CHAPTER 6

The Novelty of “Cybercrime”

An Assessment in Light of Routine Activity Theory

Majid Yar
University of Kent, UK

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 endeavor emerge, necessitating the development of a correspondingly innovative criminological vocabulary. . . . Skeptics, in contrast, see cybercrime, at best, as a case of familiar criminal activities pursued with some new tools and techniques. . . . If this were the case, then cybercrime could still be fruitfully explained, analyzed, and understood in terms of established criminological classifications and etiological schema. Grabosky . . . 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.” . . . [T]here 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 . . . memorably dubs “meatspace.” The present chapter aims to do just that in the hope of shedding some further light on whether 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.

This chapter 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 endeavor. I then explicate the formulation of routine activity theory that is utilized in the chapter, and I 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 behavior). In the third section, I examine cybercrime in relation to the general ecological presuppositions of RAT, focusing specifically on whether the theory’s explanatory dependence on *spatial* and *temporal convergence* is transposable to crimes commissioned in online or virtual environments. . . . In conclusion, I offer some comments

Source: “The novelty of ‘cybercrime’: An assessment in light of routine activity theory,” by Yar, M. in *European Journal of Criminology,* 2, p. 407–427 (2005). Reprinted by permission of Sage Publications, Ltd.

on the extent to which cybercrimes might be deemed continuous with terrestrial crimes. Substantively, I suggest that, although the core concepts of RAT are, to a 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 among those law enforcement agencies charged with tackling it. . . . [T]he 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 . . . , 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. . . .

Within the prior 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 predate the Internet, but take on a new life in cyberspace; e.g. fraud, theft, money laundering, sexual harassment, hate speech, and 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, and website defacement). . . . 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 offense).

Although this distinction may be sociotechnically 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 . . . 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. . . . [T]heorists 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. . . . 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—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 e-mail scams and distribution of viral codes being two examples). Further, great emphasis is placed on 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. . . . From a criminological perspective, this is viewed as a powerful tool for the unscrupulous to perpetrate offences while maintaining anonymity through disguise . . . and a formidable challenge to those seeking to track down offenders.

From the previous discussion, we can surmise that it is the supposedly novel sociointeractional 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 sociointeractional organization of terrestrial crimes that the criminological challenge of cybercrime is held to reside. . . .

Delimiting the Routine Activity Approach: Situational Explanation, Rationality, and the Motivated Actor

Birkbeck and LaFree . . . suggest that the criminological specificity of RAT can be located via Sutherland's . . . 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 behavior. . . .

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. . . . Routine activity theorists "take criminal inclination as given" . . . , 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. . . . Rather, the *social situations* in which actors find themselves crucially mediate decisions about whether they will act on their inclinations (whatever their origins). Consequently, routine activity theorists choose to "examine the manner in which the spatiotemporal organization of social activities helps people translate their criminal inclinations into action." . . . 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. . . . If this is the case, then the emergence of cybercrime invites us to inquire 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 inquire as to whether the analytical schema developed by RAT—in which are postulated key variables that make up the criminogenic social situation (what Felson . . . calls "the chemistry for crime")—can be successfully transposed to cyberspatial contexts, given the apparent discontinuities of such spaces vis-à-vis real-world settings.

. . . 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 on the specific orientations of the criminologists who develop and mobilize it. . . . 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*." . . . This definition has the virtue of including the "central core of three concepts," . . . 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. . . . 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. . . . and Bennett . . . 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. . . . 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. . . . It may be a mistake to view affective dispositions as inherently devoid of rationality; rather, as Archer . . . 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. . . . For the remainder of this chapter, I 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 etiological 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 spatiotemporal accessibility of targets for potential offenders is crucial in determining the possibility and likelihood of an offence being committed. As Felson . . . puts it: "The organization of time and space is central. It . . . helps explain how crime occurs and what to do about it." . . . 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 *spatiotemporal ontology* congruent with that of the physical world (i.e., that place, proximity, distance, and temporal order be identifiable features of cyberspace). I 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, and cafes, all linked together via superhighways, with mail carrying communications between one location and another. . . . 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 nonvirtual world of physical objects, locations and coordinates. . . . The virtual environment is seen as one in which there is zero distance between its points . . . , 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. . . . If this is true, then the viability of RAT as an etiological 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. . . .

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 nonvirtual 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 similarity and dissimilarity, convergence and divergence. I 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 sociotechnically generated interactional environment rooted in the real world of political, economic, social, and cultural relations. . . . Cyberspace stands with one foot firmly planted in the real world and, as a consequence, carries nonvirtual spatialities over into its organization. This connection between virtual and nonvirtual spatialities is apparent along a number of dimensions. For instance, the virtual environments (websites, chatrooms, portals, mail systems, etc.) that comprise the virtual environment are 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% of Internet domains originate in the United States, which also accounts for 83% of the total web pages viewed by Internet users. . . . 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. . . . Consequently, presence and absence in the virtual world translate real-world marginalities, which 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. . . . 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. . . . 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 nonvirtual and virtual worlds. Most significantly, they exhibit significantly different degrees of stability and instability in their geometries. Nonvirtual spatialities are relatively stable and perdurable. Granted, they can undergo significant shifts over time: patterns of land use can and do change . . . ; the sociodemographic configuration of locales is also subject to change . . . ; the proximity of places is elastic in light of developing transport infrastructures; and so on. However, given that nonvirtual spatial orderings are materialized in durable physical artefacts (buildings, roads, bridges, and 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 sociospatial 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 . . . ; actors instantaneously appear and disappear from the environment as they log in or out of the network. Consequently, the sociospatial 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 on 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". . .). It is this temporal ordering of activities that enables potential offenders to anticipate when and where a target may be converged upon. . . .

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, labor 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 . . .). 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 spatiotemporalities, identifying patterns of convergence between the criminogenic elements becomes especially difficult.

Thus far, I have largely focused on the question of cyberspatial 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 nonvirtual forms. As already mentioned, the first of these elements, the motivated offender, is assumed rather than analyzed by RAT. Therefore, I do not consider the offender further, but take the existence of motivated offenders in cyberspace as a given. Instead, I follow RAT in focusing on 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. . . .

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 noncriminal 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. . . . 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 . . . , 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 . . .); 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. . . .

Inertia

The term *inertia* 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. . . . 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. . . . This apparent weightlessness . . . 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 . . .). 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 on 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." . . . 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. . . . Moreover, because 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

The term *accessibility* denotes the "ability of an offender to get to the target and then get away from the scene of a crime." . . . Again, the greater the target's accessibility, the greater its suitability, and vice versa. Thus, Beavon et al. . . . identify the number of physical routes through which a target is accessible as a significant variable in the distribution of property crimes. . . . However, given that traversal of cyberspace is nonlinear, 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. . . . 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 or her home location via electronic-tracing techniques. However, such tracing measures can be circumvented with a number of readily available tools, such as anonymous remailers, encryption devices, and the use of third-party servers and systems from which to launch the commission of an offense . . . ; this brings us back to the problem of *anonymity*, noted earlier. The one dimension in which accessibility between nonvirtual and virtual targets might most closely converge is that of security devices that prevent unauthorized access. Cohen and Felson . . . note the significance of "attached or locked features of property inhibiting its illegal removal." The cyberspatial 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 . . . , but these can be conceived as the virtual counterparts of lock-picks, glass cutters, and crowbars.

In summary, it can be seen from the above that the component subvariables comprising target suitability exhibit varying degrees of transposability to virtual settings. The greatest convergence appears in respect of target value. . . . However, the remaining three subvariables 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 nonphysical (informational) in the case of the virtual. In respect of the other two subvariables (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 etiological variable for crime causation postulated by routine activity theory. Guardianship refers to "the capability of persons and objects to prevent crime from occurring." . . . Guardians effect such prevention "either by their physical presence alone or by some form of direct action." . . . 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. . . . Such guardians may be formal (e.g., the police), but RAT generally places greater emphasis on the significance of 'informal' agents such as homeowners, neighbors, pedestrians, and other ordinary citizens going about their routine activities. . . . 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. . . . 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. . . .

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 noncriminogenic situations rests on the guardian's copresence with the potential target at the time when the motivated offender converges on it. In terms of formal social guardianship, maintaining such copresence is well nigh impossible, given the ease of offender mobility and the temporal irregularity of cyberspatial 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 . . . 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. . . . The cyberspatial 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 behavior (such as the practice of flaming those who breach social norms on offensive behavior in chatrooms . . .). 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 . . . , to state e-communication monitoring projects such as the U.S. government's Carnivore and ECHELON systems. . . . In summary, 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 chapter was provided by the dispute over whether cybercrime should 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 etiologies 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 nonvirtual 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 etiological schema. The central difficulty arises, I have suggested, from the distinctive *spatiotemporal ontologies* of virtual and nonvirtual environments: Whereas people, objects, and activities can be clearly located within relatively fixed and ordered spatiotemporal 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 . . . , yet the cyberspatial environment is chronically spatiotemporally *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. . . . 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 sociointeractional setting of routine activities is configured.

Questions

1. Discuss the various ways in which cybercrime is defined.
2. Explain what Yar means by the acronym *VIVA*.