The Global Causes of Cybercrime and State Responsibilities. Towards an Integrated Interdisciplinary Theory

Lorenzo Pasculli

Coventry Law School,
Centre for Financial and Corporate Integrity,
Coventry University
University of Nebrija, Madrid
lorenzo.pasculli@coventry.ac.uk

Abstract: Information and communication technologies provide immediate means, motivations and opportunities for cybercrime. However, deeper cultural, social and psychological developments triggered by globalisation are the root causes of such motivations and opportunities. Successful strategies to prevent cybercrime cannot focus only on technological or infrastructural defences but must address these global developments. While scientific understanding and political awareness of such causes are still limited, studies from different disciplines, including sociology, criminology and psychology, allow to detect some global criminogenic patterns and to identify the state responsibilities of national governments for failing to address them adequately. This article integrates the findings of these studies to provide a preliminary interdisciplinary theory of the global causes of cybercrime and assess what national governments can do to mitigate them.

Keywords: *cybercrime, cybersecurity, global crime, globalization, crime prevention, anomie, hacking community, terrorism, extremism, hate crime*

1. Introduction

Cybercrimes are defined by the use of information and communication technology (ICT). One popular definition divides them into (1) crimes where a computer is a target, (2) crimes where a computer is a tool, (3) crimes where a computer plays an incidental role (Goodman 1997, 468-469; Broadhurst 2006, 413; Casey 2011, xxiv-xxv; Brenner 2012, 13). An even more effective definition (McGuire and Dowling 2013, 5; HM Government 2016, 17) distinguishes *cyber-dependent crimes*, which can only be committed through the use of ICT devices – such as developing and spreading malware – from *cyber-enabled crimes*, which are traditional crimes that can be increased in scale or reach by the use of ICT – such as computer fraud, data theft or sexual offending. The constitutive or transformational (Wall 2007) role of ICT might easily divert the focus of researchers and policymakers from the social and psychological causes of cybercrime. These are, of course, difficult to study, rooted as they are in the most complex human (cultural, socio-psychological, political, economic) developments of globalisation and their local variations. And they might be perceived as difficult to tackle, since they are often out of the direct control of individual nation-states. At a policy level, these difficulties might translate into reductive conceptions of cybercrime and cybersecurity, whereby cybercrime is perceived as an evil to be fought, and security is conceived as stronger technological defences and infrastructures, rather than adequate societal conditions to enable the individual to thrive without having to resort to crime. This seems to be the case, for instance, of the United Kingdom's (UK) National Cyber Security Strategy 2016-2021 (HM Government 2016), which is mostly focused on infrastructural and technological measures. Disabling technological means and opportunities is necessary, but not sufficient. Any effective preventive strategy should aim at removing or at least mitigating all the possible causes of crime, including those rooted in global developments. Without a clear understanding of these and a coherent plan to address them, any defensive action at a national level becomes an "exercise in shooting in the dark" that may produce adverse side effects (cf. Passas 2000, 16). In the recent years, many jurisdictions, including the EU, the US, the UK, Italy, France, Germany, Spain, the Netherlands, Finland, Estonia, Lithuania, Slovakia, Czech Republic, Luxembourg, India, and Japan, have adopted cybersecurity strategies. More are likely to follow. There is, therefore, an urgent need to improve our understanding of the causes of cybercrime to assess and, if necessary, reform existing strategies and design new ones.

Converging findings from different disciplines, including sociology, criminology and psychology, allow to identify at least some of such causes.

This article draws upon such literature to trace a preliminary interdisciplinary theoretical framework on the causes of cybercrime which can be useful for local governments to assess their policies and/or develop new ones. Hopefully, our analysis will contribute to the understanding of the causes of global crime at large, of which cybercrime is a paradigmatic expression. The article also aims to trigger further discussion on the need to adopt a more holistic interdisciplinary perspective on the causes of cybercrime (and crime in general). In the next paragraph, we will outline the methodology and limitations of our research. The third paragraph will review relevant interdisciplinary literature on cybercrime, global crime and globalisation to identify the main global causes of cybercrime. The fourth paragraph will critically discuss such findings and propose policy recommendations for States. In the final paragraph, we will draw our conclusions.

2. Methodology and limitations

The causes of crime have been studied from the most different disciplinary angles, yet they are still a source of lively debates – even more so when it comes to unprecedented forms of global criminality. The difficulty of finding a conclusive general theory, however, is more revealing than discouraging. The variety of explanatory frameworks speaks loudly of one fundamental character of the problem: its complexity. The causes of crime – especially of global crime – are multiple, diverse and mutually interdependent. This is the inevitable consequence of crime being a human behaviour, as such resulting from an innumerable, ever-changing and often unpredictable series of psychological, social, environmental and even biological conditions. Attempts to provide unilateral (monodisciplinary) explanations of crime are bound to fail. Simplification and intuition are deceiving and dangerous, as they can lead to offender stigmatisation and unreasonable policymaking. The only way to build a sensible understanding of the causes of crime is through an integrated dialogue between different disciplines. The approach of this article will be, therefore, as interdisciplinary as possible. The well-consolidated criminological distinction between criminal motivations and opportunities will provide the spine of our theoretical framework. The further distinction between remote and proximate causes of global crime, which we articulated in previous studies (Pasculli 2020; Pasculli and Ryder 2020), will add structure to it. This framework will be then integrated with converging and mutually complementary social and psychological findings on globalisation – such as anomie and strain theories, Bauman's or Gidden's analysis of modernity and the findings of the emerging social psychology of

globalisation – and on more specific aspects or forms of cybercrime – such as Holt's, Steinmetz's and Rogers's studies on the hacking subculture.

Our analysis presents inevitable limitations. The nature and economy of this work do not allow to address *all* the causes of cybercrime. Instead, we will focus on some of the most significant social and psychological developments of globalisation. Criminogenic factors concerning the individual or specific national contexts are beyond the scope of our analysis. On the other hand, our interest is to assess what national governments can do to mitigate some of the global causes of cybercrime. Therefore, our recommendations will be limited to national policies, excluding international action. Nor could we even attempt to cite *all* the literature on the many issues related to cybercrime and globalisation that we are going to deal with. Instead, we will base our analysis on well-established and largely agreed theories or other emerging and convincing theories, possibly based on empirical findings. The paper remains largely speculative in nature and, as such, it's open to criticism, integration and further development. In particular, more empirical research would be required to confirm (or disprove) some of our theoretical and policy suggestions.

3. The global causes of cybercrime

If global crime is any crime which is globalised in its causes, means, forms of perpetration, and/or effects (Pasculli 2015), then cybercrime is a paradigmatic manifestation of it, as its causes, means, forms of perpetration and effects are deeply rooted in the developments of globalisation (cf., for instance, UNODC 2013, 5; Grabosky 2001, 243 and 247; Loeb 2004a and 2004b; Pocar 2004, 28). Information technology is one of these developments, but it is neither the only nor necessarily the most significant one, as we shall see. Before we go any further, let us set out our theoretical framework on the causes of global crime.

There are two main categories of causes of global and cybercrime: *proximate* causes and *remote* ones. *Proximate* causes are personal and situational factors that influence directly individual behaviour. These include motivations and opportunities (cf. Cantor and Land 1985; Coleman 1987 and 1992; Grabosky 2001; Broadhurst 2006; Clarke 2008; Kigerl 2011). Motivations are symbolic constructions that define certain goals and activities as desirable (Coleman 1987, 409). Opportunities are situations, such as access to suitable targets, availability of means or the absence of effective controls (cf., for instance, Grabosky 2001, 248; Cohen and Felson 1979, 588-608), that make certain behaviours possible (Coleman 1992, 828) or more tempting (Clarke 2008, 179). *Remote* causes are the deeper cultural, socio-psychological, economic,

and politico-institutional developments – as such, largely independent from individual choices or particularly circumscribed contexts – that determine or aggravate individual motivations and situational opportunities for crime. The boundaries between proximate and remote causes are blurred, as remote causes often develop into proximate ones. In the following paragraphs, we will provide an overview of some of the most significant remote social and psychological causes of global crime and cybercrime as identified by existing literature. For each of these causes, we will address the transversal role of technology in enabling or amplifying criminogenic effects.

3.1. Global anomie, strains and cybercrime

One of the most powerful theoretical frameworks to explain crime is the anomie theory. Anomie ("normlessness") is the situation in which society fails to regulate the naturally unlimited desires of individuals. According to Durkheim, this state is typical of periods of great change, when society cannot instantaneously adjust individual passions to new (better or worse) standards of living (Durkheim 1897, 213). Anomie has become chronic in business and trade with industrial development and the "almost infinite" extension of the market (*ibid.*, 216). The commitment of every nation, irrespective of the economic model adopted, to industrial prosperity and the consequent subordination of the state to economic life have liberated human desires of any restraining regulation and fostered unlimited greed (*ibid.*). Merton has argued that unrealistic goals are not necessarily biological, but can be the result of social and cultural pressures. This happens when there is an unbalance between culturally-induced goals of success and the institutional means to achieve them. When there is an excessive cultural emphasis on wealth, power, status etc., but legitimate and effective means of attaining them are not available, individuals might turn to prohibited but effective means. Anti-social behaviour is, thus, induced by the class structure that prevents equal access to lawful opportunities for pursuing conventional cultural goals (Merton 1938 and 1968). Durkheim's anomie refers to the normlessness of the goals, Merton's refers to the normlessness of the means (Agnew 1997, 37). Messner and Rosenfeld have pointed out that removing structural obstacles to legitimate opportunities is not enough to reduce crime rates when all the major social institutions primarily support the quest for material success and fail to promote alternative definitions of self-worth and achievement (Messner and Rosenfeld 1997 and 2013; Chamlin and Cochran 1995). In other words, the cultural goals must be questioned, together with the adequacy of the means (Orrù 1987; Bernburg 2002).

Anomie theory is gradually expanding beyond its original sociological focus. Robert Agnew has moved the analysis from the macro-level of the social system to the socio-psychological level of the individual and their immediate environment. Expanding Merton's theory and drawing upon works by Albert Cohen (1955 and 1965) and Cloward and Ohlin (1960), Agnew developed a general strain theory of crime, whereby delinquency would depend upon the strain resulting not only from the failure to achieve positively valued goals but also from the inability to escape legally from painful situations (Agnew 1990, 1997 and 2005). A recent study by Teymoori, Bastian and Jetten (2017) has initiated a psychological analysis of anomie. Most importantly, anomie theory has progressively shifted from a nation-centred perspective – well exemplified by Merton's and Messner and Rosenfeld's focus on the American Dream – to a cross-national one. Recent empirical studies on large samples of different nations have investigated several aspects of anomie theory, such as the effects of social structure (Schaible and Altheimer 2015), rapid societal change (Zhao and Cao 2010), formalised social controls (Swader 2017), or even globalisation itself (Levchak 2015). Anomie theory or its derivatives are also being used to explain typical forms of globalised crime such as transnational financial and corporate crime (Passas 1990 and 2000), terrorism (Agnew 2010), refugee criminality (Simmler, Plassard, Schär and Schuster 2017), and online piracy (Larsson, Svensson and de Kaminski 2012). Passas (2000) observes that the structural problems typical of anomie are being reproduced throughout the world through globalism and neoliberalism. Like the American Dream, global neoliberalism fails to deliver its promises. Global interconnectedness and neoliberal discourses of economic growth, free markets, individualism, consumerism, privatisation and deregulation have created new needs, desires and fashions. International and national institutions, however, fail to provide equal legal means to pursue such goals of welfare (cf. Stiglitz 2002 and 2012). Instead, structural "asymmetries" (Passas 2000, 17-18) in economy, law, politics and culture aggravate the divergence between means and ends, which produces a sense of deprivation and frustration in those who fail to achieve the globally valued goals of success. Such strains can induce deviance of various types, particularly in the presence of criminal motives and opportunities (*ibid.*, 18). The combination of the anomic state (*remote* cause) and individual and situational criminogenic factors (*proximate* causes) produces global crime.

Two *caveats*. First, acknowledging inequality and insufficiency of means to achieve culturally valued goals as a cause of globalised forms of criminality does not imply that poverty, as such, is a cause of global crime. In fact, societies affected by poverty, characterised by a very rigid social structure

(Merton 1938, 680) and less materialistic goals (Passas 2000, 26), are more immune from the criminogenic effects of anomie, than those who are better off. Durkheim explains very clearly that poverty is a restraint in itself, for desires depend on resources: "The less one has the less he is tempted to extend the range of his needs indefinitely" (Durkheim 1897, 214). It is those who do have access to material opportunities that are easily pressured into achieving more and more. The expansion of economic opportunities reinforces the emphasis of goals of material success and provide new means to achieve them illegally. Other than financial crime, cybercrime is a paradigmatic example of this. Cybercriminals are rarely poor and uneducated, as cybercrime requires access to ICT and advanced skills (Neufeld 2010, 5). Moreover, access to the Internet increases exposure to relentless cultural pressures of consumerism, competition, and individualism. Second, the anomic strains triggered by globalisation do not explain only financially-motivated crime but can instigate other forms of criminality (Levchak 2015). This applies also to cybercrime. Although many cybercrimes are moved by monetary gain, or business benefits (Holt and Kilger 2012, 802) – empirical research suggests that the second most common motivation for computer crimes is revenge (Neufeld 2010). Shaw's review of empirical evidence on insider computer attacks reveals that "disgruntled" offenders are generally undergoing significant personal and professional strains. Pre-existing individual vulnerabilities can determine maladaptive behavioural and emotional reactions to such strains, but management failures to address the issue properly can escalate the process leading to offending (Shaw 2006, 25). Shaw cites the example of a young help desk worker with significant frustrations caused by a long history of difficult international moves caused by family financial stresses, the divorce of his parents, and the struggle to complete his training. His frustrations in the workplace began to mount rapidly when he felt he did not receive the recognition he was entitled to. He did not voice this to management, and his inconsistencies at work led to his being placed on probation before committing a cyberattack. In a lengthy memorandum, he wrote that managers must learn to handle hackers in the work environment differently than regular employees, indicating that he felt entitled to special treatment (*ibid.*). This research suggests once again that the emphasis on personal success is often neither compensated by an equal emphasis on alternative goals of self-worth and acceptable ways to achieve them, nor supported by effective legitimate means and opportunities to pursue it – such as financial and family stability, support and recognition at work, but also social and psychological support to deal with personal frustrations and vulnerabilities. This can expose the individual to various strains, which, in turn, can generate criminal behaviours, not necessarily

motivated by the will to achieve the goals illegally, but also by the anger and frustration deriving from negative stimuli (or the removal of positive ones), as suggested by Agnew (2010).

What is the role of ICT in all this? ICT magnifies global anomie, corroborates the individual strains and motivations that derive from it and provides new criminal opportunities. The global reach of communications facilitates the worldwide circulation of consumerist goals and unrealistic aspirations of material success and prestige. At the same time, cyberspace dilutes social and legal norms that regulate individual desires and the means to satisfy them. Social norms are weakened in the global virtual reality of the Internet, which disconnects people from their local communities and estrange them from each other (Passas 2000, 25; Giddens 1990, 21). The virtual nature of cyberspace also makes effective legal regulation difficult, both at a national and at an international level (Rowland 1998). All this can incite individual criminal *motivations*. Moreover, ICT offers effective illegal *means* and *opportunities* to pursue globally valued goals of success, when socially acceptable and institutionalised ones are missing. The digital avenues to do so are many, inexpensive and readily available: online file-sharing systems, peer-to-peer software, disruptive malware, fraudulent emails and websites, underground virtual marketplaces, as was Silk Road (Phelps and Watt 2014) etc. The anonymity of such instruments and the availability of encrypting tools to cover illegal activities, such as file sharing (Larsson, Svensson and de Kaminski 2012), further encourage criminal motivations and opportunities by making detection more difficult.

3.2. Anxiety, fear, hate and terror

The global era is an era of irrationalisation and "*insécurisation*" (Mathieu 1995) – or "uncertainization" (Bauman 1997, 203). The post-war individual, overwhelmed by the experience of the atrocities of war and totalitarianism and fulfilled with feelings of alienation, anxiety, "nothingness" and absurd, was invested by an existential crisis widely investigated by philosophy and psychology, and expressed by literature and arts (Pasculli 2015). These feelings have gradually eroded the trust on the power of human reason to order and regulate social life which had characterised the centuries following the Enlightenment. Irrational, instinctive or emotional perceptions of reality foster a sense of insecurity even in societies which, as Castel (2003, 5) and Bauman (2006, 129) observe, are the most secure in the history of humanity. Globalisation has aggravated this crisis. Global mobility and interconnectedness have brought together people from the most different cultures rather suddenly and without any cultural preparation to contact

with diversity and the emerging global culture. Fear, mistrust and suspicion towards the diverse grow out of post-war insecurity and irrationality and individuals withdraw into localism and traditional values – often the product of nostalgic misconceptions. The rapidity of change and the increasing subordination of individual to organisations are other reasons for psychological discontent, as Bertrand Russell observed back in 1949. Changes – also in technology – happen too quickly for individuals (Russell 1949, 1310) and societies (Durkheim 1897, 213) to be able to adjust properly. The rising power of impersonal global forces, such as financial markets or multinational corporations, worsens the sense of impotence of the individual. The nation-states' physiological incapability of governing global phenomena furthers the perception that no one is in control (Bauman 1998) and nurtures mistrust and anger. The recent waves of populism and nationalism are manifestations of all this. The openness of societies becomes "the terrifying experience of heteronomous, vulnerable populations overwhelmed by forces they neither control nor truly understand" (Bauman 2006, 96).

Both hate crimes and international terrorism seem to be rooted in intergroup conflicts (Mills, Freilich and Chermak 2017, 1197) caused or deepened by globalisation and the failure of states to adequately support and prepare their citizens to its sudden and revolutionary changes. Research in the emerging field of the social psychology of globalisation suggests that emotional and reflexive responses to intercultural contacts and the emerging global culture – characterised as new, individualist, competitive, scientific and result-oriented, as opposed to traditional local cultures – lead to exclusionary reactions (Chiu, Gries, Torelli and Cheng 2011). The fear that global culture will contaminate local culture – so-called "contamination anxiety" (*ibid.*, 668) – can result in direct attacks against or the isolation of individuals or elements of the contaminating culture. Sociological research confirms that racially motivated crimes rise when racial and ethnic minority groups move into areas populated by white people and are determined by the perceived need to "defend the neighbourhood" from the perceived threat to the majority's interests posed by the minority (Green, Strolovitch and Wong 1998; Lyons 2007). These psychological and sociological findings are in line with criminological studies that describe hate crime as a mechanism of power and oppression attempting to re-create both the threatened (real or imagined) hegemony of the perpetrator's group and the "appropriate" subordinate identity of the victim's group (Perry 2001). Criminological research also confirms that often contact with diversity alone triggers hate crime, regardless of any hate or prejudice towards specific minorities. Relying on consistent literature, Chakraborti and Garland point out that many hate crimes are motivated merely by the vulnerability and the difference of their victims, perceived by hate offenders

as undesirable and easy targets. Examples include the homeless, the elderly, members of alternative subcultures etc. (Chakraborti and Garland 2012). Incidentally, empirical data collected by Mills, Freilich and Chermak (2017) disprove a causal relationship between poverty as such and hate crimes and demonstrate that these are more common in areas which are less poor but are experiencing worsening economic conditions and higher unemployment rates over time. This also confirms the emergence of anomic strains in times of change. More comprehensive ideological rebellions to the materialistic, and largely Western-like, values and goals of the emerging global culture can lead to also violent attempts to introduce a "new social order" (cf. Merton 1938, 677-678). Aggressive foreign politics, marginalising internal policies and the xenophobia nurtured by populist and nationalist rhetoric can act as proximate causes of terrorist attacks by fuelling criminal motivations.

These dynamics are inevitably exasperated by ICT. Cyberspace allows virtual contacts between people from diverse cultures, which would be impossible or very unlikely in the real world because of geographical distance. The media and the Internet amplify feelings of fear, anger and insecurity, which are an easy way to attract public attention, promote ideological agendas or gain in sales, "clicks", or "likes" (Bauman 2006, 96). Moreover, as psychologists observe, exclusionary responses are highly contagious and the Internet is a powerful means to spread them (Chieu, Gries, Torelli and Cheng 2011, 673). Messages of hate, bigotry, fear, mistrust, xenophobia posted on social media can reach millions of people around the world. Extremist or terrorist groups can systematically disseminate their propaganda and recruit affiliates through dedicated websites and social networks, such as the white supremacist website stormfront.org and the neo-Nazi social network "for people of European descent" Newsaxon (Holt 2012, 341-343). Finally, while cyber-terrorist attacks might still be rare (Helms, Costanza and Johnson 2011), the use of computer technology by terrorists to communicate, plan and organise attacks, as well as the connections between hacking and terrorism (Holt 2012, 343-345), are well documented (Broadhurst 2006).

3.3. Lost identities

In increasingly globalised societies, identities and social relations are disembodied from local contexts of interactions. Living in a global world means doing things and identifying oneself at a distance. This is what Giddens (1990) calls "disembedding" and Bauman (2000 and 2007) "liquidity". In such a context, it becomes very difficult for institutions to give stable identities to "mobile and versatile populations" (Franko Aas 2013, 177-178). Cyberspace is perhaps the most typical expression of these

processes. Research in psychiatry suggests that the Internet transforms human functioning, personhood and identity, with important implications for knowledge and consciousness (Kirmayer, Raikhel and Rahimi 2013, 167). Anonymous virtual interactions are experienced as liberating and offer the opportunity to craft one's own identity free from the constraints of material reality (Jewkes and Sharp 2003, 3). But there are various side-effects. In the first place, cyberspace can reinforce motivations to commit cybercrime. The virtual and anonymous nature of cyberspace lowers the perception of victims and of effective legal and social controls (the likelihood of being detected and punished), as suggested by psychology and criminology (see for instance Hinduja 2008, 396; Holt and Kilger 2012, 799). As a consequence, online behaviour – or at least certain types of behaviour – can be more disinhibited than in real life. Secondly, the Internet contributes to the differentiation of groups and amplifies the perception of group cohesion and normative support to individual behaviours, which is integral to extremist violence (Mills, Freilich and Chermak 2017, 1197-1199). Cyberspace can, therefore, facilitate the identification with virtual subcultures, such as the hacking community, as we will see in the next paragraph, or extremist and terrorist ideologies (Kirmayer, Raikhel and Rahimi 2013, 172). Here, individuals looking for an identity, under the strains of dominant cultural goals perceived as oppressive, easily find in radical or otherwise deviant ideologies new values to embrace, new ideals to live up to, new causes to support. This is the case, for instance, of the radicalisation of British citizens (Townsend 2016), also from non-Muslim backgrounds, such as the Greenwich-born punk singer Sally Jones (Weaver 2017). Thus, together with global mobility, ICT plays a crucial role in the processes of radicalisation. Sally Jones herself – it is reported – used various social media accounts to recruit women to Isis and provided practical advice on how to travel to Syria (*ibid.*).

3.4. The hacking community and the quest for identity, recognition and adventure

The hacking community is a deviant subculture developed around technology (Holt 2010) but ultimately driven by deeper socio-psychological factors. Hackers are not a homogeneous group. They are highly diversified in motivations and skill, as suggested by Rogers's successful taxonomy (newbies, cyberpunks, old guard hackers, internals, petty thieves, professional criminals and information warriors: Rogers 2006). Despite such variations, scholars from different disciplines agree that the hacking community is characterised by specific cultural elements (Steinmetz 2015

and 2016) which define its collective identity (Jordan and Taylor 1998, 762). An integrated analysis of the also empirical and ethnographic findings of various studies reveals the main components of such identity. These are (1) technology; (2) skills; (3) mentality; (4) transgressiveness/moral disengagement; (5) low perception of formal and informal sanctions. The first element is an "all-consuming" relationship with technology (*ibid.*, 763). Hackers conceive technology as something to be turned to new and unexpected uses – the so-called "hacks" and "cracks" (Holt 2010, 471-472). The focus is, therefore, not on technology itself, but on the labour required to manipulate it – the hacking process. Steinmetz notes that hackers share a "sense of ownership" over technological tools and the act of labour itself (Steinmetz, 2015, 127, 133-134). To perform such labour, another essential element is required: skills. Technical skills define hackers (Rogers 2006) and their hierarchy (Jordan and Taylor 1998, 768; Holt 2010, 474). Guild-like learning structures (often secret: Jordan and Taylor 1998, 768) are in place (Steinmetz, 2015, 134-135). To gain status, novices must devote themselves to learning from more experienced hackers in a sort of master-apprentice relationship (Steinmetz 2015) or from the collective wisdom of the community available online (Jordan and Taylor 1998, 764). Hackers see skills as the product of commitment, development and training, rather than raw talent (Steinmetz 2015, 132-133, 135). The creative approach to technology and the emphasis on technical skills reveal the next important component of the hacking community: a specific mentality characterised a problem-solving orientation and systematic and technical but at the same time creative and unconventional thinking (*ibid.*, 130-132). Hackers are moved by curiosity and an appetite for exploration (Holt 2017 and 2010, 475; Jordan and Taylor 1998, 768). They crave for the thrill of the hacking process and the liberating emotional reward of a successful hack (Jordan and Taylor 1998, 768-769; Steinmetz 2015, 136-137). The gratification is such that it overshadows the frustrations and risks of the process. This goes together with another defining element of the hacking subculture, which is transgressiveness, if not moral disengagement. This is fuelled not only by rationalisations of hacking as an act of creative resistance (Steinmetz 2015, 139-140) or even as a socially useful activity (Young, Zhang and Prybutok 2007, 285) but also by a low perception of both formal and informal sanctions. These perceptions are facilitated by the peculiar environment of the hacking community, which is mostly virtual and relatively isolated from the real world and subject to very different rules and controls. Hackers are not afraid of being socially excluded for their actions, as they are rewarded with the recognition and respect from their peers. And since the regulation

and the formal controls on online activities are not as uniform and certain as in real life, their deterrent effect is rather limited (*ibid.*, 285-286).

The sharing of software and knowledge by the members of the hacking community expands criminal opportunities and strengthens criminal motivations. Nevertheless, the ultimate reasons that determine hackers to commit cybercrimes are not necessarily a product of the hacking subculture. Although media representations and popular stereotypes have made of hackers the "archetypal 'cybercriminal'" (Wall 2007, 46), the criminal element is not what characterises hacking as a subculture (Steinmetz 2015, 126 and 2016). There are, indeed, hackers who have no criminal intent ("ethical hackers" or "white hats"). Their actions are motivated by ethical purposes, such as exposing the security flaws of computer systems or programming open-source software. Ethical hacking has become a proper profession and training, certifications and university degrees are available around the world (Caldwell 2011). To find what motivates hackers to engage in criminal behaviour we need, therefore, to look outside the hacking community. Some criminal hackers are motivated by financial gain. If so, anomie and strains theory might apply. But this is not always the case. Thrill- and sensation-seeking, the curiosity of exploration, the lust for adventure, and the need for peer appreciation can be more powerful motivators (cf. Jordan and Taylor 1998, 759-760 and 767-769). Thrill- and sensation-seeking are well-known criminal motivations (see Zuckerman 1974, 1994 and 2007; Baldwin 1985 and 1990; Burt and Simons 2013). Globalisation can reinforce them. In a world increasingly dominated by business and finance the everyday life of many people does not present many opportunities for idleness and adventure. Most individuals spend their day at work, often indoors, where individual impulses must be strictly controlled. Even outside the working environment, opportunities for excitement are very limited and mostly reserved to those who have more time and money to invest on travels and thrilling activities such as skydiving, motorcycling etc. (Russell 1949, 1310; Burt and Simons 2013, 1342-1343). ICT offers a cheap and readily available opportunity to engage in new forms of "rough play" and risky behaviours, with the additional benefit that in the virtual reality of cyberspace no physical strength is required and there are no perceived immediate physical consequences to wear off the excitement (cf. Baldwin 1985, 1327). This also confirms some of our previous conclusions on the impact of socioeconomic differences on cybercrime. Entry to hacking communities is inevitably denied to those living in poverty, with no access to ICT and very low levels of education. It is rather those who can access ICT and have a good level of schooling, but limited resources to satisfy their needs for stimulation who may turn to hacking (cf. Farley and Farley 1972; Robertson 1992). The need

for thrill is coupled with the need for peer recognition and appreciation and, more broadly, the quest for identity. The hacking community offers all this. It allows the development of new forms of identity beyond national and physical boundaries and fulfils the human need to progress in a communal way of life and recognise the same commitment in others members of the community (Jordan and Taylor 1998, 763). The identification with the values of the hacking community (so-called "hacker ethic") and the support of the other members can reinforce criminal motivations (cf. Levy 1984; Himanen 2001; Brown 2008). Criminal hacking is not, therefore, a direct product of hacking subculture but yet another expression of the incapability of national institutions to provide individuals with stable non-virtual identities and the means to pursue gratifying lifestyles in the context of increasingly globalising societies.

4. Discussion and policy recommendations

The above analysis suggests that technology sits at a particular junction in the causation of global crime. ICT expands criminal *opportunities*, by providing means for criminal behaviours and access to new criminal targets in a mostly anonymous virtual environment (cyberspace) particularly difficult to control. ICT also strengthens criminal *motivations* by spreading and amplifying cultural goals, strains and anxieties brought about by globalisation and by facilitating the online dissemination and consolidation of criminogenic ideas and identities. But many of the opportunities and motivations for cybercrime originate in deeper socio-psychological developments, often related to the inability of nation-states to appropriately control the criminogenic impact of globalisation. In other words, ICT is never the ultimate cause of cybercrime, but it enables *remote* causes to turn into *proximate* ones, making the risks of cybercrime more concrete. Any successful strategy to prevent cybercrime should, therefore, address not only the *means* but also the *causes*. And not only proximate *causes* but also *remote* ones.

Proximate causes are relatively easy to detect and tackle, as suggested by the overall positive experience of situational crime prevention (Clarke 1980, 1995, 2008 and 2012). The infrastructural and technological defences proposed by most local cybersecurity strategies are a good example of this. Remote causes can be more difficult to eradicate, particularly when they depend on socio-cultural, political, or financial evolutions which are out of the direct control of the state. However, difficulties should not be exaggerated, as this can end up in deresponsibilising local governments. Indeed, the above-mentioned research provides sufficient evidence to identify some of

such causes and reveals that these are often aggravated by state action or inertia. Appropriate policies should be adopted by national governments to fulfil their duty-responsibility to mitigate the criminogenic impact of global developments in their jurisdiction. Every relevant policy should include a specific section on the possible responsibilities of the government for engendering or aggravating both proximate and remote causes of crime and should identify the possible remedies. (Of course, international action is also required, but this goes beyond the scope of this article). We will outline below some policy recommendations broad enough to be used to assess existing cybersecurity strategies in any national jurisdiction and, hopefully, to support the drafting of new ones. It will become soon evident that many of these recommendations could be helpful also to prevent global crime in general.

4.1. Interdisciplinary research and dialogue between academia and practice

Uncontroversial scientific evidence of the causal correlations between global developments and global forms of criminality can be very difficult to gather. This, however, is not a valid reason to dismiss the remote causes of crime from prevention policies. On the contrary, it is an excellent reason to promote further interdisciplinary and comparative research.

A. States should invest in research not only on technology but also on the causes and forms of manifestation of cybercrime, with a particular focus on cultural, social, psychological and behavioural developments related to globalisation. Government-funded research projects on the causes of crime should always be (i) interdisciplinary, (ii) comparative, (iii) international and (iv) pluralistic. Scholars from any relevant discipline – psychology, criminology, law, history, natural sciences – and from different institutions should be involved to allow cross-verification and mutual integration of findings. Research should address also foreign contexts, frameworks and models, also through the collaboration with international partners and institutions.

B. Every cybersecurity policy should be based on the most solid of such research findings and should indicate the scientific frameworks on which it relies. Peer-reviewed academic works should be preferred to unverified open sources. Panels of experts from different backgrounds and institutions should be involved in the process of policy-drafting to advise on the quality of the sources utilised. Governments should promote, through consultations, workshops, roundtables etc., an ongoing dialogue between academia and practice – the judiciary, law enforcement, probation officers, policymakers

etc. Governments should resort to freelance or private consultancy firms with caution – as these might be driven by their own agendas or external influences. Whenever possible, universities and recognised research institutions should be preferred. These are better placed to offer impartial and high-quality research based on verifiable scientific methods.

C. Where research findings are insufficient or contradictory, governments should abstain from adopting any action, according to the principle of precaution, and commission further research by academic institutions.

4.2. Resolving anomie: social equality, welfare and human values

Anomic strains call for interventions on two different levels: the appropriateness of the means to achieve culturally valued goals and the appropriateness of the goals themselves. Acting on the means requires interventions to reduce social inequality. Promoting global equality and welfare is, therefore, a priority. This is not only a remit of international institutions: states have important duties and responsibilities too. National governments must commit to detecting and measuring national social inequality and appropriate welfare measures to provide equal access to personal, professional, social, financial, and technological means and opportunities. This should be accompanied by initiatives to develop appropriate social and legal norms to encourage the acceptable and responsible use of the means and opportunities available.

Acting on the goals implies a continuing reflection by local policymakers on the cultural values promoted by society and its institutions. In their policies, strategies and regulation, national governments should place more emphasis on notions of self-worth and self-achievement more adherent to the individual rights and responsibilities stemming from human dignity than the mere pursuit of social prestige and financial success. Particular stress should be placed on physical and mental wellbeing, self-awareness and positive social interactions as a necessary condition for the full enjoyment of fundamental human rights. International legal instruments expressing global commitment to such rights, such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights or the International Covenant on Economic, Social and Cultural Rights, should be the legal and cultural foundations of national policies. If this becomes common practice worldwide, it would also help consolidate a global consensus on the common nucleus of values proclaimed by those instruments. The centrality of individual values and rights does not equate to individualism. On the contrary, the universal recognition of the human person as the foundation of a global system of

values implies the acknowledgement of the mutual moral, social and legal duties and responsibilities of individuals, social formations and nations. The pursuit of individual opportunity and wellbeing should be therefore always counterbalanced by an equal emphasis on solidarity, mutual respect, tolerance, inclusivity, integration, honesty, legality, integrity, and accountability as foundational principles of the human society.

4.3. Education and mental wellbeing

Some psychological criminogenic factors triggered by globalisation, including anomic strains, anxiety, insecurity and fear can be mitigated through education and measures to promote physical and mental wellbeing. Together, these can be a formidable avenue to develop, at an individual level, self-awareness, rationality, critical thinking, realistic ambitions, inclusivity, a meaningful sense of identity and a culture of legality and integrity, which can gradually grow, at a collective level, into a better social regulation of cultural goals and the acceptable means to achieve them.

A. Governments should invest not only in teaching technical knowledge and skills to be deployed in the defence from cybercrime, but also in advancing (i) critical and independent thinking, and knowledge and understanding of (ii) human psychology and human behaviour; (iii) relationships, sex, physical and mental wellbeing; (iv) the rule of law, human rights and other fundamental social values supported by international law and the international community; (v) globalisation and its cultural and socio-psychological implications, including those caused by the contact with diversity. Such provision should be mandatory at all levels of education – including higher education and professional training – and it should be monitored, revised and updated periodically.

B. The teaching of computing in schools should focus not only on the safe and respectful use of ICT but also on issues related to the hacking subculture to counter both the glorification of criminal hackers and the unfair labelling of all hackers as criminals, and to promote virtuous and ethical uses of technical skills also by guiding students towards possible professional avenues for white hackers.

C. University programmes and professional training should become more interdisciplinary and include mandatory modules on psychological and behavioural issues, as well as on legal, ethical, social, political and economic issues, including those triggered by globalisation – with a particular focus on specific problems of the selected disciplinary field. University students and young professionals need the knowledge, skills and self-awareness required to face the pressures and the anxieties (including performance

anxiety) caused by the transition from adolescence to maturity and full independence, in an extremely competitive and diverse academic and professional world.

D. Free access to adequate support should be offered, in any possible environment (schools, universities, workplaces), to anyone suffering from mental health issues or psychological pressures of any kind. But free access to such support is meaningless if those who might benefit from it do not know it is available or are not willing to take it. Through education and widespread public information campaigns also online, governments should: (i) inform the population of the available support and the ways to access it; (ii) promote mental awareness and wellbeing as a valuable instrument of personal development; (iii) contrast any stigmatisation or marginalisation of those who suffer from any mental health issues or need any sort of support. The establishment of such a culture is also a fundamental step towards the promotion of values of self-worth different than just financial success or social prestige which can help mitigate the effects of anomie and strains.

4.4. Community, identity, integration and thrill

The knowledge and skills promoted through education should be complemented by specific community-based initiatives to provide citizens with instruments and opportunities to (i) form healthy personal identities (beyond online ones); (ii) strengthen integration and inclusivity by providing safe occasions of contact with diversity; (iii) corroborate a sense of belonging not only to local communities but to one human society and promote its fundamental values; (iv) gratify the need for thrill and adventure. Such programmes should consist of diversified social activities – lectures, seminars, workshops, counselling and psychological support, sporting groups, tourist trips, outdoor activities, festivals, social clubs etc. Information campaigns should raise awareness on the benefits of an active lifestyle, the associations between physical activity and mental wellbeing, the pleasures of time spent offline. Special events (awards, competitions, workshops…) for hackers should be organised to acknowledge the societal value of ethical hacking, encourage the development of computing skills in risk-free environments and channel such skills into lawful activities. Academia and industry should be involved through networking events and open days to offer hackers study and professional opportunities. Such initiatives should be carefully planned and coordinated by national and local authorities within a comprehensive national strategy aimed at achieving minimum common objectives while addressing specific local needs.

5. Conclusions: responsibilising the state through new notions of cybercrime and cybersecurity

To effectively prevent cybercrime, intervening on technology alone is not enough. Strengthening cyber defences and restricting the access to certain technologies or computer targets might help reduce some instant criminal motivations and opportunities (*proximate* causes), but won't affect the deeper global socio-psychological factors that trigger them, which we called *remote* causes of cybercrime. These must also be addressed. Although many remote causes, rooted as they are in the evolutions of globalisation, escape the immediate control of nation-states, there is much that national governments can do to can curb their criminogenic effects at a local level. Each state has the duty-responsibility to act at the best of their ability. This calls for quite a radical shift in perspective.

In the first place, there is a need for a more holistic approach. The causes and forms of manifestation of cybercrime are so diverse that diversified interventions are required. These include sophisticated social measures that might belong to areas of policy different than cybersecurity strictly considered. Some might be related to crime in general or to specific categories of offences that can also be committed through ICT (i.e. *cyber-enabled* offences). Others, such social integration strategies, education and professional training or community programmes, might not even concern crime directly. Nevertheless, these should never be oblivious to the criminogenic aspects of the phenomena they address. Nor should cybersecurity strategies be ever oblivious to the impact of these policies on cybercrime prevention. Any cybersecurity policy should be closely coordinated with other relevant policies, including those addressing different but related crime types.

Such a holistic approach implies a radical revision of the traditional notions of crime and cybercrime and cybersecurity. Reducing cybercrime – or any other global crime – to an evil to be fought, to malignant conduct determined by individual propensities or selfish motives – such as greed, hate or revenge – means failing to grasp its human dimensions and the extraordinary complexity of its causes, which include considerable institutional and social failures. Such reductive conceptions lead to the deresponsibilisation of the state. By placing the burden of the responsibility for crime on the individual alone and forgetting the enormous responsibilities of the state and society in providing ideal conditions for individual wellbeing, they hinder the individuation of comprehensive preventive strategies. They foster antiquated, oversimplified, stigmatising and antagonistic representations of crime which nurture the same irrational reactions – fear, anxiety, suspicion, xenophobia etc. – that motivate criminality and, eventually, undermine even the best

educational and social efforts to promote tolerance, diversity and solidarity and legality. It is urgent, therefore, to develop a socio-political understanding of crime as a complex human result of societal and environmental factors, often escaping individual control and often determined by the ineptitude of state policies or social norms. The corollary of such a conception of crime is replacing any restrictive notion of cybersecurity as a set of infrastructural or technological defences with the idea that security is, first and foremost, the realisation of equal societal conditions for individuals to lawfully fulfil their needs and ambitions. The provision of opportunities, however, must be accompanied by the promotion of more meaningful goals of self-achievement consistent with the value of the human person, as expressed by fundamental rights and responsibilities.

The current global political climate, affected by waves of populism and nationalism, might appear hostile to the formation of a political will to embrace such revolutionary changes. How to persuade politicians and policymakers to do so? The answer is knowledge. The pre-condition for any shift in perspective and policy is the development of an interdisciplinary scientific understanding of the human and social causes of cybercrime and global crime at large, possibly supported by empirical data. Investment in pluralistic international and comparative academic research is, therefore, paramount. But research alone is useless if it doesn't permeate politics and practice. The dialogue amongst academics, policymakers, lawmakers, public service, business and professionals should be strengthened. Education, training and information at all levels are required to develop more accurate institutional and social conceptions of cybercrime and its causes. Knowledge can also dissipate irrationality, fears and anxieties and support rational responses not only to cybercrime but to the rapid changes brought about by globalisation. Not everything lies therefore in the hands of politicians. Scholars, researchers, and intellectuals of all kinds have the responsibility to gain social trust by engaging with the public, the professions and the institutions of all kinds to develop scientific knowledge, share it through accessible channels and put it at the service of society.

References

Agnew, Robert. 1990. "Foundation for a General Strain Theory of Delinquency." *Criminology* 30:47–87.

Agnew, Robert. 1997. "The Nature and Determinants of Strain: Another Look at Durkheim and Merton." In *The Future of Anomie Theory*, edited

by Nikos Passas and Robert Agnew, 27–51. Boston: Northeastern University Press.

Agnew, Robert. 2005. *Why Do Criminals Offend? A General Theory of Crime and Delinquency*. Los Angeles: Roxbury.

Agnew, Robert. 2010. "A General Strain Theory of Terrorism." *Theoretical Criminology* 14(2):131–153.

Baldwin, John D. 1985. "Thrill and Adventure Seeking and the Age Distribution of Crime: Comment on Gottfredson and Hirschi." *American Journal of Sociology* 90:1326–1330.

Baldwin, John D. 1990. "The role of sensory stimulation in criminal behavior, with special attention to the age peak in crime." In *Crime in biological, social, and moral contexts*, edited by Lee Ellis and Harry Hoffman, 204–217. Westport: Praeger.

Bauman, Zygmunt. 1997. *Postmodernity and its discontents*. Cambridge: Polity.

Bauman, Zygmunt. 1998. *Globalization. The Human Consequences*. New York: Columbia University Press.

Bauman, Zygmunt. 2006. *Liquid Fear*. Cambridge.

Bauman, Zygmunt. 2007. *Liquid Times: Living in an Age of Uncertainty*, Cambridge: Polity.

Bauman, Zygmunt. 2012 (2000). *Liquid Modernity*. Rev. ed. Cambridge: Polity.

Brenner, Suzanne W. 2012. *Cybercrime and the Law. Challenges, Issues and Outcomes*, Lebanon (NH): Northeastern University Press.

Broadhurst, Roderic. 2006. "Developments in the Global Law Enforcement of Cyber-crime." *Policing: An International Journal of Police Strategies & Management* 29(3):408–433.

Brown, James J. Jr. 2008. "From Friday to Sunday: The Hacker Ethic and Shifting Notions of Labour, Leisure, and Intellectual Property." *Leisure Studies* 27:395–409.

Burt, Callie H. and Simons, Ronald L. 2013. "Self-Control, Thrill-Seeking, and Crime. Motivation Matters" *Criminal Justice and Behavior* 40(11):1326–1348.

Caldwell, Tracey. 2011. "Ethical Hackers: Putting on the White Hat." *Network Security*." June:10–13.

Cantor, David and Land, Kenneth C. 1985. "Unemployment and Crime Rates in the Post-World War II United States: A Theoretical and Empirical Analysis." *American Sociological Review* 50:317–332.

Casey, Eoghan. 2011. *Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet.* 3rd ed. Waltham (MA)-San Diego-London: Academic Press.

Castel, Robert. 2003. *L'Insécurité Sociale: Qu'Est-ce Qu'être Protégé?* Paris: Seuil-La République des Idées.

Chakraborti, Neil and Hardy, Stevie-Jade. 2017. "Beyond Empty Promises? A Reality Check for Hate Crime Scholarship and Policy." *Safer Communities* 16(4):48–154.

Chamlin, Mitchell B. and Cochran, John K. 1995. "Assessing Messner and Rosenfeld's Institutional Anomie Theory: A Partial Test." *Criminology* 33: 411–429.

Chiu, Chi Yue, Gries, Peter, Torelli, Carlos J. and Cheng, Shirley Y.Y. 2011. "Toward a Social Psychology of Globalization." *Journal of Social Issues* 67(4):663–676.

Clarke, Ronald V. 1980. "'Situational' Crime Prevention: Theory and Practice." *British Journal of Criminology* 20(2):136–147.

Clarke, Ronald V. 1995. "Situational Crime Prevention" *Crime and Justice* 19:91–150.

Clarke, Ronald V. 2008. "Situational Crime Prevention." In *Environmental Criminology and Crime Analysis*, edited by Richard Wortley and Lorraine Mazerolle, 178–194. London-New York: Routledge.

Clarke, Ronald V. 2012. "Opportunity Makes the Thief. Really? And So What?" *Crime Science* 1(1):1-9.

Cloward, Richard A. and Ohlin, Lloyd E. 1960. *Delinquency and Opportunity.* Abingdon: Routledge.

Cohen, Albert K. 1955. *Delinquent Boys.* New York: Free Press.

Cohen, Albert K. 1965. "The Sociology of the Deviant Act: Anomie Theory and Beyond." *American Sociological Review* 30:5–14.

Cohen, Lawrence E. and Felson, Marcus. 1979. "Social Change and Crime Rate Trends: A Routine Activity Approach." *American Sociological Review* 44:588–608.

Coleman, James W. 1987. "Toward an Integrated Theory of White-Collar Crime." *American Journal of Sociology* 93(2):406–439.

Coleman, James W. 1992. "Crime and Money Motivation and Opportunity in a Monetarized Economy." *The American Behavioral Scientist.* 35(6):827–836.

Durkheim, Émile. 1897 (2002). *Suicide. A Study in Sociology*, translated by John A. Spaulding and George A. Simpson. London-New York: Routledge.

Farley, Frank H. and Farley, Sonja V. 1972. "Stimulus-seeking Motivation and Delinquent Behavior among Institutionalized Delinquent Girls." *Journal of Consulting and Clinical Psychology* 39:94–97.

Franko Aas, Katja. 2013. *Globalisation and Crime*. 2nd ed. London: Sage.

Giddens, Anthony. 1990. *The Consequences of Modernity*. Cambridge: Polity.

Goodman, Marc D. 1997. "Why the Police Don't Care About Computer Crime." *Harvard Journal of Law and Technology* 10(3):465–494.

Grabosky, Peter N. 2001. "Virtual criminality: Old wine in new bottles?" *Social & Legal Studies* 10(2):243–249.

Green, Donald P., Strolovitch, Dara Z. and Wong, Janelle S. 1998. "Defended Neighborhoods, Integration, and Racially Motivated Crime." *American Journal of Sociology* 104:372–403.

Helms, Ronald, Costanza, S.E. and Johnson, Nicholas. 2011. "Crouching Tiger or Phantom Dragon? Examining the Discourse on Global Cyber-terror." *Security Journal* 1–19.

Himanen, Pekka. 2001. *The Hacker Ethic: A Radical Approach to the Philosophy of Business*. London: Penguin.

Hinduja, Sameer. 2008. "Deindividuation and Internet Software Piracy." *CyberPsychology & Behaviour* 11(4): 391–398.

HM Government. 2016. *National Cyber Security Strategy 2016-2021*. London: Home Office.

Holt, Thomas J. 2010. "Examining the Role of Technology in the Formation of Deviant Subcultures." *Social Science Computer Review* 28(4):466–481.

Holt, Thomas J. 2012. "Exploring the Intersections of Technology, Crime, and Terror." *Terrorism and Political Violence* 24(2):337–354.

Holt, Thomas J. and Max Kilger. 2012. "Examining Willingness to Attack Critical Infrastructure Online and Offline." *Crime & Delinquency* 58(5): 798–822.

Jewkes, Yvonne and Sharp, Keith. 2003. "Crime, Deviance and the Disembodied Self: Transcending the Dangers of Corporeality." In *Dot. Cons: Crime, Deviance and Identity on the internet*, edited by Yvonne Jewkes, 3–17. Cullompton: Willan.

Jordan, Tim and Taylor, Paul. 1998. "A Sociology of Hackers." *The Sociological Review* 757–780.

Kirmayer, Laurence J. Raikhel, Eugene and Rahimi, Sadeq. 2013. "Cultures of the Internet: Identity, Community and Mental Health." *Transcultural Psychiatry* 50(2):165–191.

Kigerl, Alex. 2011. "Routine Activity Theory and the Determinants of High Cybercrime Countries." *Social Science Computer Review* 30(4):470–486.

Larsson, Stefan, Svensson, Måns and de Kaminski, Marcin. 2012. "Online Piracy, Anonymity and Social Change: Innovation through Deviance." *Convergence: The International Journal of Research into New Media Technologies* 19(1):95–114.

Levchak, Philip J. 2015. "Extending the Anomie Tradition: An Assessment of the Impact of Trade Measures on Cross-national Homicide Rates." *Homicide Studies* 19(4):384–400.

Levy, Steven. 1984. *Hackers: Heroes of the Computer Revolution*. London: Penguin.

Loeb, Martin. 2004a. "The Indirect Cost of Cybercrime." *Optimize* April:85–86.

Loeb, Martin. 2004b. "Cybercrime's True Price: Crime May Not Pay, but Someone Has to Pick Up the Cost." *InformationWeek* 982:55–56.

Lyons, Christopher J. 2007. "Community (Dis)organization and Racially Motivated Crime." *American Journal of Sociology* 113:815–863.

Mathieu, Jean-Luc. 1995. *L'Insécurité*. Paris: Presses Universitaires de France.

McGuire, Mike and Dowling, Samantha. 2013. *Cyber crime: A review of the evidence. Research report 75. Summary of key findings and implications*. London: Home Office.

Merton, Robert K. 1938. "Social Structure and Anomie." *American Sociological Review* 3(5):672–682.

Merton, Robert K. 1968. *Social Theory and Social Structure*. New York: Free Press.

Messner, Steven F. and Rosenfeld, Richard. 1997. "Markets, Morality, and an Institutional-Anomie Theory of Crime." In *The Future of Anomie Theory*, edited by Nikos Passas and Robert Agnew, 207–227. Boston: Northeastern University Press.

Messner, Steven F. and Rosenfeld, Richard. 2013. *Crime and The American Dream*. 5th ed. Belmont: Wadsworth.

Mills, Colleen E., Freilich, Joshua D. and Chermak, Steven M. 2017. "Extreme Hatred: Revisiting the Hate Crime and Terrorism Relationship to Determine Whether They Are 'Close Cousins' or 'Distant Relatives'." *Crime & Delinquency* 63(10):1191–1223.

Neufeld, Derrick J. 2010. "Understanding Cybercrime". In *Proceedings of the 43rd Hawaii International Conference on System Sciences*, 1-10. Washington: IEEE Computer Society.

Orrù, Marco. 1987. *Anomie: History and Meanings*. London: Unwin Hyman.

Bernburg, Jón G. 2002. "Anomie, social change and crime. A theoretical examination of institutional-anomie theory." *British Journal of Criminology* 42:729–742.

Pasculli, Lorenzo. 2015. "The Age of Prevention. Crime and Crime Prevention in the Global Era." *Centre for Crime and Justice Research Seminar Series*, February 25.

Pasculli, Lorenzo. 2020. "Foreign Investments, the Rule of Corrupted Law and Transnational Systemic Corruption in Uganda's Mineral Sector". In *Trade, Investment and the Rule of Law*, edited by Rafael Leal-Arcas. Chisinau: Eliva Press.

Pasculli, Lorenzo and Nicholas Ryder. 2020. "The Global Anti-Corruption Framework. Lights, Shadows and Prospects". In *Corruption, Integrity and the Law. Global Regulatory Challenges*, edited by Pasculli, Lorenzo and Nicholas Ryder, 3–13. Abingdon: Routledge.

Passas, Nikos. 1990. "Anomie and Corporate Deviance." *Contemporary Crises* 14:157–178.

Passas, Nikos. 2000. "Global Anomie, Dysnomie, and Economic Crime: Hidden Consequences of Neoliberalism and Globalization in Russia and around the World." *Social Justice* 27(2):16–44.

Perry, Barbara. 2001. *In the Name of Hate: Understanding Hate Crimes*. New York-London: Routledge.

Phelps, Amy and Watt, Allan. 2014. "I Shop Online – Recreationally! Internet Anonymity and Silk Road Enabling Drug Use in Australia." *Digital Investigation* 11:261–272.

Pocar, Fausto. 2004. "New Challenges for International Rules Against Cyber-crime." *European Journal on Criminal Policy and Research* 10(1):27–37.

Rogers, Marcus K. 2006. "A Two-dimensional Circumplex Approach to the Development of a Hacker Taxonomy." *Digital Investigation* 3:97–102.

Rowland, Diane. 1998. "Cyberspace: A Contemporary Utopia?" *The Journal of Information, Law and Technology* 3.

Russell, Bertrand. 1949. "Can a Scientific Society Be Stable?" *British Medical Journal* 1307-1311.

Schaible, Lonnie M. and Altheimer, Irshad. 2015. "Social Structure, Anomie, and National Levels of Homicide." *International Journal of Offender Therapy and Comparative Criminology* 60(8):936–963.

Shaw, Eric D. 2006. "The Role of Behavioral Research and Profiling in Malicious Cyber Insider Investigations." *Digital Investigation* 3:20–31.

Simmler, Monika, Plassard, Isabelle, Schär, Noëmie and Schuster, Maximilian. 2017. "Understanding Pathways to Crime: Can Anomie Theory Explain Higher Crime Rates Among Refugees? Current Findings from a Swiss Survey." *European Journal on Criminal Policy and Research* 23(4):539–558.

Steinmetz, Kevin F. 2015. "Craft(y)ness. An Ethnographic Study of Hacking." *British Journal of Criminology* 55:125–145.

Steinmetz, Kevin F. 2016. *Hacked: A Radical Approach to Hacker Culture and Crime*. New York: NYU Press.

Stiglitz, Joseph. 2002. *Globalization and Its Discontents*. New York: Norton.

Stiglitz, Joseph. 2012. *The Price of Inequality*. New York: Norton.

Swader, Christopher S. 2017. "Modernization, Formal Social Control, and Anomie: A 45-Society Multilevel Analysis." *International Journal of Comparative Sociology* 58(6):494–514.

Teymoori, Ali, Bastian, Brock and Jetten, Jolanda. 2017. "Towards a Psychological Analysis of Anomie." *Political Psychology* 38(6):1009–1023.

Townsend, Mark. 2016. "From Brighton to the Battlefield: How Four Young Britons Were Drawn to Jihad." *The Guardian*, March 31. https://www.theguardian.com/uk-news/2016/mar/31/brighton-to-battlefield-how-four-young-britons-drawn-to-jihad-syria.

UNODC. 2013. *Comprehensive Study on Cybercrime*. Vienna: United Nations.

Wall, David. 2007. *Cybercrime. The Transformation of Crime in the Information Age*. Cambridge: Polity.

Weaver, Matthew. 2017. "Sally Jones: UK Punk Singer Who Became Leading Isis Recruiter." *The Guardian*, October 12. https://www.theguardian.com/world/2017/oct/12/sally-jones-the-uk-punk-singer-who-became-isiss-white-widow.

Young, Randall, Zhang, Lixuan and Prybutok, Victor R. 2007. "Hacking into the Minds of Hackers." *Information Systems Management* 24:281–287.

Zhao, Ruohui and Cao, Liqun. 2010. "Social Change and Anomie: A Cross-national Study." *Social Forces* 88:1209–1230.

Zuckerman, Marvin. 1974. "The Sensation Seeking Motive." *Progress in Experimental Personality Research* 7:79–148.

Zuckerman, Marvin. 1994. *Behavioral Expressions and Biosocial Bases of Sensation Seeking*. New York: Cambridge University Press.

Zuckerman, Marvin. 2007. *Sensation Seeking and Risky Behavior*. Washington: American Psychological Association.