Environmental Criminology and cybercrime: shifting focus from the wine to the bottles

Fernando Miró-Llinares [a] and Asier Moneva [a]*

[a] *CRIMINA Research Center for the Study and Prevention of Crime, Miguel Hernandez University, Elche, Spain*

* Corresponding author: amoneva@crimina.es [1]

[1] Current email address (14 July 2022): <amoneva@nscr.nl>

Environmental Criminology and cybercrime: shifting focus from the wine to the bottles

This chapter addresses the ability of the criminological approaches that comprise Environmental Criminology to constitute an adequate theoretical framework to analyze and understand the situational aspects of crimes committed through cyberspace and to define the most appropriate prevention strategies. The chapter begins by examining how these approaches have been applied. Subsequently, the reasons why the environmental approach can offer much more in this area if some apparent obstacles are overcome are presented. Finally, a method of applying these mid-range theoretical frameworks to different cybercrimes is proposed. Relying on multiple empirical studies, it is stated that the essential premise of the environmental approach is also observed in cybercrime: the existence of situational patterns. These patterns are derived from the different ways in which offenders and targets, in the absence of guardians, converge in cyber places: digital interaction environments that shape the situational opportunities in which people interact. The chapter ends by summarizing the application possibilities of approaches such as The Crime Pattern Theory, and Situational Crime Prevention in connection with The Routine Activity Theory and The Rational Choice Theory. It is proposed that many of the geographical applications derived from these approaches and some of their basic theoretical premises need to be adapted, while seeking to enhance their strengths and mitigate the effects of their weaknesses.

Keywords: Environmental Criminology, Crime Science, criminological theory, prevention, opportunity, geographical gap, cyber place, crime event, crime patterns.

1. New bottles for old approaches. An introduction.

Environmental Theories (also known as Theories of Crime, Opportunity Theories, or Crime Science), which include Routine Activity Theory (RAT; Cohen and Felson 1979; see Chap. 23, Routine Activities), Rational Choice Theory (RCT; see Chap. 24, Rational Choice/deterrence) with its preventive corollary Situational Crime Prevention (SCP; Cornish and Clarke 1986) and Crime Pattern Theory (CPT; Brantingham and Brantingham 1981), are mid-range explanatory approaches to the relationship between the environment and criminal behavior. In comparison to the Theories of Criminality, Theories of Crime share an interest in crime as an event and divert attention from the offender to other elements such as the potential victim and the geographical location in which the crime may occur. This is carried out with the eminently practical intention of achieving implementable prevention strategies. From this approach come both their weaknesses as explanatory frameworks, due to their neglect of the offender and various essential aspects regarding their actions (Cullen and Kulig 2018), as well as their strengths, which are the precision of their analysis and their applicability to crime prevention (Wortley and Townsley 2016).

Environmental approaches have been present almost since the birth of academic interest in cybercrime. Some of the theoretical environmental frameworks began to be used for cybercrime analysis since Grabosky (2001), in the now classic "Virtual Criminality: Old Wine in New Bottles", warned that cyberspace might not change criminal motivations, but significantly affect the opportunities and capacity of the guardians. Special attention was paid to RAT, which has been applied analytically to cybercrime with various aims, such as: to rethink the challenges faced by Criminology concerning future crimes (Pease 2001); to analyze whether its concepts should be adapted to the emergence of cyberspace (Yar 2005; Leukfeldt and Yar 2016); to identify the temporal patterns that describe large-scale cyber-attacks (Maimon et al. 2013); or to estimate crime trends related to the appearance of new opportunities (Caneppele and Aebi 2017). But above all, RAT served as a conceptual framework for studying a wide variety of criminal behaviors, ranging from economic cybercrimes such as malware (Holt and Bossler 2013), identity theft (Reyns and Henson 2016), or phishing (Leukfeldt 2014), to social cybercrimes such as online harassment (Miró-Llinares 2015), cyberbullying (Navarro and Jasinski 2013), or sexting (Wolfe et al. 2016). The SCP approach was also used for the elaboration of preventive strategies for economic crime carried out via the Internet (Newman and Clarke 2003) and cyberstalking (Reyns 2010), as well as for the examination of DDoS operators (Hutchings and Clayton 2016), the reduction of information security vulnerabilities (Hinduja and Kooi 2013), or the analysis of online stolen data markets using crime scripts (Hutchings and Holt 2014).

It is obvious, however, that the application of the Environmental Theories to crime committed through the Internet is still incipient and, therefore, insufficient. On the one hand, when the RAT and RCT approaches have been employed to analyze cybercrime, they have been applied as if they were separate explanatory theories, when it is known that the explanatory and applicative potential of Environmental Criminology comes from the enormous synergies between all three approaches (Clarke 2010). On the other hand, CPT, despite being a successful approach used in practice especially for urban crime, has barely been used for the analysis of cybercrime (Miró-Llinares and Johnson 2018). Instead, it has been relegated to the position of a conceptual framework within the so-called Computational Criminology (Brantingham 2011), a branch focused more on addressing purely methodological aspects of data science than on analyzing the context that facilitates cybercrime (e.g. Birks et al. 2012).

Finally, the main applications of Environmental Criminology continue to focus on space in the traditional geographical sense, oblivious to digital spaces. And it is logical that this should be the case. Since the birth of the Criminology of Place (Sherman et al. 1989), the geography of crime has been studied extensively and its applications have been many for crime prevention in the physical space, including: hot spots policing (Weisburd and Green 1995), SCP (Clarke 1992), geographic profiling (Rossmo 1999), or Crime Prevention Through Environmental Design (CPTED; Cozens et al. 2005). From a theoretical perspective, cyberspace seems relegated from the potential application of these measures specifically thought for geographical spaces. This could be called the "geographical gap": the apparent difficulty to apply the techniques of crime and place to cybercrime analysis in a non-geographical area. But the fact that specific practices are not suitable to cyberspace does not mean that the whole approach cannot be applied and generate new applications to this environment.

As we will try to show, the environmental approach has much to offer when applied to the study of cybercrime. However, first must be understood: (1) that for these approaches the key organizing principle of crime is not the geographic location but the crime event itself (Clarke 2018); and, (2) that its ecological premises apparently presupposed the concurrence of people and things in geographical places, but they originated from a spatial-temporal convergence between people, and people and things which, thanks to the Internet, can also happen in cyberspace, although differently from how this occurs in physical space (Miró-Llinares and Johnson 2018). In fact, several authors have built interesting approaches to the concept of cyberspace as a comparable space of convergence, albeit with modifications with respect to the convergence in physical space (Miró-Llinares 2011; Yar 2005). There has been a recent proposal to conceive this intercommunication space as a cyber place that can assimilate the main statements is RAT and the convergence between people, and people and things (Miró-Llinares and Johnson 2018). This would enable the application of a large part of the premises of CPT and Criminology of Place to the crimes perpetrated in cyberspace.

This is the direction that this chapter also follows, as it seeks to analyze the extent to which the application of the Environmental Criminology approach to crime committed in cyberspace is feasible and how the theory should be adapted for that purpose. This analysis is founded on the belief that a better understanding of the applicability of Environmental Theories to cybercrime would be especially useful in an area that is particularly in need of preventive approaches effectively implemented. However, it also adopts a realistic vision regarding the possibilities of these strategies, based on both the review of the strengths and weaknesses of the approach itself, and on the acceptance that many of its practical contributions are thought for and from the geographical world and will not allow their functional adaptation for crime perpetrated on cyberspace. We believe, however, that there are many other contributions that can be adapted to cyberspace, as well as the essential premise that the social situations in which people find themselves do decisively influence (1) their decisions regarding offending, and (2) them being the target of a crime. In addition, the practical consequences derived from this adaptation fit perfectly with the need for prevention strategies focused on the environment and the target of cybercrime due to the characteristics of cyberspace.

2. Places in cyberspace and cybercrime patterns: overcoming the geographical gap

It seems counterintuitive to consider the application of some of the essential developments of Environmental Criminology, such as hot spots or the crime mapping technique, to the field of cybercrime. It seems less so if such tools are limited to a macro or meso level analysis. Perhaps for this reason when such terms are used in relation to crimes committed through the Internet, it is common to think of analysis such as "which countries carry out (or receive) more cyber-attacks" and in geographical analysis of their regional distribution (Maimon et al. 2015), or “what are the correlates of a specific cyber-threat for a given area” and how they concentrate at the polygon level (Khey and Sainato 2013). This is because we continue to use the concept of place in its purely geographical sense, and we identify the place of cybercrime as that from which the attack is perpetrated or that which is affected by it. And the interest in these analysis can be very profound as the academy has shown, since there is also an irregular geographical distribution of different cybercrimes at the macro level according to the uneven distribution between different countries of factors such as the implementation of the Internet, the number of computer systems to which the population has access and the value of the information they contain, among others. In this sense, although research in this area is still very limited, macro analyses based on RAT have shown that wealthiest countries with a higher proportion of Internet users report greater activity from incidents such as spam or phishing (Kigerl 2012). Similar studies also show that less developed countries report higher piracy rates than more developed countries, despite registering fewer incidents (Kigerl 2013). But, does the geographical place where a cyber-attack is conducted or received perform the role that Environmental Criminology attributed to the concept of place within crime that allows many crime patterns? To affirm this to be true would be as careless as reducing crime pattern analysis to the first studies that compared the geographic distribution of crimes at the macro level from aggregate data (e.g. Guerry 1833; Quetelet 1842). If one carries out an in-depth analysis of the meaning given to place by Environmental Theories and, particularly, by CPT, the answer is clearly negative, at least in the sense of "not completely or not on its own."

CPT is an essential contribution within Environmental Criminology as it constitutes the greatest effort to integrate the Geometry of Crime and the other approaches that constitute the environmental perspective. With this theory Branthingham and Branthingham (1981) elaborate a spatial model for crime explanation that takes into consideration many previous contributions from the ecology of crime as well as the sociological theories that different criminologists have provided regarding the social, urban and, therefore, geographical distribution of crime (e.g. Harries 1976; Shaw and McKay 1942). However, it also incorporates the idea of opportunity as a fundamental explanatory framework, stating that the spatial distribution of crime is also influenced by the distribution of opportunities, by the urban structure, and by the mobility of people. Obviously, it is easy to identify geometry with geography when all the rules, both macro and micro, expounded and later developed by the authors regarding the relationship between crime and place were applied to crimes perpetrated in what was the only existing space of personal intercommunication or, at least, the main one: the physical space. But geography and geometry are not the same. And the truth is that CPT is not only an exclusively geographical theory, but that its ultimate meaning is only distinguished at present, as we shall see, if the idea of place as a geographical environment is surpassed and the notion of convergence space is assumed.

The theoretical construction of the explanatory relationship between the crime and the place where it occurs is part of the idea that the people motivated to commit a crime, for different reasons explained by multiple etiologies, perpetrate the act in a certain place, in a specific moment, and on a particular victim, with a somewhat developed process of decision-making in which the environment plays a fundamental role (Brantingham and Brantingham 1981). The environment emits signals, or clues, about its characteristics and about the distribution of other elements (e.g. targets, guardians) that will influence the success of criminal activity from the perspective of the offender. From this premise the authors derive the importance of different elements, such as: activity spaces, which are those places in which people objectively carry out their daily lives while they travel on the routes connecting those places or activity nodes where they spend more time, and which have different characteristics according to their functionality; places that generate or attract crime (i.e. crime generators and crime attractors), which enhance criminal opportunities by concentrating a large number of people and, therefore, by increasing the number of effective convergences (e.g. a parking lot full of people where a concert is held), or by attracting criminals by harboring especially attractive criminal opportunities in terms of cost-benefit (e.g. a jewelry store that contains a large number of hot products); the journey to crime, which refers to the journey made by an offender to the place where he commits the crime and which is conditioned by the opportunities and effort he must make; or, the crime templates, which are mechanisms of automation for the offender's decision making that are relatively stable in time, that serve to select the place where the crime is committed, and that vary according to each criminal behavior. None of these suppositions is necessarily geographical, but rather spatial, since all they demand is the existence of different possibilities of convergence between people, and people and things.

What does have a geographical significance are all the applied consequences which have later been object of empirical demonstrations, such as: the relationship between the proximity of the crime scene and the offender's residence or other especially relevant activity nodes (i.e. anchor points) that are determined by the principle of distance decay (Capone and Nichols 1976); crime mapping, or use of maps for the geographic analysis of patterns that crimes describe (Harries 1999) through techniques, such as, geographic profiling, which enables the determination of the area where the residence of a serial aggressor will most likely be found (Rossmo 1999); or hot spots, which are anomalous concentrations of excessive crime in specific places and moments (Sherman et al. 1989). All these propositions are specifically geographical, because the premises are applied to this area and there have been empirically verified. But if we change the geographic scope to which they apply and we think of cyberspace as a place of convergence, it would be possible to think of different places, different spaces and nodes of activity linked by virtual routes, of cyberspaces that favor convergence between people or that attract criminals, and of digital microenvironments where cybercrime is concentrated in certain time intervals (Miró-Llinares et al. 2018).

It is true, however, that the intrinsic characteristics of cyberspace (i.e., contraction of time and space) are essentially different from those of physical space (Miró-Llinares 2011). And since these characteristics preclude thinking of a traditional form of convergence, Yar (2005) questions the applicability of RAT in cyberspace by alluding to two major reasons related to the concepts of proximity and temporality. In relation to the former, this author argues that virtual spaces are volatile as opposed to physical spaces and that there are no distances between these spaces. Regarding the latter, Yar intuits that the different way of conceiving time in cyberspace endows it with a high degree of entropy that translates into space-time disorder. Overall, this spatiotemporal divergence makes convergence difficult and suggests that the laws on which RAT is built cannot be extrapolated to cyberspace (Yar 2005). Despite the criticisms, some authors have maintained their support for the applicability of RAT to cyberspace by arguing that spatial-temporal convergence is still possible, but that it simply occurs in a different way (Miró-Llinares 2011; Reyns et al. 2011). In this regard, Reyns and colleagues (2011) explain that cyberspace is composed of a network of devices that enable virtual convergence, even if it is asynchronous. Thus, the fact that time and space are different in cyberspace does not mean that convergence is necessarily more improbable, but rather the opposite. Geographical constraints that limit actions in physical space do not exist in cyberspace, so the ability to perform certain behaviors that could have been burdened by such effort is intact. In fact, the possibilities of convergence may even expand in cyberspace due to the possibility of temporarily fixing certain actions that produce almost unlimited effects and cause potential victims to interact with them at different times than those in which the offender is actually in that space (Miró-Llinares 2011).

As has already been stated, the place of cybercrime is not only that geographical site from which an act emanates or where the attack produces its effects, but rather the digital place where, in a specific space and time, an offender and a target converge in the absence of a guardian, and that would conform "discrete nodes or areas of activity on the Internet where one is not physically located but can nevertheless act" (Miró-Llinares and Johnson 2018 p 893). It is these cyber places that enable the convergence between offenders, victims and guardians in very different ways, according to: (1) the way in which users can interact within the space, either through store-and-forward or streaming contact with perennial or expired contents; (2) the natural surveillance that the place allows according to whether it is open to the public or, on the contrary, its access is restricted, the traffic level of people and information, and the self-protection resources it offers; and (3), the type of activity (e.g. leisure, consumption, work) that users predominantly carry out in the place (Miró-Llinares and Johnson 2018).

Just as in physical space a thief must coincide in space and time with the object he wants to steal, the phishing victim must open the email that asks for his personal data. In the same way that two teenagers insult each other during break time, a user interacts by mistake with a violent message on Facebook. In addition, just as there are structural differences between the neighborhoods or streets where thefts occur, each digital space has different characteristics that allow one or another form of interaction. In this way, while forums allow communication by sending and receiving messages with a certain time-lapse, there are platforms such as Periscope that allow events to be streamed. Similarly, direct messages in Twitter guarantee the intimacy that you do not have when posting a tweet on the timeline. And these are the places where the patterns are going to be produced both at the macro and micro levels, as academic literature has shown when analyzing, even outside the theoretical framework of Environmental Criminology, the patterns of cybercrime.

Thus, and regarding the analysis of concentrations at the macro level, criminological research has shown that some Facebook accounts are used for phishing purposes (Vishwanath 2014), that certain events in the physical space generate widespread reactions of online hate speech on Twitter (Burnap and Williams 2015), that there is also considerable gang activity on both Twitter and Facebook (Décary-Hétu and Morselli 2011), that certain sexual predators can use platforms such as Myspace as hunting grounds (Guo 2008), that YouTube is used as a loudspeaker for the dissemination of violent content and jihadist propaganda (Klausen et al. 2012), that drug trafficking in crypto markets such as Silk Road yields increasing profits (Aldridge and Décary-Hétu 2014), that it is common to receive fraudulent messages through email (Cross 2015), that certain forums are used as platforms to advertise the illegal sale and purchase of personal data (Holt et al. 2016), or that cybercriminal networks use forums to establish relationships with new accomplices and facilitators (Leukfeldt et al. 2016).

Regarding the existence of patterns at the micro level, and especially from a computational perspective, studies on cybercrime show that it is possible to detect incidents of cyberbullying through the analysis of the metadata associated with Instagram publications (Hosseinmardi et al. 2015) , that it has been possible to identify spam in email by analyzing clusters of the messages' characteristics (Wei et al. 2008), that violent communication expressed on Twitter after a terrorist attack is concentrated in certain time slots (Miró-Llinares and Rodríguez-Sala 2016) and in micro-spaces with specific characteristics (Miró-Llinares et al. 2018), and, in addition, certain elements of interaction related to user accounts allow us to distinguish human users from bots in this social network (Ferrara et al. 2016), that sentiment analysis in messages can be used as a predictor of cyber-attacks (Shu et al. 2018), or that it is possible to identify potentially offensive videos on YouTube by analyzing their tags (Agarwal et al. 2017).

In addition, many of the studies conducted from the RAT perspective implicitly show potential cyber place patterns. For example, Marcum and colleagues (2010) found that prolonged exposure linked to increased use of chat rooms was a significant predictor of harassment victimization in older students. In a similar vein, Näsi and collaborators (2017) found that greater social network use was related to greater probability of suffering this type of cybervictimization, but that the natural vigilance exerted by the number of friends on

Facebook did not seem to have an influence on such dynamics. Also, Choi and Lee (2017) found a relationship between performing certain risk activities in social networks and the probabilities of being victimized, mainly related to the publication of habits, opinions and personal information. On the other hand, Reyns (2013) found that carrying out certain online activities, such as banking, shopping, messaging, and downloading, was related to a higher probability of suffering identity theft. Similarly, an integrated Self-Control-RAT study on a representative sample in the Netherlands showed that some activities such as downloading or using dating sites favor malware infection victimization (Holt et al. 2018). In line with previous studies that indicate that online shopping is linked to consumer fraud (Pratt et al. 2010; Van Wilsem 2013), Junger and colleagues (2017) found that those users who used the Internet as a platform for the sale of products were also those who were most likely to be defrauded when they were buyers.

3. Environmental Criminology as a theoretical framework for the situational analysis of cybercrime

The studies referenced above not only demonstrate the essential premise of Environmental Criminology regarding the non-random distribution of crime events (Brantingham and Brantingham 1981), but also highlight the existence of cybercrime concentrations in specific moments and digital spaces as a result of the different way criminal opportunities manifest themselves in cyber places. In other words, there seems to be enough evidence to sustain that cybercrimes do pattern according to different situational environments of communication where offenders, targets, and guardians interact. These patterns can be both macro as well as micro. This means we have overcome the main obstacle impeding the assertion that the environmental approach can constitute an adequate framework both to analyze the relationship between situational factors and cybercrime, and on which to base adequate preventive strategies. Thus, this process entails substantial adaptations derived from how the diverse communicative architecture of cyberspace function. It is time to more thoroughly develop the applicability of the environmental approach to the analysis of cybercrime. To do so, we will take as a point of reference the analysis that authors such as Cullen and Kulig (2018), and Bottoms (2012) have provided regarding its strengths and weaknesses, and to which we will add the specificities that may arise from the new situational environment to which it is applied. After all, and as these authors have rightly identified, the environmental approach has already brought important analytical and practical advances to our discipline. And although it also has limitations, these are typical of a mid-range perspective and have never been denied by its proponents. However, these but must be understood in order to define the explanatory potential of the environmental approach with respect to cybercrime.

3.1. The normality of crime, cyberspace and the new everyday life

One of the greatest achievements of Environmental Criminology has been to emphasize the normality of crime and to focus its research on the everyday aspects that surround delinquency. Cullen and Kulig (2018) refer to this feature and underline two strengths of the approach: on the one hand, it focuses on ordinary people, and on the other, it goes beyond the roots of crime. The people who commit crimes and the victims who suffer them are ordinary people who, at a given moment, find opportunities to converge in the absence of guardians. This convergence occurs regardless of the individual nature of each subject; that is, the personal criminogenic characteristics that academic literature attributes to offenders or victims have little influence on the appearance of opportunity. It does not matter if an offender has low self-control, or if a victim has a certain propensity to ingest alcohol. As long as both actors do not converge spatiotemporally, no crime will be committed.

This has not changed, but everyday life has, and this no longer happens only in physical space but also in cyberspace. Until a few decades ago, the only way for offenders and suitable targets to converge was through physical contact in the "meatspace" (Pease 2001). Nowadays, the development of IT has increased what telephony already made clear a long time ago: that it would be possible to contact others without having to physically coincide. We no longer only converge with other people and goods while we go to work or a place of leisure, or when we return from them, but when we open our email in the morning, when we download attachments at work, when we make purchases or carry out online banking transactions, or when we interact with other people by mobile phone on the different social networks and instant messaging platforms that we occupy when we are connected to the Internet (Felson 2012). Of course, this form of digital convergence is different from the physical in two senses: (1) the spatial sense, because it is unrelated to distances; and (2) in the temporary sense, because the actions we perform on the Internet can be fixed and can produce their effects at another time, resulting in an asynchronous convergence with a potential receiver (Miró-Llinares 2011).

The normality of crime highlights that the most effective short-term prevention mechanisms are those that affect the contexts of immediate convergence and take into account the way in which the different minimum elements for crime converge. In fact, in reference to the SCP, Clarke (1997) said that "the implementation must be specific in nature, and cater precisely to addressing particular types of crime" (pp. 4-5). When applying the environmental approach to cybercrime it is necessary, therefore, to pay attention to the manner of convergence that enables the occurrence of each crime type and to the routine activities carried out online and offline. In relation to cyber-dependent crimes, where convergence is digital, we must consider the routine activities of the offenders and the victims in the physical space in which they act (Maimon et al. 2013), but we must pay special attention to the digital situational environment in which convergence occurs to understand why it occurs (Miró-Llinares and Johnson 2018). For example, while it is important to have updated antivirus software on a computer, it is even more important that it is activated when browsing through download web sites where there is considerable threat of being infected by malware. On the other hand, if the crime originates from a dual convergence (i.e. combining physical and digital), as in some cyber-enabled crimes, the analysis of the environment should also cover both dimensions of everyday life. For instance, cyberbullying is often related to traditional bullying dynamics or the personal relationships of minors in school. Thus, the school environment will affect what happens later in cyberspace, but it is also necessary to pay attention to the space of digital convergence, in this case to the social networks on which minors interact and harassment occurs. The mobile phone intertwines physical space and cyberspace routine activities. And the Internet of Things will increase this interdependence.

3.2. Focusing on prevention (and going micro)

Another strength of the environmental approach is its applied and preventive nature. In fact, it is claimed that Environmental Criminology has, through a range of prevention techniques, contributed enormously to invert the Nothing Works paradigm that predominated in mainstream criminology during the 70s (Cullen and Kulig 2018; Medina-Ariza 2011).

Among the most salient examples are: the establishment of preventive strategies through the identification of situational contexts that promote or reduce the risk of victimization (Cornish and Clarke, 1986); the incorporation of deterrence and surveillance systems for the control of crime such as the installation of CCTV systems (Welsh and Farrington 2009) or hot spot policing strategies (Braga 2005); and, the design of physical elements to reduce criminal opportunities such as CPTED (Jeffery 1977) or Design Against Crime strategies (DAC; Ekblom 1997). Some of these techniques can be directly extrapolated to cybercrime prevention, as shown by the research that applies the analytical framework of RAT to cyberspace in order to identify risk factors for victimization (e.g., Holt and Bossler 2008; Miró-Llinares 2015; see also Chap. 23, Routine Activities). While those techniques focusing on intrinsically geographical aspects seem less applicable, as we have pointed out, reducing them to their situational and opportunity essence and adapting them to the new environment enables their use in a preventive sense.

This is the case with measures such as CCTV or hot spot policing which are based on the reinforcement of deterrence strategies and surveillance systems. Despite their geographical nature, the basic principles on which they are founded clearly transcend the physical and extend their relevance to the field of cybercrime prevention: their aim is to increase the costs perceived by (cyber) offenders in terms of effort and risk, while reducing potential benefits and provocations, and eliminating excuses (Cornish and Clarke 2003; Newman and Clarke 2003). Although there are already investigations that have shown, for example, the deterrent effects of warning banners with respect to unauthorized access to computer systems through honeypot structures (Maimon et al. 2014), research in this field is still incipient. In this sense, there has not been in-depth investigation on the control and dissuasion effect of administrators or moderators with regards to the management of cyber places such as forums or chats (Reyns 2010), or on the preventive impact of the regulatory functions performed by service providers. On the other hand, we know that the strategies used to manage places go beyond the inclusion of super controllers and can also include environmental design. Although both CPTED and DAC have always focused on the modification of urban spaces or corporeal objects, the truth is that digital environments are also susceptible to modification in order to condition cybercrime. For example, it is possible to limit the frequency with which a user can broadcast messages in a certain period of time, to implement CAPTCHA systems to restrict access to certain websites only to people and not bots, or to configure a website to automatically filter certain content according to its potential harmfulness.

As for hot spot intervention strategies, both cybercrime police units and service providers are already using various software to identify clustered patterns for different types of cybercrime (Wall 2007). Yet, if we also want to improve understanding of the dynamics of victimization in cyberspace, it is necessary to relate the design and application of these tools with the environmental theoretical framework by studying the situational elements of cyber places. The starting hypothesis for this reasoning is that just as there are geographical places which, due to their characteristics, become attractors or generators of crime (Brantingham and Brantingham 1995), digital spaces can also provide the same conditions depending on their configuration. On the Internet, cyber places will be crime attractors insofar as the targets they contain have been previously introduced, have considerable value, and it is possible to converge with them in the absence of guardians (Miró-Llinares 2011). Cyber places will be crime generators depending on the interaction possibilities they offer, which is defined by the level of transit of people and information at specific times. And this happens both at the macro and micro levels. In this sense, and in line with the tendency found in the Criminology of Place to analyze increasingly micro units in order to avoid measurement errors (Weisburd et al. 2009), it is necessary to analyze and decompose each problem in its environment with the same levels of specificity. This is because the same specificity that characterizes the geographical distribution of crime can be observed in the different forms of cybercrime that are similarly concentrated in specific spaces and time, creating spatial-temporal hot spots of cybercrime (Miró-Llinares and Johnson 2018).

The implementation of SCP measures, particularly those based on the identification of hot spots and the subsequent interventions, has always faced criticism regarding the displacement of crime (e.g. Gabor 1981). The main objective of this type of intervention has been to effectively reduce crime in high-crime places, causing zero or little crime displacement (Bowers and Johnson 2016). Scientific evidence has consistently shown that displacement affects only a small part of the total volume of crime and that, in any case, crime is reduced in absolute terms (Guerette and Bowers 2009). In addition, it has been observed that the preventive effects of SCP are propagated to places close to their implementation, a phenomenon known as diffusion of benefits (Clarke and Weisburd 1994). This is not to deny that crime can be displaced, but to affirm that this circumstance does not invalidate the preventive benefits that are obtained from the implementation of SCP measures. It is logical to think that cybercrime also moves, adapting to the different preventive measures that are implemented (Miró-Llinares 2012). Although, as some authors have pointed out (Hartel et al. 2010; Newman and Clarke 2003) no studies have been found that formally evaluate the effect of SCP implementation in relation to cybercrime displacement, others suggest plausible forms of displacement. For example, in the context of online black markets, Hutchings and Holt (2017) suggest that when an offender is threatened by an attempt to disrupt their communications, they can replace the use of Internet Relay Chats with forums. This circumstance constitutes a form of spatial displacement, since the offender changes their cyber place of action for another. In addition to spatial displacement, other forms can be produced: temporal, when the crime is committed at another time; tactical, when the commission method changes; target, when the objective of the crime is different; functional, when a different crime is committed; and, perpetrator displacement, when the crime is committed by another author (Barr and Pease 1990).

3.3. The neglect of offenders in cybercrime analysis: problem or opportunity?

One of the pioneers of Environmental Criminology, Ray Jeffery (1977), coined this term for the first time to defend the need for a school of thought that shifted the focus of attention from the individual offender to the environment. Jeffery aimed to go further than the ecological approaches of Social Disorganization Theory, in which emphasis was placed not on the area where the crime occurred but on the offender who committed the crime in a given area (Shaw and McKay 1942). In this way, the author placed the ecological (geographic) pattern of crime, and not the offender, at the center of the analysis. And others subsequently followed this scheme, such as: RAT, which started from a static concept of motivation regarding the offender and placed the dynamism in the targets and the guardians; CPT, which gave full prominence to the role of the place; and RCT, which seemed to be built on the figure of the offender, but which in the end still focused its attention on the situational environment. The discipline’s general lack of interest in the elements that surround the offender (e.g., motivation, punishment, rehabilitation) in favor of the environment has been called neglect of offenders. Some authors have pointed out that such neglect may harm the development of the approach or, at least, it can limit it considerably (Bottoms 2012; Cullen and Kulig 2018).

It is not that criminal motivation is not relevant to the configuration of the crime event, but rather that analytically it is preferable to divert attention from this element and focus on those for which the implementation of preventive strategies is more plausible. This may be particularly appropriate in the case of crime events in cyberspace, where criminal motivations are the most static of all elements of crime, so diverting focus from the offender to other elements may be the best way to approach the analysis of the issue and the implementation of prevention strategies. To a certain extent, this is what happens especially, but not only, with cyber-dependent crimes. When this typology of cybercrime is studied, there is a tendency to assume the economic motivation of the offender, while what is unknown are those elements that, in effect, end up configuring the crime itself, such as: cybercrime enablers (Broadhurst et al., 2014), vulnerabilities defined by the daily activities of the victim (Bossler and Holt 2009), or the lack of surveillance in certain digital environments (Maimon et al. 2014).

Peter Grabosky (2001) was the first to highlight this situation in relation to cybercrime. When analyzing the similarities and differences between cyber criminality and physical crime, the author affirmed that criminals' motivations would remain the same, but that criminal opportunities would change. In this way, he emphasized the need to focus the analysis on guardians and, in particular, on victims by stating: "In cyberspace today, as on terrestrial space two millennia ago, the first line of defence will be self-defence" (p 248). We believe that the criminological analysis of the motivations of cybercriminals is still necessary and that very interesting advances have been made from various theoretical approaches (Bossler and Holt 2016). But we also believe that in the cybercrime event it is so difficult to obtain real information about the offender and his motivations, the variability of the potential objectives is generally enormous, the most stable element is the criminal motivation, and, moreover, the technological and situational seems intuitively so determinant (especially in cyber-dependent crimes). Thus, the environmental approach is particularly suitable as it is not particularly focused on "why someone commits a crime", but rather on "why a cyber-attack has affected one system and not another", "how an offender has managed to access a system", or "at what time there are more cyber-attacks". This does not mean that applying an environmental approach to cybercrime necessarily implies ignoring the offender, but rather understanding that within this analytical framework their motivations are relevant when they are related to the criminal opportunity structure. Some authors have already conducted research in this regard and have used crime scripts to analyze interviews of cyber offenders with the ultimate goal of proposing evidence-based SCP strategies (Hutchings and Holt 2017). But it is also possible to apply other frameworks of Environmental Criminology to advance the study of the cyber offender. For example, RAT and CPT could be applied to determine which cyber places are visited by cyber offenders and when they do so, to apply social network analysis techniques to identify with whom they relate and how, or to conduct studies of (near) repeat victimization to understand which targets they prefer to choose and why.

3.4. Cybercrime and crime controls: beyond self-protection

We tend to almost intuitively relate the function of crime control to the police. In fact, most experiments that have evaluated the effectiveness of crime control have done so based on a concept of formal control (Braga 2005; Weisburd et al. 2010). However, Environmental Theories have always placed the emphasis on social controls as the main elements of crime control. When Felson develops RAT and refers to the capable guardian, he does not necessarily refer to the police or the justice system, but to ordinary people whose mere presence can discourage the occurrence of a crime (Cohen and Felson 1979). In the same way, when developing the concept of the handler, this does not refer to a probation officer who watches over a potential offender, but to anyone who has such a close relationship with the offender that they are able to exercise control over them (Felson 1986). And despite the fact that when Eck (1994) introduces place managers he does so in the context of his work on illicit drug markets, he does not do this with formal controls in mind, but rather any person responsible for taking care of specific places (e.g., janitors, bus drivers, waiters).

When guardianship is analyzed in cyberspace, it is generally assumed that surveillance and protection related to technical self-protection systems (e.g., antivirus, firewall) are analogous to the concept of a capable guardian. Aside from the question of whether these measures should be integrated into the idea of capable guardian or target suitability, the indisputable fact is that to assess the effect of guardianship on cybercrime we must go further and return to: (1) the notion of social control, and (2) specific control figures such as managers and handlers. The social control exercised by a parent through the tools of parental control installed on their child's computer is very different from that practiced by a high school teacher who detects a case of cyberbullying in his class and this, in turn, is different from the control performed by one workmate over another in a social network when the latter publishes a scam message. However, all of them fall within the category of social controls. In addition, we must analyze what are the elements that turn a control into an effective prevention system. In this sense, Vakhitova and Reynald (2014) have suggested that for a person to actively perform the role of guardianship in cyberspace they must first have enough contextual awareness of their environment. The authors add that place managers perform the important function of facilitating the intervention of these potential guardians by increasing their contextual awareness.

Environmental Criminology has always placed emphasis on the specificity of situations and, therefore, it is inconsistent to encompass all informal controls in a homogeneous category. The main consequence of this is the difficulty to evaluate informal controls, which leads to an almost complete lack of knowledge about their effects on crime. And, ultimately, it raises a debate about the usefulness of the concept (Cullen and Kulig 2018). If informal social control has as much relevance in the environmental approach as is presumed, it is necessary to break down the concept in such a way that we are able to specify its comprising elements and, later, develop a taxonomy of controls that serve to delimit each typology in each context. Thus, in the process of elaborating explanatory models of cybervictimization, Bossler and Holt (2009; Holt and Bossler 2013) develop a classification for the guardian in which they distinguish three categories: social guardianship (i.e., peers), physical guardianship (i.e., antivirus), and personal guardianship (i.e., skills). This is the only way to design adequate methodologies to measure the phenomenon in a manner that enables understanding of its preventive scope in cyberspace. In fact, there are constructs of similar complexity that have a defined methodological standard. For example, Sampson's concept of collective efficacy, defined as "social cohesion among neighbors combined with their willingness to intervene on behalf of the common good" (Sampson et al. 1997 p 918), has shown its operationalization and methodological consistency as an indicator of informal social control over violence. It is essential to carry out a similar methodological exercise that allows the elements of informal social control of crime proposed by environmental theories to be adapted to the virtual environment, for example, a concept of digital community constituted by the existence of interpersonal interactions in a social network.

4. Conclusions

After more than a decade of reflection on the applicability of traditional criminological theories to crime committed through Internet, it is rightly stated that the analysis and explanation of each cybercrime requires consideration of a variety of theoretical frameworks (Bossler and Holt 2016). Some of the environmental approaches such as RAT or RCT are among those that academic literature has considered for the task of understanding some of the explanatory aspects of cybercrime, in this case those related to the environment where they are perpetrated. In this chapter we have tried to further the debate.

Firstly, it has been demonstrated that all the approaches that comprise Crime Science are applicable to the new space of personal intercommunication that is cyberspace. This includes CPT and the applications of the "crime and place" approach, if it is understood that the "place" of convergence of offenders and targets in the absence of guardians in cybercrime will generally be a digital place, and provided that the implications of this are properly developed. Environmental Criminology was conceived for the geographical-physical, because it arose from the need to refocus prevention from the subject to the place and, at that time, the only place was physical. But, as the most important theorists of this perspective have shown, the key to the approach was never the geographical place, but the crime event (Clarke 2010; Felson and Eckert 2016); in other words, the spatial-temporal convergence of the minimum elements of crime that can also be found on the Internet: an environment that also configures the daily actions of people and that is structured in different spaces where they interact.

Secondly, it was stated that the greatest explanatory potential of environmental theories is obtained from the symbiosis between them and not so much from the use of each of them as separate pieces. RAT acquires a much greater explanatory potential for each cybercrime if it is linked to the diverse places where, in different ways, people converge on the Internet. The questions that CPT tries to solve, such as which cyber places are the most relevant in each crime event, what are the characteristics of the cyber places that contain more crime, or in which moments is the risk of cybervictimization higher, cannot be answered without considering the daily routines of offenders and victims. RCT and its preventive corollary, SCP, or CPTED, will acquire all their applicative potential in relation to cybercrime if we take into consideration the natural surveillance in the cyber places and other features of CPT, as well as if we understand the role of super controllers in cybercrime prevention.

Finally, this chapter shows that Environmental Criminology can be more than just another theoretical approach, and that it is complementary to others, for cybercrime analysis. If it adapts to the new environment and maintains the essence of the approach, it can constitute an appropriate situational explanatory framework from which to design the best preventive strategies to avoid cybercrime and to reduce its harmful effects. After all, this has always been the strength of the environmental approach: shifting analysis from what is most difficult to intervene in and modify (i.e. individual motivation) to what is easiest (i.e. opportunity, and the environment). The demands of cybercrime prevention fit perfectly with this analytical and preventive philosophy. If, as one of the pioneers of the subject said when referring to crime committed in physical space, crime prevention requires focusing on the environment (Jeffery 1977), then environmental approaches constitute social approaches to understanding the cybercrime event that, by focusing on the different digital environments in which these events occur, will be highly effective in the future.

Funding

This research has been funded by the Spanish Ministry of Economy, Industry, and Competitiveness under the Criminology, empirical evidence, and Criminal policy Project: on incorporating scientific evidence to decision-making regarding criminalization of conducts. Reference DER2017-86204-R.

This research has been funded by the Spanish Ministry of Education, Culture and Sports under the FPU Grant. Reference FPU16/01671.

Acknowledgements

We thank the editors of this fantastic Handbook, and especially Prof. Tom Holt from Michigan State University, for their confidence in us to write this chapter on Environmental Theories. We would also like to thank Prof. Marcus Felson of Texas State University for his insights in several discussions that have served to consolidate the research presented here. Finally, we would like to thank Prof. Steven Kemp of the University of Girona for his comments that have greatly improved the translation of this work.

Cross-references

Chapter 23, Routine Activities.

Chapter 24, Rational Choice/deterrence.

References

Agarwal, N., Gupta, R., Singh, S. K., & Saxena, V. (2017). Metadata based multi-labelling of YouTube videos. In *7th International Conference on Cloud Computing, Data Science & Engineering-Confluence* (pp. 586-590). Noida: IEEE. http://dx.doi.org/10.1109/CONFLUENCE.2017.7943219

Aldridge, J., & Décary-Hétu, D. (2014). Not an 'Ebay for Drugs': the Cryptomarket 'Silk Road' as a paradigm shifting criminal innovation. http://dx.doi.org/10.2139/ssrn.2436643

Barr, R., & Pease, K. (1990). Crime placement, displacement, and deflection. *Crime and justice*, *12*, 277-318. https://doi.org/10.1086/449167

Birks, D., Townsley, M., & Stewart, A. (2012). Generative explanations of crime: using simulation to test criminological theory. *Criminology*, *50*(1), 221-254. https://doi.org/10.1111/j.1745-9125.2011.00258.x

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, *3*(1), 400-420.

Bossler, A., & Holt, T. J. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. New York, NY: Routledge.

Bottoms, A. (2012). Developing socio-spatial criminology. In, M. Maguire, R. Morgan and R. Reiner (Eds.), *The Oxford Handbook of Criminology* (pp. 450-488). Oxford, UK: Oxford University Press. https://doi.org/10.1093/he/9780199590278.003.0016

Bowers, K., & Johnson, S. D. (2016). Situational prevention. In, D. Weisburd, D. P. Farrington and C. Gill (Eds.), *What works in crime prevention and rehabilitation: Lessons from systematic reviews* (pp. 111–36). New York, NY: Springer.

Braga, A. A. (2005). Hot spots policing and crime prevention: A systematic review of randomized controlled trials. *Journal of Experimental Criminology*, *1*(3), 317-342. https://doi.org/10.1007/s11292-005-8133-z

Brantingham P. L., & Brantingham, P. J. (1981). Notes on the Geometry of Crime. In, P. J. Brantingham and P. L. Brantingham (Eds.), *Environmental Criminology* (pp. 27-53). Beverly Hills, CA: Sage Publications.

Brantingham, P. L. (2011). Computational criminology. In *2011 European Intelligence and Security Informatics Conference (EISIC),* (pp. 3-3). IEEE.

Brantingham, P., & Brantingham, P. (1995). Criminality of place. *European journal on criminal policy and research, 3*(3), 5-26. https://doi.org/10.1007/BF02242925

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). An analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology*, *8*(1), 1-20.

Burnap, P., & Williams, M. L. (2015). Cyber hate speech on twitter: An application of machine classification and statistical modeling for policy and decision making. *Policy & Internet*, *7*(2), 223-242. https://doi.org/10.1002/poi3.85

Caneppele, S., & Aebi, M. F. (2017). Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes. *Policing: A Journal of Policy and Practice*. https://doi.org/10.1093/police/pax055

Capone, D., & Nichols, W. J. (1976). Urban Structure and Criminal Mobility. *American Behavioral Scientist, 20*(2), 199-213. https://doi.org/10.1177/000276427602000203

Choi, K. S., & Lee, J. R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers in Human Behavior, 73,* 394-402. https://doi.org/10.1016/j.chb.2017.03.061

Clarke, R. V. (1992). *Situational Crime Prevention: Successful Case Studies*. New York, NY: Harrow and Heston Publishers.

Clarke, R. V. (1997). *Situational Crime Prevention: Successful Case Studies*. 2nd edition. Guilderland, NY: Harrow and Heston Publishers.

Clarke, R. V. (2010). Crime science. In, E. McLaughlin and T. Newburn (Eds.), *The SAGE Handbook of Criminological Theory* (pp. 271-283). London, UK: SAGE Publications. http://dx.doi.org/10.4135/9781446200926.n15

Clarke, R. V. (2018). Book Review [Review of the book *Place Matters: Criminology for the Twenty-First Century*, by Weisburd, D., Eck, J. E., Braga, A. A., & Cave, B.]. *Journal of Criminal Justice Education, 29*(1), 157-159.

Clarke, R. V., & Weisburd, D. (1994). Diffusion of crime control benefits: Observations on the reverse of displacement. *Crime prevention studies*, *2*, 165-184.

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*(4), 588-608.

Cornish, D. B., & Clarke, R. V. (1986). *The Reasoning Criminal*. New York, NY: Springer-Verlag.

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime prevention studies*, *16*, 41-96.

Cozens, P. M., Saville, G., & Hillier, D. (2005). Crime prevention through environmental design (CPTED): a review and modern bibliography. *Property management*, *23*(5), 328-356. https://doi.org/10.1108/02637470510631483

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International review of victimology*, *21*(2), 187-204. https://doi.org/10.1177/0269758015571471

Cullen, F. T., & Kulig, T. C. (2018). Evaluating Theories of Environmental Criminology: Strengths and Weaknesses. In, G. J. N. Bruinsma and S. D. Johnson (Eds.), *The Oxford Handbook of Environmental Criminology* (pp. 160-176). Oxford, UK: Oxford University Press. https://doi.org/10.1093/oxfordhb/9780190279707.013.7

Décary-Hétu, D., & Morselli, C. (2011). Gang Presence in Social Network Sites. *International Journal of Cyber Criminology*, *5*(2), 876-890.

Eck, J. (1994). Drug markets and drug places: A case-control study of the spatial structure of illicit drug dealing. Doctoral dissertation. University of Maryland.

Ekblom, P. (1997). Gearing up against crime: A dynamic framework to help designers keep up with the adaptive criminal in a changing world. *International Journal of Risk Security and Crime Prevention, 2*, 249-266.

Felson, M. (1986). Linking criminal choices, routine activities, informal control, and criminal outcomes. In, D. Cornish and R. Clarke (Eds.), *The Reasoning Criminal* (pp. 119-128). Secaucus, NJ: Springer-Verlag

Felson, M. (2012). Prólogo. In F. Miró-Llinares, *El Cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio* (pp. 13-16) [Foreword]. Madrid: Martial Pons.

Felson, M., & Eckert, M. (2016). *Crime and Everyday Life*. 5th edition. Los Angeles, CA: Sage Publications.

Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The rise of social bots. *Communications of the ACM*, *59*(7), 96-104. https://doi.org/10.1145/2818717

Gabor, T. (1981). The crime displacement hypothesis: An empirical examination. *Crime & Delinquency*, *27*(3), 390-404. https://doi.org/10.1177/001112878102700306

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies*, *10*(2), 243-249. https://doi.org/10.1177/a017405

Guerette, R. T., & Bowers, K. J. (2009). Assessing the extent of crime displacement and diffusion of benefits: A review of situational crime prevention evaluations. *Criminology*, *47*(4), 1331-1368. https://doi.org/10.1111/j.1745-9125.2009.00177.x

Guerry, A. M. (1833). *Essai sur la statistique morale de la France*. Paris: Crochard.

Guo, R. M. (2008). Stranger danger and the online social network. *Berkeley Technology Law Journal*, *23*(1), 617-644. https://doi.org/10.15779/Z38J69J

Harries, K. (1999). *Mapping crime: Principles and practice.* Washington, DC: National Institute of Justice.

Harries, K. D. (1976). Cities and crime: A geographic model. *Criminology*, 14, 369-386. https://doi.org/10.1111/j.1745-9125.1976.tb00029.x

Hartel, P. H., Junger, M., & Wieringa, R. J. (2010). Cyber-crime science = crime science + information security. University of Twente. Retrieved from: https://research.utwente.nl/files/5095739/0_19_CCS.pdf

Hinduja, S., & Kooi, B. (2013). Curtailing cyber and information security vulnerabilities through situational crime prevention. *Security Journal, 26*(4), 383-402. https://doi.org/10.1057/sj.2013.25

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30*(1), 1-25. https://doi.org/10.1080/01639620701876577

Holt, T. J., & Bossler, A. M. (2013). Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice, 29*(4), 420-436. https://doi.org/10.1177/1043986213507401

Holt, T. J., Smirnova, O., & Hutchings, A. (2016). Examining signals of trust in criminal markets online. *Journal of Cybersecurity*, *2*(2), 137-145. https://doi.org/10.1093/cybsec/tyw007

Holt, T. J., van Wilsem, J., van de Weijer, S., & Leukfeldt, R. (2018). Testing an Integrated Self-Control and Routine Activities Framework to Examine Malware Infection Victimization. *Social Science Computer Review*. https://doi.org/10.1177/0894439318805067

Hosseinmardi, H., Mattson, S. A., Rafiq, R. I., Han, R., Lv, Q., & Mishra, S. (2015). Detection of cyberbullying incidents on the Instagram social network. *arXiv preprint arXiv:1503.03909.*

Hutchings, A., & Clayton, R. (2016). Exploring the provision of online booter services. *Deviant Behavior*, *37*(10), 1163-1178. https://doi.org/10.1080/01639625.2016.1169829

Hutchings, A., & Holt, T. J. (2014). A crime script analysis of the online stolen data market. *British Journal of Criminology*, *55*(3), 596-614. https://doi.org/10.1093/bjc/azu106

Hutchings, A., & Holt, T. J. (2017). The online stolen data market: disruption and intervention approaches. *Global Crime, 18*(1), 11-30. https://doi.org/10.1080/17440572.2016.1197123

Jeffery, C. R. (1977). *Crime prevention through environmental design*. Beverly Hills, CA: Sage Publications.

Junger, M., Montoya, L., Hartel, P., & Heydari, M. (2017). Towards the normalization of cybercrime victimization: A routine activities analysis of cybercrime in Europe. In, 2017 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA), (pp. 1-8). IEEE. https://doi.org/10.1109/CyberSA.2017.8073391

Khey, D. N., & Sainato, V. A. (2013). Examining the correlates and spatial distribution of organizational data breaches in the United States. *Security Journal*, *26*(4), 367-382. https://doi.org/10.1057/sj.2013.24

Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. *Social Science Computer Review, 30*(4), 470-486. https://doi.org/10.1177/0894439311422689

Kigerl, A. C. (2013). Infringing nations: Predicting software piracy rates, bittorrent tracker hosting, and p2p file sharing client downloads between countries. *International Journal of Cyber Criminology, 7*(1), 62-80.

Klausen, J., Barbieri, E. T., Reichlin-Melnick, A., & Zelin, A. Y. (2012). The YouTube Jihadists: A social network analysis of Al-Muhajiroun's propaganda campaign. *Perspectives on Terrorism*, *6*(1), 36-53.

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking*, *17*(8), 551-555. https://doi.org/10.1089/cyber.2014.0008

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. Deviant Behavior, 37(3), 263-280. https://doi.org/10.1080/01639625.2015.1012409

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2016). Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks. *British Journal of Criminology, 57*(3), 704-722. https://doi.org/10.1093/bjc/azw009

Maimon, D., Alper, M., Sobesto, B., & Cukier, M. (2014). Restrictive deterrent effects of a warning banner in an attacked computer system. *Criminology*, *52*(1), 33-59. https://doi.org/10.1111/1745-9125.12028

Maimon, D., Kamerdze, A., Cukier, M., & Sobesto, B. (2013). Daily trends and origin of computer-focused crimes against a large university computer network: An application of the routine-activities and lifestyle perspective. *British Journal of Criminology*, *53*(2), 319-343. https://doi.org/10.1093/bjc/azs067

Maimon, D., Wilson, T., Ren, W., & Berenblum, T. (2015). On the relevance of spatial and temporal dimensions in assessing computer susceptibility to system trespassing incidents. *British Journal of Criminology*, *55*(3), 615-634. https://doi.org/10.1093/bjc/azu104

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behavior*, *31*(5), 381-410. https://doi.org/10.1080/01639620903004903

Medina-Ariza, J. J. (2011). *Políticas y estrategias de prevención del delito y seguridad ciudadana*. Madrid: Edisofer.

Miró-Llinares, F. (2011). La oportunidad criminal en el ciberespacio: aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. *Revista Electrónica de Ciencia Penal y Criminología*, 13(7), 1-55.

Miró-Llinares, F. (2015). That Cyber Routine, That Cyber Victimization: Profiling Victims of Cybercrime. In, R. G. Smith, R. C. C. Cheung and L. Y. C. Lau (Eds.), *Cybercrime Risks and Responses* (pp. 47-63). London, UK: Palgrave Macmillan. https://doi.org/10.1057/9781137474162_4

Miró-Llinares, F., & Johnson, S. D. (2018). Cybercrime and Place: Applying Environmental Criminology to Crimes in Cyberspace. In, G. J. N. Bruinsma and S. D. Johnson (Eds.), *The Oxford Handbook of Environmental Criminology* (pp. 883-906). Oxford, UK: Oxford University Press. https://doi.org/10.1093/oxfordhb/9780190279707.013.39

Miró-Llinares, F., & Rodriguez-Sala, J. J. (2016). Cyber hate speech on twitter: Analyzing disruptive events from social media to build a violent communication and hate speech taxonomy. *International Journal of Design & Nature and Ecodynamics*, *11*(3), 406-415. https://doi.org/10.2495/DNE-V11-N3-406-415

Miró-Llinares, F., Moneva, A., & Esteve, M. (2018). Hate is in the air! But where? Introducing an algorithm to detect hate speech in digital microenvironments. *Crime Science, 7*(15), 1-12. https://doi.org/10.1186/s40163-018-0089-1

Näsi, M., Räsänen, P., Kaakinen, M., Keipi, T., & Oksanen, A. (2017). Do routine activities help predict young adults' online harassment: A multi-nation study. *Criminology & Criminal Justice, 17*(4), 418-432. https://doi.org/10.1177/1748895816679866

Navarro, J. N., & Jasinski, J. L. (2013). Why girls? Using routine activities theory to predict cyberbullying experiences between girls and boys. *Women & Criminal Justice, 23*(4), 286-303. https://doi.org/10.1080/08974454.2013.784225

Newman, G. R., & Clarke, R. V. (2003). *Superhighway Robbery: preventing e-commerce crime*. New York, NY: Routledge.

Pease, K. (2001). Crime futures and foresight: Challenging criminal behaviour in the information age. In, D. Wall (Ed.), *Crime and the Internet* (pp. 30-40). London: Routledge.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267-296. https://doi.org/10.1177/0022427810365903

Quetelet, L. A. J. (1842). *A treatise on man and the development of his faculties*. Edinburgh: W. and R. Chambers.

Reyns, B. W. (2010). A situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers. *Crime Prevention and Community Safety*, *12*(2), 99-118. https://doi.org/10.1057/cpcs.2009.22

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior, 38*(11), 1149-1169. https://doi.org/10.1177/0093854811421448

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency, 50*(2), 216-238. https://doi.org/10.1177/0022427811425539

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International journal of offender therapy and comparative criminology, 60*(10), 1119-1139. https://doi.org/10.1177/0306624X15572861

Rossmo, D. K. (1999). *Geographic profiling*. Boca Raton, FL: CRC press.

Sampson, R. J., Raudenbush, S. W., & Earls, F. (1997). Neighborhoods and violent crime: A multilevel study of collective efficacy. *Science, 277*, 918-924. https://doi.org/10.1126/science.277.5328.918

Shaw, C. R., & McKay, H. D. (1942). *Juvenile delinquency and urban areas: A study of rates of delinquency in relation to differential characteristics of local communities in American cities.* Chicago: University of Chicago Press.

Sherman, L. W., Gartin, P. R., & Buerger, M. E. (1989). Hot spots of predatory crime: Routine activities and the criminology of place. *Criminology, 27*(1), 27-56. https://doi.org/10.1111/j.1745-9125.1989.tb00862.x

Shu, K., Sliva, A., Sampson, J., & Liu, H. (2018). Understanding cyber attack behaviors with sentiment information on social media. In, R. Thomson, C. Dancy, A. Hyder and H. Bisgin (Eds.), *Social, Cultural, and Behavioral Modeling* (pp. 377-388). Cham: Springer. https://doi.org/10.1007/978-3-319-93372-6_41

Vakhitova, Z. I., & Reynald, D. M. (2014). Australian Internet users and guardianship against cyber abuse: An empirical analysis. *International Journal of Cyber Criminology*, *8*(2), 156-171.

Van Wilsem, J. (2013). 'Bought it, but never got it' Assessing risk factors for online consumer fraud victimization. *European Sociological Review, 29*(2), 168-178. https://doi.org/10.1093/esr/jcr053

Vishwanath, A. (2014). Habitual Facebook use and its impact on getting deceived on social media. *Journal of Computer-Mediated Communication, 20*(1), 83-98. https://doi.org/10.1111/jcc4.12100

Wall, D. S. (2007). Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research, 8*(2), 183-205. https://doi.org/10.1080/15614260701377729

Wei, C., Sprague, A., Warner, G., & Skjellum, A. (2008, March). Mining spam email to identify common origins for forensic application. In *Proceedings of the 2008 ACM symposium on Applied computing* (pp. 1433-1437). ACM.

Weisburd, D., & Green, L. (1995). Policing drug hot spots: The Jersey City drug market analysis experiment. *Justice Quarterly*, *12*(4), 711-735. https://doi.org/10.1080/07418829500096261

Weisburd, D., Bernasco, W., & Bruinsma, G. (Eds.). (2009). *Putting crime in its place*. Springer New York.

Weisburd, D., Telep, C. W., Hinkle, J. C., & Eck, J. E. (2010). Is problem-oriented policing effective in reducing crime and disorder? Findings from a Campbell systematic review. *Criminology & Public Policy*, *9*(1), 139-172. https://doi.org/10.1111/j.1745-9133.2010.00617.x

Welsh, B. C., & Farrington, D. P. (2009). Public area CCTV and crime prevention: an updated systematic review and meta-analysis. *Justice Quarterly*, *26*(4), 716-745. https://doi.org/10.1080/07418820802506206

Wolfe, S. E., Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2016). Routine cell phone activity and exposure to sext messages: Extending the generality of routine activity theory and exploring the etiology of a risky teenage behavior. *Crime & Delinquency*, *62*(5), 614-644. https://doi.org/10.1177/0011128714541192

Wortley, R., & Townsley, M. (Eds.) (2016). *Environmental criminology and crime analysis*. 2nd edition. London: Routledge.

Yar, M. (2005). The Novelty of ‘Cybercrime’ An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407-427. https://doi.org/10.1177/147737080556056