Copyright © 2015 International Journal of Cyber Criminology (IJCC) – Publisher & Editor-in-Chief – K. Jaishankar
ISSN: 0973-5089 - January – June 2015. Vol. 9 (1): 35–54. DOI: 10.5281/zenodo.22239

Understanding Cyber Victimization: Digital Architectures and the Disinhibition Effect

Jose R. Agustina[1]
Universitat Internacional de Catalunya, Barcelona, Spain

Abstract

Researchers in the fields of sociology, psychology, behavioural sciences and law are trying to comprehend the radical rise of a new relational paradigm derived from the current proliferation of ICT. Crime dynamics and victimisation are not alien to the set of changes wrought by the digital era. The way in which victims behave in cyber space decisively elevates their risk of victimization. In connexion with this, the design of digital architectures notably increases criminal opportunities and facilitates cyber victimisation i.e. the defining traits of cyber space affect people's daily lives and incline them to adopt riskier lifestyles. Based on Routine Activity Theory and Lifestyle Theory, along with the interesting work of Suler (2004), the present article shows the importance of victimological perspective in explaining cyber criminal events and designing prevention strategies. Stemming from literature review, this analysis will focus on describing a set of psychological and sociological traits that comprise the profile of victims and explaining how the surroundings influence one's thoughts, desires, and actions.

Keywords: Cyber Victimization, Digital Architecture, Disinhibition Effect.

Introduction

We live immersed in a society that has undergone vertiginous changes in a remarkably short amount of time. Researchers in the fields of sociology, psychology, behavioural sciences, and law are trying to comprehend the more-or-less radical rise of a new *relational paradigm* of personal and social interactions (e.g. Castells, 1997). The proliferation of Information and Communication Technologies (hereafter, ICT) is a reality that continues to advance inexorably, permeating everything in our daily lives. We often hear about an intergenerational 'digital gap' (Tapscott, 2008; Palfrey & Gasser, 2008); however, aside from the fact that this supposed gap will soon cease to exist, technology actually affects everyone. Crime dynamics and, consequently, victimisation are not alien to the set of changes wrought by the digital era.

With a focus on the prevention of cyber crime, in the following lines I will describe the way in which the behaviour of victims in cyber space decisively elevates their risk of victimisation, singling out some environmental predictors of online victimisation. To do so, I will first outline why the design of digital architectures notably increases criminal opportunities and facilitates cyber victimisation, and how the defining traits of cyber space

[1] Professor, Department of Criminal Law and Criminology, Universitat Internacional de Catalunya, Barcelona, Spain. Email: jragustina@uic.es

affect people's daily lives and incline them to adopt riskier lifestyles. Then, I will try to show the importance of the victimological perspective in explaining the criminal event, designing prevention strategies and assigning criminal liability. My analytical perspective is supported, principally, by *routine activity theory* (Cohen & Felson, 1979) and *lifestyle theory* (Hindelang, Gottfredson & Garofalo, 1978), along with the criminological perspectives encompassed by *opportunity theory*. The latter are related to the theory formulated by Jaishankar, "*Space Transition Theory of Cyber Crimes*" (Jaishankar, 2008), in which he shows why people act differently when transitioning from a physical space to a virtual one. In his view, the fundamental criminogenic factors of cyber space include alack of dissuasion associated with anonymity, as well as a criminal propensity of some people who feel repressed in the 'real' world to liberate themselves online and commit crimes in cyber space. The interesting work of Suler (2004) follows the same line, as we will see in detail. Finally, in the Spanish context, my analysis will be strongly influenced by the excellent contribution of Miró Llinares (2012).

Subsequently, beginning with the criminogenic characteristics of digital architectures, I will describe based on literature review a set of psychological, anthropological, and sociological traits that comprise the profile of victims or, at least, certain groups of victims. This analysis will focus on describing how the surroundings influence one's thoughts, desires, and actions. Finally, I will summarise some cyber crime (or more accurately, cyber victimisation) prevention strategies, concluding my reflections with a critical review of certain profile stereotypes of both offenders and victims.

1. Introduction: Digital Architectures and Human Nature—Technology and Crime

In the face of new forms of delinquency associated with the rise of internet users, I suggested elsewhere (Agustina, 2009) that the field of criminology should resolutely undertake the study of those criminogenic factors that facilitate illicit behaviour. Digital architectures generate an atmosphere of anonymity that protects, promotes, and nourishes new methods of attack against people and institutions. Furthermore, due to the very nature of the web and the possibilities of intercommunication presented by ICT, criminal conduct acquires a harmful potential that multiplies the potential injuries to third parties. In this sense, it is necessary to define and deepen the existing relationships between (i) the limits and rules governing this virtual space, and (ii) the consequent attraction or generation of delinquency. But situational prevention strategies run up against internet users' privacy, freedom of expression and freedom of navigation.

Although cyber space continues to be a 'dark space' that foments anonymity (Katyal, 2003), as concerns about cyber crime increase, strength is gained by the idea that certain structural changes in digital architectures could cause an abrupt turn similar to the eruption of gas lighting and electricity in the dark streets of crime-prone cities. From this perspective, we should be looking for ways to cast light on the users of cyber space (Katyal, 2003).

However, the adoption of mechanisms of transparency and control on the internet would be an attack on the aforementioned freedom of navigation, for a *principle of limited privacy* would lessen one's freedom to act unidentified. The tension between freedom (privacy) and security (prevention) has been central in the social and political debate. Thus, the dilemma is clear: we must choose between greater freedom to navigate the web, free of controls or the need for identification; and greater tolerance with respect to the new criminal opportunities that come naturally in a space where anonymity has clear criminogenic consequences.[2] The web is—within the typology of spaces coined by Brantingham and Brantingham (1995)—as much a criminogenic space generating by its very nature delinquency (i.e. *crime-generator*), as a propitious space enticing the delinquent to commit crimes (i.e. *crime-attractor*), since the risk of detection is lower while highly attractive targets abound.

However, despite proposals favouring certain improvements and higher security, it does not appear that today's societies will choose to make the internet safe at all costs. It is therefore of greater importance to focus on protecting potential victims from the risks specific to virtual environments, and to delve into the causes of the imprudent use of ICT and the internet. The question lies, therefore, in analysing the vulnerability of victims and correcting shortcomings in their use of ICT—specifically, their inclination not to consider the risks of their actions.

Which parts of human nature are influenced by digital architectures? Marcus Felson (1994, p. 16) carefully studied human nature in order to understand criminal behaviour, examining how human situations vary according to context and how this influences our understanding of crime. His reflexions are as applicable to the explanation of offenders' inclination towards crime as to the victims' tendency to act without caution.

> First, consider the insight of *basic human frailty*. This is nothing more than the biblical notion that human beings are morally weak and that each individual needs help from society in order to withstand immoral temptations and pressures. Thus people with moral beliefs have difficulty meeting their own standards in practice, being capable of good and evil. The practical problem is to help people overcome their weaknesses by structuring society to reduce temptation. To be sure, some people are more "frail" than others, but all people have some frailty and temptability. This is quite different from saying people do not have strong enough beliefs about right and wrong. Rather it states that people have difficulty putting their moral beliefs into action, that is, in resisting temptations (Felson, 1994, p. 16).

How does the offender take advantage of the victim's weaknesses? Traditionally, there have been two forms in which one could commit a crime: *duobus modis fit iniuria: aut vi, aut fraude.* This famous maxim, excerpted from the work of Marco Tulio Ciceron (*De officiis, Liber 1, Caput 13),* indicates that all crimes—and, therefore, all victimisation—can be committed either by means of force or deceit. Later, however, crimes of imprudence were added to the classical catalogue, in which neither force nor deceit were the offender's *modus operandi.*

[2] In the final reviewing stage of this article, the scandal of the secret cyber space communications surveillance undertaken by the United States government had come to light, following a leak by Edward Snowden, a worker subcontracted by CIA to perform computer espionage tasks ("Un joven experto en espionaje pone contra las cuerdas a Obama" -*"A young espionage expert puts Obama on the ropes"*-, *El País*, 10 June 2013). For an interesting sociological analysis of the current tensions between privacy and public needs (e.g. with regard to former sex offenders, terrorism or medical histories), see Amitai Etzioni (2012).

Due to the particularities of the virtual space, deceit is the most common means of committing a cyber crime. And even in those offences allowed by ICT where deceitful artifices are not characteristic (e.g. libel and slander), offenders often resort to simulation or anonymity to achieve impunity.

The inclination to lie in order to manipulate and harm others is part of human nature, especially if the victim shows vulnerability or if the context presents a large number of suitable opportunities. Cyber space fosters attitudes of excessive trust, naivety or thoughtlessness, which are exploited by the offender to cloak him/herself in an appearance of veracity through anonymity.

Fraud and deceit are ancient arts, but cyber space provides a much higher number of victims, even for a sole perpetrator. In effect, technological changes have led to important changes in our ways of thinking and acting, with significant repercussions not only for anthropology, sociology or culture, but also for crime rates (Ogburn, 1964). Ogburn's principal thesis is that first a technological change irrupts, and then a sociological or cultural change occurs, leading to a changing tendency in the number and *modus operandi* of crimes. Felson (1997, pp. 82-83) suggests that the sociological description proposed by Ogburn reveals an important lesson in the criminological field, which is that we must stop assuming that changes in delinquency are caused by changes introduced into the culture. Without denying that this is relevant, he affirms that technology is ultimately the principal force driving social transformations and, thus, technological changes are what provoke changes in the forms of delinquency.

The consequences of this are intensely manifested at an anthropological level. It appears that technological changes maximise both human ingenuity and stupidity. With the help of ICT, *there's a sucker born every minute*—a well-known phrase attributed to Phineas T. Barnum—and the internet allows them to connect with each other and, above all, with those who might convert them into victims, with no need to interact in person.

Still, there continue to be few and unreliable studies of the incidence of the various forms of cyber victimisation, although among those few it is found that the number of cyber victims increases annually (Gordon et al., 2004). The statistical data are unreliable for various reasons (Choi, 2008). In the first place, the dark figure is very high, as it deals with crimes that cannot be detected without a high level of investigation. Police investigation in cyber space is especially complex due, often; to the high sophistication of cyber delinquents, and/or to the fact that these crimes are committed through systems or channels that hinder the offender's identification (emails (re)sent anonymously, message encryption systems, identity impersonation, etc.) (Furnell, 2002; Grabosky & Smith, 2001; Yar, 2005). Also, few crimes committed in cyber space are ever reported to authorities (Standler, 2002).

I will highlight, however, the results of the first study conducted in Spain about cyber victimisation (Miró Llinares 2013). These results demonstrate a prevalence of cyber crimes with the aim of cyber-fraud. Concretely, more than 45% of the Spanish population reports having received emails soliciting some type of suspicious favour or economic negotiation; and 43.6% report having received some type of email from a false identity. In terms of *malware* infections, 72.8% of the population recognizes having suffered one. And, significantly, 24.4% of the Spanish population has effectively suffered a patrimonial loss as a cyber fraud victim.

2. Some victimological considerations applied to cyber space

An examination of the victimological field's evolution reveals a diverse set of victimological typologies and classifications of victims (Schafer, 1997, p. 36; Mendelsohn 1956, pp. 105-7). Those typologies based upon a plurality of factors of risk, propensity or vulnerability has an advantage due to their multi-axial character (Herrera Moreno, 2006, p. 82). According to Herrera Moreno's classification (1996), victimisation in cyber space fits into the category of *contextual vulnerability*, a perspective that concentrates on the victim's interaction with the 'victimogenic environment' as a key factor.

Certainly, the interactions between offender and victim in virtual crimes are unique. Following the routine activity theory (Cohen & Felson, 1979), Miró Llinares (2011, 2012) has completed an exhaustive analysis of the modulations experienced by the three elements that must concur, in a given space and time, for a crime to occur: a *motivated offender*, an *adequate victim* (for the offender's motive), and the absence of *capable guardians.* His principal thesis is that the victim's own role in cyber space is far more determinant than her daily activities in the physical realm. According to his/her own personality, the victim sets the margins of the field of risk to which he/she will be subject (2012, p. 263). More importantly, given the particularities of the virtual environment, such risk exposure is diffuse and characterised by the difficulty in controlling one's own information, a tendency to remain over time (digital fingerprints are difficult to erase once the digital threshold has been crossed), and a highly expansive projection (since the victim opens herself up to a wider and more diverse circle of potential offenders).

In sum, the explanation, phenomenology and implications of criminal offences follow, above all from the victim's perspective, distinct patterns and characteristics when the crime is committed in cyber space (e.g. *bullying* or *cyber-stalking*, where the victim is constantly exposed to the harasser). As Miró Llinares indicates, using a metaphor put forth by Grabosky (2001), the question lies in determining the extent to which cyber crime, in contrast to the equivalent classical offences, is *old wine in new bottles*; that is to say, (i) if we are facing an essentially new type of delinquency to which traditional criminological theories from the physical realm do not apply; or, instead, (ii) we are dealing with the same types of crimes, though with different characteristics in the different contexts, but to which the same traditional theories and instruments still apply; or, finally, (iii) if it is a matter of "a criminality with identical configuring elements that are, however, essentially affected once translated into cyber space, which may significantly influence the explanation of crime and, therefore, its prevention" (Miró Llinares, 2001, p. 5).

In this way, classic crimes, whether they be against assets (such as robbery or fraud) or individuals (crimes against honour, sexual freedom or privacy), take on new features that considerably affect the *modus operandi* and, above all, the main protagonist of the criminal event, thereby intensely increasing the victim's exposure. In the words of Max Estrella, a central character in *Lights of Bohemia*, "[t]he classical heroes have gone to stroll in *Callejón del Gato* […] The classical heroes reflected in the concave mirrors become Esperpento" (Valle Inclán, 1920, Scene XII). The online offender grotesquely deforms his/her true image when presenting him/herself online and comes to alter the normal interactions between people and, consequently, the classical patterns of crime, in such a way that it becomes necessary to significantly modify the current criminological and dogmatic categories when analysing the same offences.

The relationship between offender and victim, mediated by 'virtual masks', helps the offender resort to deceitful appearances, camouflage and manipulative techniques, while also potentiating in the victim a series of cognitive-behavioural deficits that notably increase the risk of victimisation. Along with the unusual speed, intensity and extent with which crimes are committed online, interactions in cyber space foment highly criminogenic factors, such as: greater anonymity; greater impulsiveness, thoughtlessness and naivety in decision-making by the victim, who is frequently prisoner to impulsive consumerism; a lost sense of privacy, leading to a tendency to indiscriminately provide personal data to strangers; greater exhibitionism of feelings and corporeity, a source of greater imprudence that acts as an attractive force (for sexual harassers or swindlers); and a multiplication of the degrading effects, victimisation being suffered on a global stage.

Given the many masks provided by virtual environments, it can become difficult to delimit and distinguish the real self from the digital self. In this sense, Guinchard (2010, p. 178) points out that, "[a]s the Greek etymology suggests, a person may have two masks or personalities, one embodied, the other disembodied or 'virtual', represented by language with or without visual imagery. They may feel equally wounded when each 'mask' is attacked". Nevertheless, we must distinguish between a completely virtual reality in which the disassociation between the digital self and the real self is complete, and a virtual reality in which the physical reality continues to be present, however tenuously. Since the dividing line between the two categories is not at all clear, the existence of a *tangible impact* in the victim's real life becomes a key element for criminological and legal purposes. In this respect, again citing Guinchard, we can distinguish between those crimes that require an inescapable *physicality*, such as a murder or rape, from those other that do not (such as fraud, moral or sexual assault, or libel or slander). All this brings us to suggest that the traditional legal standards—the dogmatic categories of crime theory—need to be modified to take into account that, in fact, crimes can be committed in a distinct virtual form (Smyth, 2011, p. 22).

In the following lines, I will outline some of the principal criminal characteristics relating to context that should be taken into account when approaching the victimological question, especially in relation to the measures of self-protection taken by victims in virtual environments. To that end, I will focus on the implications of the victimological perspective regarding *crime prevention strategies* (criminological perspective), and I will refer tangentially to how this influences the *application of certain categories of the criminal theory* (criminal law perspective), when the space in which the crime occurs escapes to a direct relationship in the physical realm.

3. Place and Crime: Digital Architectures, Space Convergence and Schizophrenic Divergence

In the digital era, everyday activities, especially those of people who have "grown up digital" (Tapscott, 2008),[3] are increasingly wrapped up in digital architectures. In fact, the line between the virtual and the physical is not always clear. Today, adolescents find themselves increasingly connected through ICT; they express their identities and interact with each other in virtual space with surprising naturalness, expressing intimacy with greater intensity.

[3] The terms 'digital natives' and 'born digital' tend to be used to designate those who are born immersed in the digital era; it therefore is preferable to refer to the generation that has grown and matured in a digital environment as 'grown up digital' or the 'net generation'.

What distinguishes, then, these two spaces of social relations and communication? Without a doubt, the difference between the two realities stems from physical "contiguity" (Gutiérrez Puebla, 1998). But virtual reality continues to advance and, in some cases, almost bodily contact between people occurs, despite the distance. Think, for example, about remote surgical operations and advances in tele-medicine. Furthermore, with the birth of entirely virtual worlds, beginning in June 2003 with the creation of *Second Life*, we have opened up a new realm of social interactions—and therefore possible crimes—that present relevant legal questions.

Second Life, effectively, exists; it is a three-dimensional world in which its virtual inhabitants can shop, work, and explore endless new opportunities; the whole virtual community is an open space in which one can create her own personality and decide her own destiny, where the economy operates with its own form of currency (*Linden dollars)* convertible to American dollars, and where people can have all kinds of interactions (Guinchard, 2010). According to Smyth, "[t]his virtual mecca has provided new opportunities for crime because of its global reach, relatively low cost and near perfect anonymity. The damage that users can inflict in Second Life is not limited to the virtual world, but can result in significant harm to victims in real life" (2011, p. 21).

But let's return to more normal interactions within the virtual realm. These are relevant because human relationships between real people exist. For this reason, Miró Llinares refers to cyber space as "a space of communication that does not have a primary physical nature, but instead an essentially relational one", in which distance and space are contracted and, at the same time, the possibilities of encounter and communication between people expand (2011, p. 6). There is no doubt, then, that we can no longer refer to the 'virtual world'[4] versus the 'real world', since both dimensions form part of reality. Pease (2001) graphically contrasts *cyber space* with *meat space:* the only thing distinguishing the two spaces is the presence of the subject in flesh and bone, even though the effects of a relationship in cyber space can occasionally affect the victim's corporeity.

Based on the significant contributions of Katyal (2002), it is common to refer to digital architecture as a criminological factor, above all due to the conditions of anonymity that go along with it, and to point out the necessity of arbitrating strategies of crime prevention in function of context (Agustina, 2009). Thus, based upon the earlier contribution of Lawrence Lessig (1999, pp. 4-14)— whose idea is to identify architecture as a key element that could constrain online behaviour—there have since been interesting focuses on and approaches to space, geography and cyber crime (see, extensively, Miró Llinares 2012).

What difference is there between deception through the internet and in person; between stalking a victim at her home and doing it in cyber space; or between spying on someone through direct visual contact and doing so by installing a Trojan in the victim's webcam?

As Grabosky (2001, p. 248) indicates, certainly "the emotions of the scam characterized by the introduction of the Trojan Horse continue to be relevant in the creation of its digital descendants"; but what have changed are the offenders' abilities, their *modus*

[4] In fact, according to the Dictionary of the Royal Spanish Academy the term 'virtual' comes from Latin, specifically the term *virtus-is*: force, virtue. In its first sense it is defined as "1. adj. Having the virtue to produce an effect, even if it does not produce it presently, frequently as opposed to effective or real.

operandi, and the consequent increased risk of victimisation. That is to say, the change has operated in opportune conditions: the offenders find adequate victims in relatively favourable circumstances.

Nevertheless, the unity achieved by the convergence of the physical and virtual spaces contrasts with a tendency towards self defragmentation, giving rise to pathological ICT-user conducts showing symptoms of a certain *digital schizophrenia.*[5] It produces, as we shall see, a tendency towards divergence or disassociation between the digital self and the real self, to the extent that one can lead a double life online, separate from her everyday social life in the physical realm. Below we will see some manifestations.

4. Victimogenic Environments and Victimologic Profiles: the Disinhibition Effect in Online Behaviour and Victims' Naivety/Thoughtlessness

4.1. Online Disinhibition Effect

A primary characteristic of victims in cyber space relates to the disinhibition effect that the context exercises upon them. Various investigations of the behaviours of habitual internet users indicate that people say and do things in cyber space that they would not ordinarily say or do in their face-to-face relationships (Suler, 2004; Jaishankar, 2008; Agustina 2012). In online contexts people feel less constrained and they express themselves more openly than in their direct relationships. This phenomenon is already so widespread that it has begun to be called the *online disinhibition effect.* We can also speak of a tendency towards *digital schizophrenia,* when people are pushed to lead a double life online, a tendency that is strongly reinforced by conditions of anonymity and the subsequent defragmentation or splitting of the person, giving rise to a digital self separate from the real one.

Such disinhibition can give rise to certain benign effects, but it can also be accompanied by negative or even perverse ones. For example, indicates Suler (2004), it can be cathartic for some people to empty their hostile thoughts into an online *chat.* In an increasingly intimate e-mail relationship, people can quickly come to reveal personal information, later regretting it and feeling exposed, vulnerable or embarrassed. An intimate relationship can take shape excessively quickly and even falsely and is later destroyed when one of the two parties feels confused, anxious or disconcerted. Suler asks, "What elements of cyber space lead to this debilitation of the psychological barriers that block hidden feelings and needs?"

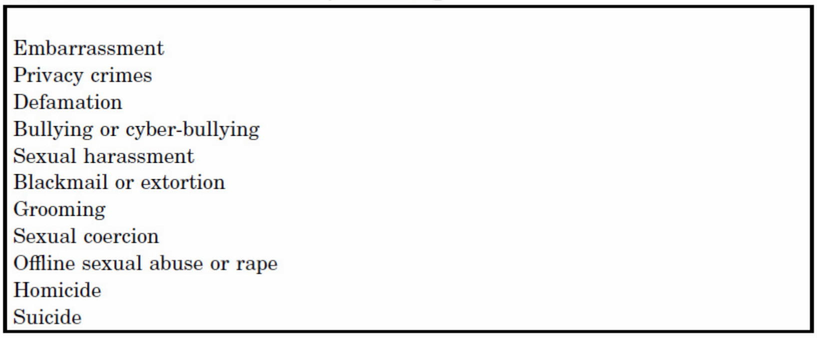
Suler (2004), while developing the characteristics of a *psychology for cyber space,* enumerates the following elements: (1) *dissociative anonymity:* the possibility of anonymity means that a person can guarantee that her online activity will not be associated with her "real life" activities, dissociating the two identities; (2) *invisibility:* the fact that people can enter web sites or chat rooms not only anonymously but also secretly, causing them to dare to enter sites that, otherwise, they would never visit—above all for shame and the consequences to their own reputations; (3) *asynchronicity*: in cyber space, interactions are not necessarily produced in real time. This provides a greater ability to think about and

[5] Understand the expression in a metaphorical-colloquial sense. Additionally, despite its etymology, *schizophrenia* is not the same as *dissociative identity disorder* (or 'multiple personality disorder', or 'split personality'), with which it has frequently been confused.

edit one's way of presenting oneself, giving greater security to adolescents (Valkenburg et al., 2011); it also facilitates situations in which, in a moment of impulse, a person writes a message that is very personal, hostile, or charged with emotions and then flees, a phenomenon that could be described as an 'emotional hit and run'; (4) *solipsistic introjection:* the fruit of an absence of reliable data on the other person, which can produce a psychological effect through which the subject assigns imaginary traits to the people with which she interacts online. The fantasies of the imagination, which can also occur in 'real' life, are considerably disinhibited online; (5) *dissociative imagination:* consciously or unconsciously, web users can come to perceive that the imaginary characters that they themselves created exist in another space; that their digital self, along with these other online people, lives in another dimension, separate from the demands and responsibilities of 'real' life, in this way producing a fragmentation or dissociation between the fictional online world and the facts of real offline life; (6) *minimization of status and authority:* on the internet everyone starts, more or less, from the same position, since all people (whether famous or possessing some position of authority) have equal access; and, additionally, the fact of being online means that people with a certain status or authority can lose the visible attributes of the 'real' world that distance them from the other mortals.

These disinhibition effects elevate, logically, the probability that users practise risky behaviours and end up being cyber victimised. Disinhibition causes the victim to cross the *risk threshold*. I have referred elsewhere to the inherent risks of the practice of *sexting* (Agustina, 2012) as a paradigmatic example of crossing a *red line* that opens the doors to an elevated risk of victimisation ("Sexting as a Threshold for Victimization"). Marginal to the complex discussion of whether certain conducts of *sexting* can be considered criminally relevant (for constituting the crime of distributing child pornography), there is no doubt that *sexting* is an important predictor of eventual forms of cyber-victimisation (Reyns et. al., 2011b). The simple act of putting explicitly sexual images into the hands of a third party opens the doors to extortion, blackmail, and vengeful or simply frivolous actions, because that graphic or audiovisual material can end up being distributed to an unlimited number of people (see below the table of *Crimes and risks derived from sexting*: Agustina, 2012, p. 93).

Table 7: *Crimes and risks derived from sexting*



Embarrassment
Privacy crimes
Defamation
Bullying or cyber-bullying
Sexual harassment
Blackmail or extortion
Grooming
Sexual coercion
Offline sexual abuse or rape
Homicide
Suicide

4.2. Naïve and Thoughtless Victims

As Bossler and Holt (2010) have mentioned, criminological theories with a situational focus (i.e. routine activity and lifestyle theories, as well as the other opportunity theories) have dominated the field of victimology. This has meant, unfortunately, that theories oriented to the individual have been practically ignored in the studies of victimisation, Along with the structural or situational disinhibition effect that generally influences online conduct, digital culture has especially affected those generations who have grown up within a digitalised environment since early childhood. How do today's adolescents act in their everyday lives? After the Cartesian maxim (*Cogito ergo sum,* or, *I think, therefore I am)*, we could formulate a new guideline for the generation that has 'grown up digital': "I tweet, I post, I blog, therefore I am!" That is to say, the disinhibition effect described here should be considered along with the fact that today's adolescents pass many hours a day between SMS, Whatsapp and Twitter, navigating online, participating in social networks or chats, and connected on their mobile phones. Despite the scarcity of empirical studies about which conducts are especially risky (Miró Llinares, 2012, pp. 272-273), as indicated by the author, the majority of studies of online victimisation focus on youth, "to whose guardianship society is especially sensitive", for the clear fact that it is youth who practice a more widespread use of ICT and carry out their daily activities in cyber space. Nevertheless, we need to see if youth are always the *adequate victim* that those *motivated delinquents* wish to encounter and, to do so, we would have to determine what motivates the offenders. For example, it appears reasonable, such as confirmed by the investigation of Ngo and Paternoster (2011) that, at a greater age, there is greater probability of suffering a malware infection or being subject to offensive or degrading messages. In any case, there are no studies covering a wide enough age range to permit differentiation by age, most studies having been performed on samples from juvenile, high school and university-aged populations (Miró Llinares, 2012; Reyns, et al., 2011a).

The disinhibition effect derived from a digitalized environment generates an acceleration of conduct in the use of ICT that frequently shows *compulsive traits,* and is transferred to the subject's decisional sphere in terms of a greater confidence or relaxation in her interactions (naivety) and an absence of reflection in her decision-making processes (thoughtlessness). Such conduct brings us to affirm that cyber space, in fact, can have an effect on determining an individual's level of self-control. As such, the application of the principal theses of the self-control theory (Gottfredson & Hirschi, 1990) should receive greater attention in determining to what extent the greater risks of cyber-victimisation are due to a lack of self-control, applying the test of self-control to the victims and not the delinquents (the original subjects of that theory). To that respect, it is necessary to consult the important work on self-control and cyber-victimisation of Bossler and Holt (2010), who also highlight the necessity of a greater exploration of this hypothesis. Confirming it at least for certain groups of cyber victims would underline the importance of educating minors in the use of ICT, a factor of enormous relevance which surely deserves a primary place in cyber victimisation prevention strategies.

I cannot resist noting here the possibilities that Wikström's *situational action theory* (2006) could have in this context. Though this criminologist has not yet applied his theory to cyber delinquency, it would be interesting to adapt it to cyber space relative to the way in which the subject's moral perceptions interact with the cultural and situational surroundings. Think not only of the disinhibition effect, but also of the cultural and normative patterns, which certainly change from one society to another, for example in terms of copyright or data protection laws.

5. Prevention and Self-Protection Strategies for Cyber space Victims

I will now analyse the problems that I have been addressing from a prevention perspective. Criminological literature distinguishes 3 crime prevention focuses (for all three, see Tonry & Farrington, 1995) that logically can and should be adapted to cyber crime. For example, in relation to the strategies of *primary prevention* in cyber space, one could note different instruments and measures directed to strengthen or correct deficits in the population of ICT users as a whole, fomenting a greater education in internet use (Marcum, 2011), a greater consciousness of the dangers of pornography on the internet (Eberstatd & Layden, 2011), or a strengthening of the culture of privacy according to the current scenario.

From the point of view of *secondary prevention*, concrete policies for correcting prevention deficits in *concrete risk groups* should be designed, as much for offenders as for potential victims. To such an end, Wolak et al. (2004) have described identifying factors for certain populations vulnerable to sexual cyber-victimisation: (1) poor or conflictive relationships with parents; (2) loneliness and depression; (3) dubious sexual orientation as a predictor of risky behaviour; (4) the victims' unawareness of their own victimisation.

Finally, from a focus of *tertiary prevention,* specific treatment programs for online offenders and victims may be defined. Doubtless, some characteristics of offenders and victims may be common, but that does not diminish the necessity of a specific focus in function of the type of crime and victimisation. It is therefore reasonable to design specific treatment programs for paedophiles or education programs in cases of *sexting*. To such ends, in the United States specific instruments have already been designed and applied (see, among others, the program *Before you Text* cited in the References of this article). More could be said about programs directed towards victim recovery.

Along with the three preventive focuses above, over several decades different proposals and intervention measures specific to the environments in which crimes occur have emerged, which have received the name of *situational prevention techniques*. These are measures of diverse content and focus that arise from opportunity theory, and their main objective is to reduce the opportunity for crime by modifying environmental conditions. Through different versions of the standard catalogue of situational crime prevention (from now, SCP), Cornish and Clarke (2003) name 25 techniques of SCP that have been applied to concrete *criminal problems* and may therefore orient police work. A number of concrete guides to diagnose and intervene in concrete criminal phenomena can be found on the web page of the *Center for Problem-Oriented Policing*. Until now such techniques have principally been applied to non-virtual environments (Reyns, 2010). However, along with Reyns's work, specific instruments oriented to prevent cyber crime—such as *cyber stalking, cyber bullying, sexting, grooming,* and online child pornography—have begun to emerge (Wortley & Smallbone, 2012).

Table 1: Twenty-Five Techniques of Situational Crime Prevention from Cornish and Clarke (2003)

INCREASE THE EFFORT	**INCREASE THE RISKS**	**REDUCE THE REWARDS**	**REDUCE PROVOCATIONS**	**REMOVE EXCUSES**
Target harden	Extend guardianship	Conceal targets	Reduce frustrations and stress	Set rules
Control access to facilities	Assist natural surveillance	Remove targets	Avoid disputes	Post instructions
Screen exits	Reduce anonymity	Identify property	Reduce arousal and temptation	Alert conscience
Deflect offenders	Use place managers	Disrupt markets	Neutralise peer pressure	Assist compliance
Control tools/weapons	Strengthen formal surveillance	Deny benefits	Discourage imitations	Control drugs and alcohol

In this context, the work of Miró Llinares is especially remarkable. He presents a combination of concrete measures for cyber crime prevention from a situational focus (Miró Llinares, 2012, pp. 203-216). Elsewhere I will develop a wider commentary on this combination of measures—noted in the table below—while here only making a few brief observations.

Table 2: Twenty types of situational prevention measures for cyber-criminality from Miró Llinares (2012)

REDUCING ENVIRONMENT OF INCIDENCE	**INCREASING PERCIEVED EFFORT**	**INCREASING PERCEIVED RISK**	**REDUCING PERCEIVED REWARDS**	**ELIMINATING EXCUSES**
Don't introduce targets Separation of hard drives with and without access to system; Systems of parental control; Content filters; ActiveX security controls; No access to chat rooms *(grooming)*	**Control access to system** Firewall; Update operating systems; Passwords for system access; Passwords for access to web; Update passwords; Profiles on social networks	**Extend guardianship** Forum moderators; Echelon, Enfopol, Carnivore and Dark Web systems	**Hide targets** Use systems of encryption; Hide personal data on social networks; Don't use bank passwords; Perfect e-commerce systems	**Set rules** International legal harmonisation; "Netiquette"

Identify risk zones
Informational campaigns about risks;
Advise network of spam infections;
White and blacklists of web and spam;
Identify bots
	Detect and impede the attack
	Antivirus;
	Antispyware;
	Antispam;
	systems of control for electronic banking
		Reduce anonymity
		Identify IPs;
		Registration on web forums;
		User identification systems;
		Biometric identification and authentication
			Remove targets
			Removable hard drives;
			Alternative payment systems (PayPal);
			Change web addresses, domains and other
				Set rules
				Web licence notifications: copyright and 'copyleft';
				Privacy notifications on social networks

Decontamination/residue cleanup Erase and destroy latent viruses; Bot disinfection	**Deflect offenders** Close networks; Request removal of illicit content; Flagging mechanisms on social networks; Denial of access to specific IPs.	**Strengthen formal surveillance** Control networks through proxy; Specialized teams for cyber crime persecution	**Remove benefits** Persecution of buyers of illicit content; persecution of money laundering	**Strengthen moral conscience** Raise consciousness about intellectual property; Morally enforce legitimate businesses

Separatation of targets
Internet2;
Creation of local security sub-networks
	Control tools/weapons
	Obligatory vigilance through IPPPS;
	Control data through RSS
		Assist natural surveillance
		Improve IP identification systems;
		Reconstruct architecture with defensive ends
			Disrupt markets
			Offer economic systems of file sharing (Spotify and others);
			Control direct file download sites
				Assist compliance
				New business models (Apple);
				Legal hacker competitions;
				Strengthen open software

1) With regards to the first column, *Reducing the environment of incidence*, significant advances could be made by organising educational courses on the use of ICT, such as the interesting project ROBERT, or *Risktaking Online Behaviour Empowerment Through Research and Training*; or some educational programs that have been put in action in the US to respond to the phenomenon of *sexting*, such as the aforementioned Texas-designed *Sexting Prevention Educational Program for Texas 'Before you Text'* (both initiatives cited in the references).

In the context of raising consciousness about the risks of online lifestyles, we should call attention to the use of GPS location systems by social networks, by means of which an offender can follow a trail, for example on Facebook, of the places where a potential victim tends to be. Knowledge of these locations, along with the information that one puts online about friends, hobbies, interests, etc., can be used by different types of offenders, for example to know when a victim tends to be away from her house or in a specific place; or to give an appearance of truthfulness to an offender who wants to pass for someone the victim had met before, or someone having friends in common, giving confusing signals by means of all the personal information the victim published on her profile.

Finally, in relation to the supervision of minors using ICT, certain measures tend to reduce exposure. For example, one effective measure is for parents to pay their child's cell phone bill. *Trend Micro*, a company dedicated to secure content on the internet, advises this, citing a study conducted by *Pew Research Center*, the results of which indicate that 7% of adolescents who pay their own bill send *sexts*, as opposed to 3% of those who don't pay their own expenses (or only a part). Another measure proposed by *Trend Micro* for parents with children between the ages of 12 and 17 is to limit the number of text messages the child can send. The study indicates that only 8% of adolescents that practice *sexting* have a restricted number of text and other messages, while 28% of those who do not practice *sexting* have such limited number of messages.

Another measure along the same lines is to cover or disable webcams on home computers; or to give adolescents mobile phones that, without being relatively unattractive, do not have an incorporated camera.

2) In relation to measures aimed towards *increasing the perceived effort* and *increasing the perceived risks*, a question with special legal implications must be highlighted, viz., the use of police as *undercover agents* and *provocative agents*. Increasing the number of *capable guardians*—especially if they possess technical and criminological knowledge—could increase the perceived risk for potential offenders and, *ex post facto*, increase the success of police operations—even if, as we shall see, occasionally police do not intervene after the crime, but in its very generation, in order to finalise or secure a course of investigation, or through fishing expeditions.[6]

Currently in Spain, as opposed to the United States, the use of *undercover agents* against child pornography and paedophilia does not enjoy the necessary legal coverage. Under Spanish legislation (art. 282 bis of the Criminal Procedure Act), undercover agents are only allowed, by means of judicial authorisation, to investigate "activities of organised crime". In addition, the same article defines "organised crime" as the association of three or more people organised in a permanent or repeated fashion to commit one of the crimes therein enumerated. In that enumeration, the crime of pederasty or grooming (art. 183 bis of the Penal Code) is not directly contemplated. If the case were to arise, it could only be included indirectly through the crime of kidnapping or prostitution and corruption of minors—as long as there is "organised crime" as defined above.

On the other hand, the *provocative agent* who provokes a crime for the sole reason of verifying its actual committal is for now an illegal figure in Spain. His/Her acts could constitute a crime for which the agent could be condemned as abettor, or on grounds of a preparatory act of propositioning or provoking a particular crime.

[6] Since 1993, in the United States 83 islamist attempts have been aborted, according to the calculations of Martha Crenshaw, a terrorism expert from Stanford University, with up to 79 of those due to the actions of *provocative* FBI agents ("El enemigo está entre nosotros" — "The enemy is among us" —, *La Vanguardia*, 2nd June 2013, p. 3).

The police agent who uses the internet with the sole goal of proving the existence of crimes, without ever coming to provoke them, is the only current legal figure in Spain. The proposals processed by the Senate to modify the Criminal Procedure Law and the Penal Code, in order to create new legal figures to fight sexual exploitation of minors, have been so far unsuccessful. Finally, in the frame of police action in cyber space, novel questions are posed about the legal limits of using Facebook and other social networks as a means of investigating criminal activity, prospectively or retrospectively (Nieto Martín & Maroto Calatayud, 2013, p. 430).

3) In terms of methods to e*liminate excuses*, a significant mention is merited by the *effective* adoption of ICT use policies by public and private businesses and organisations. Elsewhere I have analysed how to prevent abusive conduct and technological crimes in companies (Agustina, 2013). By means of an interdisciplinary study of ICT use policies and the prevention and management of 'conflicts' in a sample of Spanish companies, we verified that many companies, despite having designed and communicated an ICT use policy, had not operationally implemented the approved policies or did not complete a deep analysis of the risks of new technologies. Together with a questionnaire addressed to the companies' directors, we created a second survey-simulation directed towards those in charge of information services, which revealed a significant lack of technical capacity to detect and identify offenders.

It is therefore not enough to approve and communicate a policy for the use and control of ICT—suitable instruments for ensuring compliance must also be provided. Thus, to enforce an adequate corporate strategy of cyber crime prevention, not only formal and legal aspects must be taken into account (relative to controlling workers and the possible effects on the right to privacy). Above all, opportune technical instruments must be established, together with training for those in charge of technical services and action protocols enabling to effectively prevent, control and react to eventual crimes.

6. Some Paradoxes: Offenders' Profile versus Not-So-Naive Victims

Given all that has been discussed thus far, what profiles are exhibited by cyber-criminals? Can certain common patterns be identified? According to Miró Llinares (2012, p. 229), a hacker is not equivalent to a cyber criminal, given the diversity of criminal typologies, motives and, therefore, criminological profiles. For this reason, we must distinguish between economic, social and political cyber criminality.

The terrain of offenders' profiles lends itself to distorted images of reality, stereotypes that must be demystified. Criminological investigation must provide us with a faithful picture based upon empirical data, which may reveal certain paradoxes. One example of a paradox is the online sexual predators' profiles provided by Wolak et al. in their study (2004):[7] (1) they are not paedophiles (99% of the sample interacted with victims between

[7] Another example in which the construction of a myth, in this case clearly by the mass media, appears to distance us from reality is that of terrorists with no apparent connection to any organised structure, called 'lone wolves'. In fact, by studying the mechanisms leading to situations like the recent terrorist actions in Toulouse, Boston or London, anti-terrorist specialists conclude that the term 'lone' does not correctly reflect reality. In the absence of external connections, the internet is an important tool in which, by means of a very effective propaganda network of *jihadists*, this 'wolf' finds his reason to be and, most importantly, no longer feels alone ("Lobos puede; solitarios, no tanto" —

13 and 17 years); (2) although they use certain forms of manipulation, they do not deceive or hide their intentions towards their victims, who are adults interested in having sexual relations (the victims knew the intentions of the offenders before their first offline encounters); (3) the majority did not use force or coercion to perpetrate sexual abuse, nor did they detain or kidnap the victims (who acted with consent, sometimes on multiple occasions); and, finally, (4) it is misleading to characterise the offenders as 'strangers' to the victims: in the majority of cases they had communicated extensively before the first encounter.

The study referenced above has important implications for prevention strategies and poses important questions about the victims' profiles, at least in the type of crimes mentioned here. Previously I mentioned the deficits presented by victims in this particular risk group. But we must recognize that, in reality, we are not up (only) against *sexual predators* in search of naive victims. On the contrary, and to be more exact, sexual abuses only occur *if the victim wants it*; that is to say, sooner or later the victim 'accepts', although in certain circumstances a *psychopathological symbiosis* is developed. In evaluating the dimension of the problem, it is difficult to know the true number of solicitations, approaches, failed ruses or rejected attempts that occur on the internet; and this dark figure—owing in large part to the lack of 'victimisation' surveys and the lack of consciousness of one's own victimisation—makes it enormously difficult to understand the problem's true nature.

If, as it appears, some victims 'want it', such slogans as "don't accept messages from strangers" will not be effective. This poses questions about how to prevent this type of victimisation, showing the need for a greater understanding of the why's of consent, surrender and active pursuit (despite eventual defects of consent) by victims.

In reality, victims are not so naïve, nor are their resolution unconditional, nor are offenders so completely sincere; *the circumstances matter*. Staging and deceit continue to exist, and therefore it is useful to recognise the different types of *modus operandi*. It is not enough to concentrate on correcting the *unhealthy attitude* of adolescents; surroundings are important.

Conclusion

I will conclude with some final reflections, divided into two perspectives of analysis: the *prevention strategies perspective* (based on the victimological analysis presented here) and the *anthropological perspective* (relative to human nature changes introduced by digital age).

I have analysed different aspects of cyber victimisation from the criminological/victimological point of view, with the aim of improving the victims' protection from a *prevention strategies perspective* (*ex ante* analysis). Using Katyal's metaphor, *the internet continues to be a dark place* in which we need to shed more light and create order. In the physical world, the desire for safety in our streets and neighbourhoods has translated into all sorts of measures: from the architectural design of public space, police patrols and the creation of community ties within the neighbourhood, to cautions taken by pedestrians themselves, who know where and at what hours it is better not to transit. *Mutatis mutandis*, cyber space is a space of transit that essentially follows similar rules,

"Maybe wolves, but not so alone" —, E. Martín de Pozuelo, *La Vanguardia*, 24 May 2013, p. 4). Also see Cano Paños (2013).

despite greater conditions of anonymity and a greater chance of contact with strangers. In this sense, transiting through cyber space without taking the necessary precautions would be, in a way, like walking down a busy street exposed to everyone, naked or scantily clad, or showing off valuable jewels. The lack of awareness of ICT users logically increases the risk of victimisation; their careless conduct can unexpectedly attract the attention of innumerable invisible observers who are anonymously seeking an attractive target. Such naïveté—*there's a sucker born every minute,* in Barnum's words—should make us *reflect* and stop the uninhibited or *thoughtless* way in which we carry out our daily activities in cyber space, and to adopt instead the maxim *don't do in the virtual world what you wouldn't do in the real one*. This opens many questions for investigation. Among others, an especially relevant one would be: what correlations are there between the personal, social and virtual contexts, and the disinhibited attitudes of individuals in their routine and non-routine activities?

With respect to the *anthropological perspective,* the digital era has led to transcendent changes not only in people's everyday lives, but also in their very ways of being and thinking. Given this sociological fact, I have tried to anchor the changes suffered in human nature and their innate vulnerability in the context of their surroundings. In ancient Greece, the celebrated philosophical debate between Heracles and Parmenides about the hypothesis of *universal flow between beings*—"panta rei" (*πάντα ρεῖ*): everything flows—manifested that, although *a man cannot bathe twice in the same river* (the river and the man being different the second time), man does not lose his essential attributes despite the flow of changes. There is an essential part of human nature that resists historic and cultural changes, and also technological ones, despite the fact that those changes enormously affect relational conditions, lifestyles and, to our interest, the opportunities for victimisation. Our diagnosis could be summarised stating that the defragmenting tendencies in people's lives, due to the digital age, considerably elevate the risks of victimisation. As such, without ignoring the positive advances of the digital age and the widespread use of ICT and the internet, we must begin the *search for the lost identity* to avoid the defragmentation of the self. This is a challenge with enormous anthropological implications in the formation of the new generations of digital natives.

References

Agustina, J. R. (2009). Arquitectura digital de Internet como factor criminógeno: Estrategias de prevención frente a la delincuencia virtual. *International E-Journal of Criminal Sciences*, num. 3 (2009).

Agustina, J. R. (2012). Analyzing Sexting from a Criminological Perspective. Beyond Child Pornography Issues: Sexting as a Threshold for Victimization. In Pauline C. Reich (Eds.), *Cybercrime & Security*, West, Thomson Reuters, Section 4:4, 64-96.

Agustina, J. R. (2013). ¿Cómo prevenir conductas abusivas y delitos tecnológicos en la empresa? Estudio interdisciplinar sobre políticas de uso de las TIC, prevención y gestión de "conflictos" en una muestra de empresas españolas. IDP. *Revista de Internet, Derecho y Política* (in press).

Antón Oneca, J. (1958). Term "Estafa" in *Nueva Enciclopedia jurídica*, Calos-E. Mascareñas (dir.), Tomo IX, Barcelona, Editorial Francisco Seix.

Bossler, A. M. & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice, 38*, 227–236.

Brantingham P. & Brantingham P. (1995). Criminality of place: Crime generators and crime attractors. *European Journal on Criminal Policy and Research, 3*(3), 5–26.

Cano Paños, M. A. (2013). El caso "Mohammed Merah" en el contexto actual del terrorismo islamista. *Revista Electrónica de Ciencia Penal y Criminología* RECPC 15-02 (2013).

Castells, M. (1997). La era de la información: Fin de milenio. Vol. 3. Madrid: Alianza.

Choclán Montalvo, J. A. (2006). Infracciones patrimoniales en los procesos de transferencia de datos. In C.M. Romeo Casabona (coord.) *El cibercrimen. Nuevos retos jurídico-penales, nuevas respuestas político-criminales*. Granada: Ed. Comares.

Choi, K. (2008). Computer Crime, Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology*, *2*(1), 308-333.

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

Cornish, D., & Clarke, R.V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. In: M. J. Smith and D. Cornish (eds.) *Theory for Practice in Situational Crime Prevention (pp.* 41–96), Vol. 16. Monsey, NY: Criminal Justice Press.

Díaz Cortés, L.M. (2012). Aproximación criminológica y político criminal del contacto TICspreordenado a la actividad sexual con menores en el Código penal español-art. 183 bis CP. *Revista De Derecho Penal y Criminología*, 3^rd^Period, num. 8 (July 2012), 289-318.

Eberstatd, M. y Layden, M.A., Witherspoon Institute (ed.) (2011).Los costes sociales de la pornografía. Una exposición de hallazgos y recomendaciones, in *La pornografía y sus efectos sociales y criminógenos. Una aproximación multidisciplinar*, J.R. Agustina (dir.), Social TrendsInstitute (ed.), Colección Actualidad Criminológica y Penal, BdeF–Edisofer.

Ebert, "VerbrechensbekämpfungdurchOpferbestrafung?", *Juristenzeitung (JZ)* 1983, 633-643.

Etzioni, A. (2012). *Los límites de la privacidad* (trans. A. López Lobo y J.R. Agustina). Montevideo, Uruguay: BdeF.

Felson, M. (1994). *Crime and Everyday Life* (1st ed.). Thousand Oaks, CA: Pine Forge Press.

Felson, M. (1997).Technology, Business and Crime. In Felson, M. & Clarke, R.V. (ed.), *Business and Crime Prevention*, Monsey, NT: Willow Tree Press, 81–96.

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

Gordon, M. P., Loef, M. P., Lucyshyn, W., & Richardson, R. (2004). *CSI/FBI computer crime and security survey*. Los Angeles: Computer Security Institute.

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

Grabosky, P. (2001). Virtual Criminality: Old Wine in New Bottles? *Social & Legal Studies 10*, 243–9.

Grabosky, P., & Smith, R. (2001). Telecommunication fraud in the digital age: The convergence of technologies. In D. Wall (Ed.) *Crime and the Internet (pp.* 23-45). London: Routledge.

Green, S.P. (2013). *Mentir, hacer trampas y apropiarse de lo ajeno. Una teoría moral de los delitos de cuello blanco* (trans. JR. Agustina, M. Amorós e I. Ortiz de Urbina). Madrid: Marcial Pons.

Herrero Moreno, M. (1996). *La hora de la víctima. Compendio de Victimología*. Publicaciones del Instituto de Criminología de la Universidad Complutense. Madrid: Edersa.

Herrero Moreno, M. (2006). Victimización: aspectosgenerales. In E. Baca, E. Echeburúa y J.M. Tamarit (coords.), *Manual de Victimología*, Valencia: Tirant lo Blanch, 79-128.

Hindelang, M., Gottfredson, M. & Garofalo, J. (1978). *Victims of Personal Crime: an Empirical Foundation for a Theory of Personal Victimization*. Cambridge MA: Ballinger.

Hurd, H. M. (2005). Blaming the Victim: A Response to the Proposal that Criminal Law Recognize a General Defense of Contributory Responsibility, 8 *Buff. Crim. L. Rev.* 504, 5.

Jaishankar, K. (2008). Space transition theory of cyber crimes. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283–301). Upper Saddle River, NJ: Prentice Hall.

Katyal, N.K. (2003). Digital Architecture as Crime Control, 111 *Yale Law Journal* 1039.

Lenhart, A. (2009). *Teens and Sexting. How and why minor teens are sending sexually suggestive* nude *or nearly nude images via text messaging*. Pew Internet & American Life Project. Washington: Pew Research Center.

Lessig, L. (1999). *Code and Other Laws of Cyber space*. NY: Basic Books.

Marcum, C. D. (2011). Adolescent Online Victimization and Constructs of Routine Activities Theory. In Jaishankar, K (Ed.), *Cyber Criminology*: *Exploring internet crimes and criminal behavior* (pp. 253-276). Boca Raton: CRC Press.

Mendelsohn, B. (1956). The Victimology. In *Etudes Internationales de Psycho-Sociologie Criminelle* 1 (1956).

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, num. 13-07.

Miró Llinares, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid, Marcial Pons.

Miró Llinares, F. (2013). La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del phishing. *Revista Electrónica de Ciencia Penal y Criminología* (in press).

Ngo, F. & Paternoster, R. (2011). Cyber crime Victimization: An Examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773-793.

Nieto Martín, A. & Maroto Calatayud, M. (2013). Las redes sociales en Internet como instrumento de control penal: tendencias y límites. In A. Rallo Lombarte y R. Martínez Martínez (eds.), Derecho y redes sociales (2ª ed.). Pamplona: Civitas, 427-484.

Ogburn, W. F. (1964). *On Culture and Social Change: Selected Papers* (Ed. Otis Dudley Duncan). Chicago: University of Chicago Press.

Palfrey, J. & Gasser, U. (2008). *Born Digital: Understanding the First Generation of Digital Natives*. New York: Basic Books.

Pereda, N., Abad, J. & Guilera, G. (in press). Victimización de menores a través de internet: descripción y características de las víctimas de online grooming, in *Delito, Pena, Política Criminal y Tecnologías de la Información y la Comunicación en las modernas Ciencias Penales*. Ediciones Universidad de Salamanca, Salamanca.

Puppe, I. (1995). In Neumann/Schild (Gesamtred.), *Nomos Kommentarzum Strafgesetzbuch*, Band 2, BesondererTeil, Baden-Baden num. marg. 4, cited in Silva Sánchez (1999) op. cit.

Quayle, E., Jonsson, L., & Lööf, L. (2012). *Online behaviour related to child sexual abuse: Interviews with affected young people*. Council of the Baltic Sea States, Stockholm: ROBERT project.

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*, 99-118.

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

Reyns, B. W., Burek, M. W., Henson, B., & Fisher, B. S. (2011b). The unintended consequences of digital technology: exploring the relationship between sexting and cyber-victimisation. *Journal of Crime and Justice*, 1–17.

Schafer, S. (1977). *Victimology: The Victim and His Criminal*. Reston, Va: Reston Pub. Co.

Silva Sánchez, J.M. (1989) Consideraciones victimológicas en la teoría jurídica del delito? Introducción al debate sobre la victimodogmática, in *Criminología y derecho penal al servicio de la persona: libro homenaje al profesor Antonio Beristain*, (coord. by Enrique Echeburúa Odriozola, José Luis de la Cuesta Arzamendi, Iñaki Dendaluce Segurola), 633-646.

Standler, B.R. (2002). *Computer crime*. Retrieved on 12th October 2014 from http://www.rbs2.com/ccrime.htm.

Tapscott, D. (2008). *Grown Up Digital: How the Net Generation is Changing Your World*. McGraw-Hill.

Tonry, M., Farrington, D. P. (1995). *Strategic Approaches to Crime Prevention*. 19 Crime & Justice 1.

Valkenburg, P. M & Peter, J. (2011). Online communication among adolescents: An integrated model on its attraction, opportunities, and risks. *Journal of Adolescent Health*, *48*, 121-127.

Villacampa Estiarte, C. (2010). La respuesta jurídico-penal frente al stalking en España: presente y futuro. *ReCRIM:* Revista *de l'InstitutUniversitarid'Investigació en Criminologia i CiènciesPenals de la UV*, *4*, 33-57.

Wikström, P.-O. (2006). Individuals, settings, and acts of crime: situational mechanisms and the explanation of crime. In P.-O. H. Wikström y R.J. Sampson, *The Explanation of Crime*. Cambridge: Cambridge University Press.

Wolak, J., Finkelhor, D., & Mitchell, K.J. (2004). Internet-initiated sex crimes against minors: Implications for prevention based on findings from a national study. *Journal of Adolescent Health*, *35*, 424.e11– 424.e20.

Wolak, J., Finkelhor, D., Mitchell, K. J. & Ybarra, M. L. (2008), 'Online "predators" and their victims'. *American Psychologist*, *63*(7) 111-126.

Wortley, R. & Smallbone, S. (2012). *Internet Child Pornography: Causes, Investigation, and Prevention*. Praeger: California, Colorado, England.

Yar, M. (2005). The novelty of 'cyber crime': An assessment in light of routine activity theory. *European Journal of Criminology*, *2*, 407-427.