that rhythm and timing as structuring properties of routine activities become problematic – for offenders, for potential targets and for guardians. Given the 'disordered' nature of virtual spatio-temporalities, identifying patterns of convergence between the criminogenic elements becomes especially difficult.

Thus far, I have largely focused on the question of cyber-spatial convergence between the entities identified as necessary for the commission of an offence. Now I turn to consider the properties of those entities themselves, in order to reflect upon the relative continuity or discontinuity between their virtual and non-virtual forms. As already mentioned, the first of these elements, the 'motivated offender', is assumed rather than analysed by RAT. Therefore I shall not consider the offender further, but take the existence of motivated offenders in cyberspace as given. Instead I shall follow RAT in focusing upon the other two elements of the criminogenic formula, namely 'suitable targets' and 'capable guardians'.

Targets in cyberspace: VIVA la différence?

For routine activity theory, the suitability of a target (human or otherwise) for predation can be estimated according to its four-fold constituent properties – value, inertia, visibility and accessibility, usually rendered in the acronym VIVA. Below I shall reflect on cyber-spatial targets in terms of these four dimensions.

Value

The valuation of targets is a complicated matter, even when comparing ‘like with like’, e.g. property theft. This complexity is a function of the various purposes the offender may have in mind for the target once appropriated – whether it is for personal pleasure, for sale, for use in the commission of a further offence or other non-criminal activity, and so on. Equally, the target will vary according to the shifting valuations attached socially and economically to particular goods at particular times – factors such as scarcity and fashion will play a role in setting the value placed upon the target by offenders and others (Felson 1998: 55). Most cybercrime targets are *informational* in nature, given that all entities that exist and move in cyberspace are forms of digital code. Prime targets of this kind include the various forms of ‘intellectual property’, such as music, motion pictures, images, computer software, trade and state secrets, and so on. In general terms it may well be that, in the context of an ‘information economy’ (Webster 2002: 12–14), increasing value is attached to such informational goods, thereby making them increasingly valued as potential targets. The picture becomes more complex when the range of targets is extended – property may be targeted not for theft but for trespass or criminal damage (a cybercriminal case in point being ‘hacking’, where computer systems are invaded and websites are ‘defaced’, or ‘malware’ distribution, where computer systems are damaged by ‘viruses’, ‘Trojan horses’ and ‘worms’ – Clough and Mungo 1992: 85–105); the target may be an individual who is ‘stalked’ and ‘abused’; or members of a group may be subjected to similar victimization because of their social, ethnic, religious, sexual or other characteristics; the target may be an illicit product that is traded for pleasure or profit (such as child pornography). Broadly speaking, we can conclude that the targets of cybercrime, like those of terrestrial crime, vary widely and attract different valuations, and that such valuations are likely to impact on the suitability of the target when viewed from the standpoint of a potential offender (on the need to incorporate subjective definitions of situation and value, see Birkbeck and LaFree 1993: 119–23; and Bernburg and Thorlindsson 2001: 544–5).

Inertia

This term refers to the physical properties of objects or persons that might offer varying degrees of resistance to effective predation: a large and heavy object is relatively difficult to remove, and a large and heavy person is relatively difficult to assault (M. Felson 1998: 57; R. Felson 1996). Therefore, there is (at least for terrestrial crimes against property and persons) an inverse relationship between inertia and suitability, such that the greater the inertial resistance the lower the suitability of the target, and vice versa. The operability of the inertial criteria in cyberspace, however, appears more problematic, since the targets of cybercrime do not possess physical properties of volume and mass – digitized information is 'weightless' and people do not carry their physical properties into the virtual environment. This apparent 'weightlessness' (Leadbetter 2000) seemingly deprives property in cyberspace of any inherent resistance to its removal. Information can be downloaded nearly instantaneously; indeed, it can be infinitely replicated thereby multiplying the offence many-fold (the obvious example here being media 'piracy' – Grabosky and Smith 2001: 30–1). However, further reflection shows that even informational goods retain inertial properties to some degree. First, the volume of data (e.g. file size) impacts upon the portability of the target – something that will be familiar to anyone who has experienced the frustration of downloading large documents using a telephone dial-up connection. Secondly, the technological specification of the tools (the computer system) used by the 'information thief' will place limits upon the appropriation of large informational targets; successful theft will require, for example, that the computer used has sufficient storage capacity (e.g. hard drive space or other medium) to which the target can be copied. Thus, although informational targets offer *relatively* little inertial resistance, their 'weightlessness' is not absolute.

Visibility

RAT postulates a positive correlation between target visibility and suitability: 'the potential offender must know of the existence of the target' (Bennett 1991: 148). Property and persons that are more visible are more likely to become targets. Conceptualizing visibility in cyberspace presents a difficult issue. Given that the social raison d'etre of technologies such as the Internet is to invite and facilitate communication and interaction, visibility is a ubiquitous feature of virtually present entities. The Internet is an inherently *public* medium (unlike other more closed ICT networks, such as 'Intranets' and 'virtual private networks' that restrict access, and hence visibility, to a selected range of actors). Moreover, since the internal topology of cyberspace is largely unlimited by barriers of *physical* distance, this renders virtually present entities *globally* visible, hence advertising their existence to the largest possible 'pool of motivated offenders'.

Accessibility

This term denotes the 'ability of an offender to get to the target and then get away from the scene of a crime' (Felson 1998: 58). Again, the greater the target's accessibility, the greater its suitability, and vice versa. Thus Beavon et al. (1994) identify the number of physical routes through which a target is accessible as a significant variable in the distribution of property crimes – a house situated in a cul-de-sac is less accessible than one situated on a street that intersects with a number of other thoroughfares. However, given that traversal of cyberspace is 'non-linear', and it is possible to jump from any one point to any other point within the space, it is difficult to conceive targets as differentiated according to the likelihood of accessibility to a potential offender in this manner. Similarly, the availability of egress from the 'scene of the crime' is difficult to operationalize as a discriminating variable when applied to cyberspace. The ability to 'get away' in cyberspace can entail simply severing one's network connection, thereby disappearing from the virtual environment altogether (Newman and Clarke 2003: 17, 63). It is, of course, possible that an offender may be noticed during the commission of the offence (e.g. by an 'Intrusion Detection System') and subsequently 'trailed' back to his/her 'home' location via electronic tracing techniques. However, such tracing measures can be circumvented with a number of readily available tools, such as 'anonymous re-mailers', encryption devices, and the use of third-party servers and systems from which to launch the commission of an offence (Grabosky and Smith 2001: 35; Furnell 2002: 101, 110); this brings us back to the problem of *anonymity*, noted earlier. The one dimension in which accessibility between non-virtual and virtual targets might most closely converge is that of security devices that prevent unauthorized access. Cohen and Felson (1979: 591) note the significance of 'attached or locked features of property inhibiting its illegal removal'. The cyber-spatial equivalents of such features include passwords and other authentication measures that restrict access to sites where vulnerable targets are stored (e.g. directories containing proprietary information). Such safeguards can, of course, be circumvented with tools such as 'password sniffers', 'crackers' and decryption tools (Furnell 2002: 26–8), but these can be conceived as the virtual counterparts of lock-picks, glass-cutters and crowbars.

In sum, it can be seen from the above that the component sub-variables comprising target suitability exhibit varying degrees of transposability to virtual settings. The greatest convergence appears in respect of target value, perhaps unsurprisingly because valuations do not emanate from the (real or virtual) ecological environment, but are brought into that environment from elsewhere – namely, the spheres of economic and symbolic relations. However, the remaining three sub-variables exhibit considerable divergence between real and virtual settings. In the case of inertia, the difference arises from the distinctive *ontological properties* of entities that exist in the two domains – they are physical in the case of the 'real world' and non-physical (informational) in the case of the virtual. In respect of the other two sub-variables (visibility and accessibility), divergences between the real and the virtual arise from the structural features of the environments themselves; as previously discussed, features such as distance, location and movement differ markedly between the two domains, and these configurations will affect the nature of visibility and accessibility within the respective environments.

Are there 'capable guardians' in cyberspace?

'Capable guardianship' furnishes the third key aetiological variable for crime causation postulated by routine activity theory. Guardianship refers to 'the capability of persons and objects to prevent crime from occurring' (Tseloni et al. 2004: 74). Guardians effect such prevention 'either by their physical presence alone or by some form of direct action' (Cohen et al. 1980: 97). Although direct intervention may well occur, routine activity theorists see the simple presence of a guardian in proximity to the potential target as a crucial deterrent. Where the guardian is a person, she/he acts as someone 'whose mere presence serves as a gentle reminder that someone is looking' (Felson 1998: 53; see also Jacobs 1961). Such guardians may be 'formal' (e.g. the police), but RAT generally places greater emphasis on the significance of 'informal' agents such as homeowners, neighbours, pedestrians and other 'ordinary citizens' going about their routine activities (Cohen and Felson 1979: 590; Felson 1998: 53). In addition to such 'social guardians', the theory also views *physical* security measures as effecting guardianship – instances include barriers, locks, alarms, and lighting on the street and within the home (Tseloni et al. 2004: 74). Taken together, the absence or presence of guardians at the point at which potential offenders and suitable targets converge in time and space is seen as critical in determining the likelihood of an offence taking place (although the importance of guardianship has been questioned by some researchers – see Miethe and Meier 1990; Massey et al. 1989).

How, then, does the concept of guardianship transpose itself into the virtual environment? The efficacy of the concept as a discriminating variable between criminogenic and non-criminogenic situations rests upon the guardian’s co-presence with the potential target at the time when the motivated offender converges upon it. In terms of formal social guardianship, maintaining such co-presence is well nigh impossible, given the ease of offender mobility and the temporal irregularity of cyber-spatial activities (it would require a ubiquitous, round-the-clock police presence on the Internet). However, in this respect at least, the challenge to formal guardianship presented by cyberspace is only a more intensified version of the policing problem in the terrestrial world; as Felson (1998: 53) notes, the police ‘are very unlikely to be on the spot when a crime occurs’. In cyberspace, as in the terrestrial world, it is often only when private and informal attempts at effective guardianship fail that the assistance of formal agencies is sought (Grabosky and Smith 2001: 36–7). The cyber-spatial world, like the terrestrial, is characterized by a range of such private and informal social guardians: these range from in-house network administrators and systems security staff who watch over their electronic charges, through trade organizations oriented to self-regulation, to ‘ordinary online citizens’ who exercise a range of informal social controls over each other’s behaviour (such as the practice of ‘flaming’ those who breach social norms on offensive behaviour in chat rooms – Smith et al. 1997). In addition to such social guardians, cyberspace is replete with ‘physical’ or technological guardians, automated agents that exercise perpetual vigilance. These range from ‘firewalls’, intrusion detection systems and virus scanning software (Denning 1999: 353–69), to state e-communication monitoring projects such as the US government’s ‘Carnivore’ and ‘ECHELON’ systems (Furnell 2002: 262–4). In sum, it would appear that RAT’s concept of capable guardianship is transposable to cyberspace, even if the structural properties of the environment (such as its variable spatial and temporal topology) amplify the limitations upon establishing guardianship already apparent in the terrestrial world.

Conclusion

The impetus for this article was provided by the dispute over whether or not cybercrime ought to be considered as a new and distinctive form of criminal activity, one demanding the development of a new criminological vocabulary and conceptual apparatus. I chose to pursue this question by examining if and to what extent existing aetiologies of crime could be transposed to virtual settings. I have focused on the routine activity approach because this perspective has been repeatedly nominated as a theory capable of adaptation to cyberspace; if such adaptability (of the theory's core concepts and analytic framework) could be established, this would support the claim of *continuity* between terrestrial and virtual crimes, thereby refuting the 'novelty' thesis. If not, this would suggest *discontinuity* between crimes in virtual and non-virtual settings, thereby giving weight to claims that cybercrime is something criminologically new. I conclude that there are both significant continuities and discontinuities in the configuration of terrestrial and virtual crimes.

With respect to the 'central core of three concepts', I have suggested that 'motivated offenders' can be treated as largely homologous between terrestrial and virtual settings. The construction of 'suitable targets' is more complex, with similarities in respect of value but significant differences in respect of inertia, visibility and accessibility. The concept of 'capable guardianship' appears to find its fit in cyberspace, albeit in a manner that exacerbates the possibilities of instituting such guardianship effectively. However, these differences can be viewed as ones of *degree* rather than *kind*, requiring that the concepts be adapted rather than rejected wholesale.

A more fundamental difference appears when we try to bring these concepts together in an aetiological schema. The central difficulty arises, I have suggested, from the distinctive *spatio-temporal ontologies* of virtual and non-virtual environments: whereas people, objects and activities can be clearly located within relatively fixed and ordered spatio-temporal configurations in the 'real world', such orderings appear to destabilize in the virtual world. In other words, the routine activity theory holds that the 'organization of time and space is central' for criminological explanation (Felson 1998: 148), yet the cyber-spatial environment is chronically spatio-temporally *disorganized*. The inability to transpose RAT's postulation of 'convergence in space and time' into cyberspace thereby renders problematic its straightforward explanatory application to the genesis of cybercrimes. Perhaps cybercrime represents a case not so much of 'old wine in new bottles' as of 'old wine in *no* bottles' or, alternatively, 'old wine' in bottles of varying and fluid shape. Routine activity theory (and, indeed, other ecologically oriented theories of crime causation) thus appears of limited utility in an environment that defies many of our taken-for-granted assumptions about how the socio-interactional setting of routine activities is configured.

Acknowledgement

My thanks to David B. Smith for reading and commenting on an earlier version of this article. The usual caveat stands, and any errors and omissions are my sole responsibility.

References

Adams, P. (1998). Network topologies and virtual place. *Annals of the Association of American Geographers 88*, 88–106.

Archer, M. (2000). *Being human: The problem of agency.* Cambridge: Cambridge University Press.

Beavon, D., Brantingham, P. L. and Brantingham, P. J. (1994). The influence of street networks on the patterning of property offenses. In R. V. Clarke (ed.) *Crime prevention studies, Vol II*, 149–63. New York: Willow Tree Press.

Bennett, R. (1991). Routine activities: A cross-national assessment of a criminological perspective. *Social Forces 70*, 147–63.

Bernburg, J. G. and Thorlindsson, T. (2001). Routine activities in social context: A closer look at the role of opportunity in deviant behavior. *Justice Quarterly 18*, 543–67.

Birkbeck, C. and LaFree, G. (1993). The situational analysis of crime and deviance. *Annual Review of Sociology 19*, 113–37.

Capeller, W. (2001). Not such a neat net: Some comments on virtual criminality. *Social & Legal Studies 10*, 229–42.

Castells, M. (2002). *The internet galaxy: Reflections on the internet, business, and society.* Oxford: Oxford University Press.

Clarke, R. and Felson, M., eds (1993). *Routine activity and rational choice*. London: Transaction Press.

Clough, B. and Mungo, P. (1992). *Approaching zero: Data crime and the computer underworld*. London: Faber & Faber.

Cohen, L. and Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review 44*, 588–608.

Cohen, L., Felson, M. and Land, K. (1980). Property crime rates in the United States: A macrodynamic analysis, 1947–1977; with ex ante forecasts for the mid-1980s. *American Journal of Sociology 86*, 90–118.

Cohen, L., Kluegel, J. and Land, K. (1981). Social inequality and predatory criminal victimization: An exposition and a test of a formal theory. *American Sociological Review 46*, 505–24.

Davis, M. (1990). *City of quartz: Excavating the future of Los Angeles*. London: Verso.

Denning, D. (1999). *Information warfare and security.* New York: Addison Wesley.

Dodge, M. and Kitchin, R. (2001). *Mapping cyberspace*. London: Routledge.

Felson, M. (1986). Routine activities, social controls, rational decisions and criminal outcomes. In D. Cornish and R. Clarke (eds) *The reasoning criminal*. New York: Springer Verlag.

Felson, M. (1998). *Crime and everyday life*, 2nd edn. Thousand Oaks, CA: Pine Forge Press.

Felson, M. (2000). The routine activity approach as a general social theory. In S. Simpson (ed.) *Of crime and criminality: The use of theory in everyday life*. Thousand Oaks, CA: Sage.

Felson, R. (1996). Big people hit little people: Sex differences in physical power and interpersonal violence. *Criminology 34*, 433–52.

Furnell, S. (2002). *Cybercrime: Vandalizing the information society.* London: Addison Wesley.

Grabosky, P. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies 10*, 243–9.

Grabosky, P. and Smith, R. (2001). Telecommunication fraud in the digital age: The convergence of technologies. In D. Wall (ed.) *Crime and the internet*. London: Routledge.

Harvey, D. (1989). *The condition of postmodernity.* Oxford: Blackwell.

Hollis, M. (1987). *The cunning of reason*. Cambridge: Cambridge University Press.

Jacobs, J. (1961). *The life and death of great American cities*. New York: Random House.

Johnston, N. (2003). Plan approved to save U.S. digital history. *Washington Post*, 15 February.

Joseph, J. (2003). Cyberstalking: An international perspective. In Y. Jewkes (ed.) *Dot.cons: Crime, deviance and identity on the internet*. Cullompton: Willan Press.

Katz, J. (1988). *The seductions of crime*. New York: Basic Books.

Leadbetter, C. (2000). *The weightless society.* New York: W. W. Norton.

Lynch, J. (1987). Routine activity and victimization at work. *Journal of Quantitative Criminology 3*, 275–82.

Massey, J., Krohn, M. and Bonati, L. (1989). Property crime and the routine activities of individuals. *Journal of Research in Crime and Delinquency 26*, 378–400.

Miethe, T. and Meier, R. (1990). Opportunity, choice and criminal victimization: A test of a theoretical model. *Journal of Research in Crime and Delinquency 27*, 243–66.

Miethe, T., Stafford, M. and Long, J. S. (1987). Social differentiation in criminal victimization: A test of routine activities/lifestyle theories. *American Sociological Review 52*, 184–94.

Mitchell, W. J. (1995). *City of bits: Space, place and the Infobahn*. Cambridge, MA: MIT Press.

Newman, G. and Clarke, R. (2002). *Etailing: New opportunities for crime, new opportunities for prevention*. Produced for the Foresight Crime Prevention Panel by the Jill Dando Institute of Crime Science, UCL; URL (consulted 13 May 2005): http://www.foresight.gov.uk/Previous_Rounds/Foresight_1999__2002/Crime_Prevention/Reports/Etailing_New_Opportunities_for_Crime_New_Opportunities_for_Prevention.html.

Newman, G. and Clarke, R. (2003). *Superhighway robbery: Preventing e-commerce crime*. Cullompton: Willan Press.

NHTCU/NOP (2002) Hi-tech crime: The impact on UK business. London: NHTCU.

Pease, K. (2001). Crime futures and foresight: Challenging criminal behaviour in the information age. In D. Wall (ed.) *Crime and the internet*. London: Routledge.

Poster, M. (1995). *The second media age*. Oxford: Polity.

Shields, R., ed. (1996). *Cultures of the internet: Virtual spaces, real histories, living bodies*. London: Sage.

Smith, C., McLaughlin, M. and Osborne, K. (1997). Conduct control on Usenet. *Journal of Computer-Mediated Communication 2*; URL (consulted 13 May 2005): http://www.ascusc.org/jcmc/vol2/issue4/smith.html.

Snyder, F. (2001). Sites of criminality and sites of governance. *Social & Legal Studies 10*, 251–6.

Stalder, F. (1998). The logic of networks: Social landscapes *vis-a-vis* the space of flows'. *Ctheory 46*; URL (consulted 13 May 2005): http://www.ctheory.net/text_file.asp?pick = 263.

Sutherland, E. (1947). *Principles of criminology.* Philadelphia: Lippincott.

Thomas, D. and Loader, B. (2000). Introduction – Cybercrime: Law enforcement, security and surveillance in the information age. In D. Thomas and B. Loader (eds) *Cybercrime: Law enforcement, security and surveillance in the information age*. London: Routledge.

Tseloni, A., Wittebrood, K., Farrell, G. and Pease, K. (2004). Burglary victimization in England and Wales, the Unites States and The Netherlands: A cross-national comparative test of routine activities and lifestyle theories. *British Journal of Criminology 44*, 66–91.

Turkle, S. (1995). *Life on the screen: Identity in the age of the internet*. New York: Simon & Schuster.

Wall, D. (2001). Cybercrimes and the internet. In D. Wall (ed.) *Crime and the internet*. London: Routledge.

Webster, F. (2002). *Theories of the information society*, 2nd edn. London: Routledge.

Zukin, S. (1988). *Loft living: Culture and capital in urban change*. London: Radius.

Majid Yar

Majid Yar is lecturer in criminology at the School of Social Policy, Sociology and Social Research (SPSSR), Cornwallis Building, University of Kent at Canterbury, Canterbury, Kent, CT2 7NF, UK. His research interests include criminological and social theory, crime and the Internet, intellectual property crimes, and crime and media. He is the author of numerous articles, which have appeared in journals such as the *British Journal of Criminology, Theoretical Criminology, Theory, Culture & Society, Economy & Society, Surveillance & Society* and *History of the Human Sciences*. He is currently working on a book entitled *Cybercrime and society*, to be published by Sage in 2006.
m.yar@kent.ac.uk