Towards a Conceptualisation of Cloud (Cyber) Crime

David S. Wall(✉)

Centre for Criminal Justice Studies, School of Law, University of Leeds,
Leeds, UK
d.s.wall@leeds.ac.uk

Abstract. The term ‘Cloud’ is a misnomer that diverts attention from the level of conceptual clarification that is needed to understand the implications of cloud technologies upon criminal behavior, crime analysis and also law enforcement. Cloud technologies have increased computing power and storage capacity whilst reducing the cost of computing; all are qualities that have not been lost on criminals who have been using them to commit DDoS attacks, Data theft, mass spam attacks and other mass cyber-dependent crimes. This paper offers a framework for conceptualising cybercrimes in the cloud (cloud crimes) and for understanding how they drive offenders and affect victims. It also outlines the key challenges for law enforcement.

Keywords: Cybercrime · Cloud crime · Policing cybercrime in the cloud · DDoS · Data theft · Mass spam attacks

1 Introduction[1]

The ‘Cloud’ is a term that is frequently misused and often obfuscates attempts to understand its implications for criminal behavior. Some commentators refer to it as a ‘thing’, an object, whereas others see it as simply a technological method of increasing computer storage and power. Of course, there are also those who either see it as both, or neither, with the latter vehemently denying its existence at all. Yet, despite contradictory views about cloud technologies, it is clear that they have had a significant impact upon increasing computing power, increasing storage and generally making computing much cheaper than before. Cloud technologies provide an up-scale in criminal activity that is not lost on criminals who have already exploited the digital and networked technologies of the internet to commit high volume cybercrimes that greatly challenge preventative, investigative, and prosecution processes. They both facilitate and escalate cybercrimes. Furthermore, this ‘cloud’ lift also brings into play a range of new forms of (cyber) crimes against the machine; crimes that use the machine and crimes that are in the machine. All are crimes that need to be further understood in terms of their offending behaviors and their impact on victims. Such understanding will

[1] Paper delivered at the Human Dimensions of Cybersecurity panel of the 5th International Conference on Human Aspects of Information Security, Privacy and Trust, Vancouver Convention Centre, Vancouver, Canada 9-14 July 2017.

T. Tryfonas (Ed.): HAS 2017, LNCS 10292, pp. 529–538, 2017.
DOI: 10.1007/978-3-319-58460-7_37

inform policy debates and help resolve legal and law enforcement challenges in order to restore and maintain public confidence in the internet. This paper will suggest a framework for understanding cybercrimes and the way that they have been impacted upon by cloud technologies.

2 Methods

This paper draws upon previous work into the conceptualisation of cybercrimes (Wall 2017) (EPSRC CeRes EP/K03345X/1), including 'cloud', to begin a dialogue that seeks a more informed and workable conceptualisation of cloud crime and criminal behavior in the cloud? It forms an essential basis for the EPSRC funded CRITiCal project (Combatting cRiminals In The Cloud - EP/M020576/1) and the paper effectively outlines the structure and thinking behind the first work package. This conceptual paper also draws upon a couple of decades of my own work into technology and crime before and after the introduction of cloud technologies. It attempts to synthesize my own work and that of others on cybercrime and consider it as a platform for understanding cloud crime (see further the references cited in this paper and then the references that those works are based upon). The data requirements for this paper are therefore mainly library based, plus some secondary data to be re-analysed for the CRITiCal project that will feed into a later version of this paper. Later in the project cycle, work completed on the work packages will be fed back into the conceptualisation.

3 Framework

The conceptualisation of cybercrimes and the 'cloud' will be the focus of this paper and also the challenges they raise for law and law enforcement. They are challenges and conceptualisations that will need to be approached from an interdisciplinary perspective because different stakeholders' experience cloud technologies in different ways. Computer scientists, on the one hand, need to explore changes in cloud technologies and criminal behavior and they also need to understand the 'difference' between before and after cloud. Yet, police officers, on the other hand, for various reasons linked to the reporting, recording and investigating processes, will be unlikely to see any major direct impacts of cloud technologies in reports they receive of cybercrimes. Yet, a broader and more accurate conceptual understanding of cloud technologies and cloud crimes is vital if new predictive and investigative tools are to be created that will not only meet evidential legal standards where cybercrimes are investigated and prosecuted, but also to prevent them from happening in the first place.

The first part of this paper explores what is and is not a cybercrime. The second part then looks at the conceptual differences between cyberspace and the cloud (and also the Internet of Things). The third part explores the new criminal opportunities that the cloud adds to the cybercrime landscape and also raises questions as to whether, or not, the cloud changes patterns of criminal organisation online? The fourth and final part of the paper will consider the key challenges being faced by policing agencies who police cloud crimes.

3.1 What Is and What Is Not a Cybercrime

Over the past quarter century Cybercrime has changed from little more than a cyberpunk fantasy into a matter of national priority and international policy. Research and teaching programs have proliferated alongside a large and sophisticated cybercrime security industry with investments being counted in the $billions. Yet, whilst there is no doubt that everyone agrees that the problem exists, there is still considerable disagreement as to what cybercrime exactly is and how to deal with it, even so far on in time from the early 1990s.

Before exploring what is or what is not a cybercrime it is important to first outline the changing technological environment which has transformed criminal behavior. The following are observations about that transformation drawn from my own work and that of others (found in the references of those works). The first is that cybercrime takes place in a cyberspace; an 'imaginary' space created by the social reaction to the combination of Digital and Network technologies and culturally shaped by social science fiction (Wall 2012). Social behavior online has been transformed by digital and networked technologies across networks of communication, which has created behaviors that are *global*, *informational*, and *distributed* (see the references to Castells 2000 in my 2007 book). Important here is the fact that whilst this space may be imaginary, the consequences of criminal actions in cyberspace have very real consequences in the physical world.

The second observation is that cybercrimes are enabled by the same technologies that create cyberspace. The same technologies that create cyberspace have also transformed criminal behavior in much the same ways to make crime global, informational and distributed (Wall 1997, 2007). This virtual world has not only had a massive impact upon our everyday lives, but it has also created new criminal opportunities, causing victimizations that have very real consequences for individuals. Originating in 1980s cyberpunk literature, the term cyberspace and cybercrime causes much confusion, even conflict, between different commentators. But, cybercrime and cyberspace are here to stay because they have become so culturally embedded in the common parlance - despite attempts to avoid them by using the term 'digital' or some other word instead (see further, discussion in Wall (2002, 2007, 2012)).

The third observation is that cybercrimes become more and more automated as digital and networked technologies become advanced and more sophisticated. Networked and digital technologies do what other advanced technologies do, they deskill and then re-skill labor - this deskilling and reskilling process also applies to the crime labor that commits cybercrime (for offending is a form of labor) (see Wall 2007). As with many aspects of ordinary work (labor) over time, technology and the ideas behind it have tended to separate out work tasks and automate them; usually to make them cheaper to perform and improve efficiency. In so doing, many skills have been absorbed by an automation process, but this deskilling has also created new skills to control the technology that controls those new processes (re-skilling). The fact that one or two people can now control an entire criminal process that once required many people and with specialist skill sets has profound implications for our understanding of the organization of cybercrime. In a rather cynical way, the internet has effectively democratized crimes such as fraud that were once seen as the crimes of the powerful and the privileged. In a nutshell, networked and digital technologies have created an environment in which there is no longer any need for criminals to commit a large crime at great risk to themselves, because one person can commit many small crimes with lesser risk to themselves. The financial criminal no longer needs to commit a single $50 million robbery with its complex collection of criminal skill sets and high levels of personal risk when he or she can, for example, commit 50 million X $1 low risk thefts themselves from the comfort and safety of their own home (Wall 2007: 3, 70). If not a bank robbery, then criminals can commit a major hack, a DDOS (Distributed Denial of Service) attack, a hate speech campaign, or suite of micro-frauds; see for example, the case of Lomas in the UK who scammed 10,000 victims out of £21 million or the 15 year old hacker who, with three others, allegedly hacked the TalkTalk database and stole personal information on 1.2 million customers (Wall 2015).

At the far end of this automation process, some forms of malware can operate totally by itself (see for example, fake anti-virus scams and Ransomware). Or it can run crime portals that can rent out bespoke malware via crimeware-as-a-service (Wall 2015). In such circumstances, the scientific entry level required of cybercrime offenders has fallen and the technology effectively 'disappears' because its operation becomes intuitive and offenders no longer require the high-end programming skills that they once needed. Another significant development has been the drop in the cost of technologies, which has dramatically reduced the start-up costs of crime, thus increasing the level of incentive. The impact of these transformations upon cyber crime is that the average person can, in theory, now commit many crimes simultaneously in ways not previously imagined possible, and on a global scale. These three observations set out the basic differences between online and offline crime as well as outlining the changes in the technological environment in which cybercrimes take place. But what they do not do is explain the differences in cybercrime and the many competing explanations of them that exist in the literature. There are two differentiating factors here:

The first differentiating factor is that cybercrime accounts often confusingly address different victim groups, which each proscribe different security debates. Although there may be similarities in 'crime type' used, individual victims are quite different from business and organizational victims, who in turn are different from nation state victims (national infrastructure) (see Wall 2015). Each has different motivations, offender groups and also attack tactics, different stakeholders and agencies. In addition, we also need to separate the cybersecurity debates over risk and threats from the cybercrime debates (cybersecurity) over *actual* harms to individuals, businesses and nation states (policing). These two sets of issues are often confused, sometimes deliberately, when in fact they each represent different actions. As in the offline world, not all threats and risks manifest themselves as harms to the individual, and not all harms are crimes. But some do and how do we make sense of them?

The second differentiating factor is that cybercrime should be understood as a process of transformation rather than a thing or things. One of the problems with contemporary explanations of cybercrime is that they often attempt to button hole online actions into a definition; which never seems to explain satisfactorily the complete phenomenon - only parts of it at any one time.

3.1.1 Understanding Cybercrime as Transformational Rather than Definitional

Instead of taking a definitional approach, I have suggested that cybercrime really describes a transformational process from one state (offline) to another (online) (see Wall 2007) - a process that is continuing into the future with the development of cloud technologies and the internet of things. By using this approach the multiple layers of cybercrime offending can be understood, not just in legal terms, but also the different acts and different motivations. The most important characteristic is that cybercrime disappears if you take away digital and networked technologies. This is possibly the most significant of all observations when understanding cybercrime. If it does not disappear, then it is not a 'true' cybercrime. By applying this 'transformation test' (Wall 2007), either scientifically or metaphorically, then the possibility arises that in addition to 'true' cybercrimes there are a range hybrids, which might explain some of the rather confusing definitions. It also helps explain what the 'cyber-difference' is. This test also helps reflect upon how the crime was committed and the levels to which networked and digital technology have impacted upon the criminal behavior. We can use this 'transformation test' to understand how crimes have been transformed in terms of their mediation by technologies. At one end of the spectrum are '*cyber-assisted*' crimes that use the internet in their organization, but which would still take place if the internet was removed (e.g. a murderer web searching 'how to kill someone' or 'dispose of the body'). At the other end of the spectrum are '*cyber-dependent*' crimes which are the spawn of the internet, such as DDoS attacks, spamming, piracy etc. If the internet (networked technology) is taken away, then they simply disappear. In between the cyber-assisted and cyber-dependent crimes are a range of hybrid '*cyber-enabled*' crimes. These include most types of frauds and deception, but not exclusively, and are existing crimes in law, but are given a global reach by the internet, see for example the Ponzi frauds and pyramid selling scheme scams. Take away the internet, and these crimes still happen, but at a much more localized level, and they lose the global, informational and distributed lift that is characteristic of 'cyber' (see further discussion in Wall (2007, 2015)).

In addition to mediation by technologies, cybercrime offending has a number of different *modus operandi* (objectives and intents). This is a difference that is rarely commented upon systematically in the literature. We therefore need to distinguish '*cybercrimes committed against the machine*', such as hacking and DDOS attacks etc., from '*cybercrimes that use the machine*', such as frauds etc. Both of these also differ from '*cybercrimes in the machine*', such as extreme pornography, hate speech, offensive imagery and social networking originated offences and others. Yet, the distinction between them is rarely made in practice, even though the three types of *modus operandi* each relate to different bodies of law in most jurisdictions. Each of the three dimensions of cybercrime (influence of technology; *Modus Operandi*, victim group) can also be checked against each other in a matrix, see example in Fig. 1, to illustrate the different implications for understanding the levels of victimization experienced, but also the offenders and the way that they organize cybercrimes.

Technology by *Modus Operandi*	**Crimes against the machine**	**Crime using the machine**	**Crimes in the machine**
Cyber-assisted	Social engineering password theft	P2P fraud	Informational crime – terror handbook
Cyber-enabled		Mass Frauds	
Cyber-dependent	DDoS attacks, mass hacks	Phishing, Ransomware,	SNM, Hate speech

Fig. 1. Developing a cybercrime matrix (Mediation by technology v *modus operandi*)

3.2 What Are the Conceptual Differences Between Cyberspace and the Cloud (and the Internet of Things)

Mapping out cybercrime in the way described above enables cybercrime to be differentiated from offline crime and also in terms of different *modus operandi*, plus, also important for this discussion, levels of mediation by technology. The key question arises, what, therefore, happens when the technologies transforming or mediating criminal behavior change? Do the crimes change, does the criminal behavior change? These are essentially some of the objectives of the CRITiCal research project which this paper briefs. Early observations suggest that cloud technologies are impacting upon criminal behavior online in three transformational ways; by *increasing computing power*, they *increase storage capacity* and *reducing the cost of computing power*. This means that (cyber) criminals can commit a larger volume of more complex crimes at a reduced cost. So, cloud technologies are yet another form of force multiplier and one that helps to facilitate 'the internet of things' which greatly increases the number of devices that can be accessed by the internet and also potentially be exploited by criminals.

As stated earlier, cloud technologies both facilitate and enable cloud cybercrimes (cloud crime). They facilitate cloud crimes via Botnets, Crime-ware-as-a-service and also via ancillary procedures such as password decryption which requires the massive computing power that only cloud technologies can bring to the table. Cloud technologies also greatly escalate the scale of DDoS (Distributed denial of service) attacks, frauds and deception through spam transmission, and even the theft of complete clouds (mass data storage facilities). In a nutshell, the difference is that whereas networked and digital technologies meant that criminals no longer needed to commit a high risk $50 million robbery when they could commit 50 million low risk $1 robberies using a networked computer (see earlier example). The changes of scale that cloud technologies bring to the table now enable the same criminals to commit 50 billion robberies of, say, 0.1 cent, to achieve a greater yield and reduce the risk of prosecution even further.

In reality, cybercrimes have been gradually facilitated by cloud based technologies for about 15 years now and are part and parcel of cybercrimes already. But, whilst the differences mapped out here between cybercrime and cloud (cyber)crime are largely conceptual, they still need to be established in order to understand the technological aspects of crime for this project. Also, to refine the model or framework for understanding cybercrime outlined above. Furthermore, it also suggests that a further conceptual level could be related to the impact of cloud technology on the facilitation of cybercrime. Using the 'transformation' test or logic outlined above, we could hypothetically consider what would happen if the cloud technologies were to be removed. So, in this *cloud mediation model*, some cybercrimes are, for example, *cloud-assisted*, in that the underlying facilitating technologies assist them but, were the cloud aspect to be removed, they would still take place. At the other end of the spectrum, *cloud-dependent* cybercrimes would disappear if the cloud technologies were to be removed. In between, *cloud enabled* cybercrimes would lose the cloud lift (as described above) and crime volumes would return to their pre-cloud state.

3.3 What New Criminal Opportunities Are Facilitated and Enabled by Cloud Technologies?

This discussion raises the question as to what sort of cloud cybercrimes are emerging and what new cybercrimes can we expect in the future. As mentioned earlier cloud technologies facilitate cybercrimes via botnets, crimeware-as-a-service etc. They also enable a large volume of more complex crimes to take place etc. To understand this change, we can follow through the cloud mediation model outlined earlier. People will always source physical products from the internet so whilst these purchases are *cloud assisted* – assisted by cloud technologies - they would still take place regardless of the cloud. In contrast, a *cloud dependent* cybercrime would include, for example, some forms of data-theft, especially the theft of, or manipulation of a complete cloud. Take away the cloud aspect and the crime disappears. In between are *cloud enabled* cybercrimes; mass scam spams, for example, would (in estimation) reduce from 10 billion every 10 seconds to 10 million every 10 minutes if the cloud technologies were removed.

This cloud 'lift' has potential implications for changes in the organisation of cybercrime and the organisation of (cyber)criminals. The organisation of cybercrime and cybercriminals is very different to the organization of crime offline. Whilst there has been a tendency by media to sensationalize cybercrime by linking it with mafia groups, the literature covering this issue suggest that the nature of cybercrime and conceptualizations of traditional organized crime groups are highly incompatible (see Wall 2015). Indeed, the literature points to new forms of organization online that follow the distributed (networked), globalized and informational patterns of cybercrime. So, using the transformation terminology once again, we can talk about cyber-assisted forms of organization, where crime groups use technologies to assist their existing operations, including some traditional organized crime groups taking their existing areas of crime business online. There are also examples of cyber-enabled organization, where new groups of criminals use the internet networks to organize themselves to commit financial crimes. They obtain personal information online (say, though Phishing), then give it to offline money mules to monetarize the information. Take away the internet and they would commit the same crimes more locally and in much smaller volumes. Finally there are cyber-dependent organized crime groups, who commune online and commit crimes online. They are likely never to have met and are often unlikely to know each other's identity other than by pseudonym. They are also very ephemeral, even fluid because they tend to be a collaboration of ideas. Their organization is disorganized by comparison to other criminal groups and if you could take away the internet they would vanish.

To understand the potential for the growth of new forms of organized crime groups online in a cloud technology environment an economic model of cybercrime developed for the CeRes project (EP/K03345X/1) is combined with an analysis of organized crime online (Wall 2015). One of the potentially most obvious aspects of the force multiplier effect of cloud technologies' is the increased impact of cybercrimes upon mass victims. Because of the 'cloud lift' the financial or political yield of cybercrime (depending upon motivation) would be theoretically be much the greater, especially without any strong and effective organized crime groups online controlling the market for victims – as they do offline. Once a cybercrime is successful, however, then many other cybercriminals copy and try to commit the same form of cybercrime. This means that particular cybercrime types have a very short active life because, on the one hand, the victim market is diluted as other cybercriminals want to capitalise and there is no one preventing them from doing so. On the other hand, however, the potential victims (the victim market) become risk averse to cybercrime quite quickly through the words of mouth and warnings from the internet itself. The first generation of each cybercrime is therefore always the most successful in terms of yield from cybercrimes. But, the yield potential means that the stakes are high and it also means that organized crime groups are paradoxically incentivised to police other criminals in order to control their own share of the market.

Whilst there is little evidence to date of traditional organized crime groups moving activities online (as stated above), some have developed an online capacity to some of their more conventional criminal activities such as gambling. The concern is that there is now a strong incentive and means for online organized crime groups to develop and establish themselves online, especially as yields from crime grow, for example, as with Ransomware and extortion crimes more generally online.

3.4 What Are the Key Challenges Being Faced by Policing Agencies and the Criminal Justice System by Cloud Crimes

Cybercrime continues to challenge the criminal justice processes because of its very nature. One of the most distinctive characteristics of 'true' cybercrimes (cyber-dependent) is that they tend to be small-impact bulk-victimizations. So, cyber-frauds are micro-frauds and DDOS attacks and hacks of data are, with some exceptions, all individually small and most significant in their aggregate. This means that they are often *de minimis non curat lex*, too small to prosecute, and police and the criminal justice system find it hard to act on them individually. Police can only really act when a perpetrator is found, along with the aggregated proceeds of the crime as evidence. Furthermore, for reasons linked to the reporting, recording and investigating processes, police officers will be unlikely to see any major direct impacts of cloud technologies in reports they receive of cybercrimes. Because of their globalized nature, cybercrimes are also jurisdictionally problematic, unless the perpetrator is found and the evidence is strong enough to warrant an extradition order-if a treaty exists between the countries involved. Finally, there is also the need for policing expertise in cybercrime to be able to collect the relevant forensic evidence, build a case and present it to the court for prosecution – also to instruct a specialist when needed, say, a criminal psychologist. The final challenge is the 'reassurance' problem in policing cybercrime. A 'culture of fear' exists around cybercrime which, for various reasons, exaggerates its impacts and causes a 'reassurance gap' between levels of security demanded by the public which policing agencies that cannot deliver. This 'gap' broadly shifts the policing focus towards answering those demands, highly publicized arrests, visible actions, which often shifts resources from essential cybercrime policing functions. The 'cloud lift' will widen this shift and potentially cause the 'reassurance gap' to increase.

4 Conclusion

In this paper I have observed that Cybercrimes take place in a cyberspace and are therefore enabled by the technologies that create cyberspace, including cloud technologies. Cybercrimes are also becoming increasingly automated and they address a series of quite different victim groups. They should also be understood as techno-social-behaviors in a process of transformation rather than as a thing or things. So, adding these up, if you take away digital and networked technologies, then 'true' cybercrime disappears, but there are actually a range of cybercrime types. They differ according to the level of technological transformation and different *modus operandi*. Their organization also differs to that of crime offline. Furthermore, cybercrime creates immense challenges for the criminal justice system and its processes, which impacts upon public opinion. Finally, cybercrime is not going to go away as the internet cannot be switched off and there is no silver bullet solution.

The best we can do is mitigate their impact as new forms of cybercrime and threats arise. For this we need to keep on top of developments, design out some weaknesses and mitigate issues as they arise, however, over the next 5–10 years three key types of technological developments could further challenge law enforcement and keep criminologists and colleagues awake at night. Mesh technologies will probably join our digital 'devices' to develop lateral networks; self-deleting communications, such as Tiger texts or Snapchat will eradicate evidence before it can be captured, and crypto-currencies such as Bitcoin, Robocoin, Dodgecoin, Litecoin and especially Zerocoin, which claims to be anonymous will create alternative value-exchange systems. All three will potentially challenge existing forms of governance in different ways. Collectively, these three technologies, further amplified in time by cloud technologies that will make more computing power available to criminals at a cheaper cost and the 'internet of things' which will expand the scope of devices connected to the internet and also the volume of data flows which will provide new criminal opportunity. Most worrying is the fact that the technology will become so intuitive that it will tend to disappear as we will not notice it any more.

One final point to make is that the solutions to cybercrime are not always simply high tech. On the one hand, cybercrimes are a product of the social reaction to new (criminal) opportunities created by networked and digital technologies, so some technical solutions are needed. But on the other hand, there is a need to also respond to the social impacts of cybercrime, especially where young and other vulnerable people are either not understanding the gravity of their own actions. Or their actions are being misunderstood by significant others (parents, teachers, police), particularly the transgressive behaviors which drift into serious crime without the offender leaving their bedroom!

Acknowledgements. I must acknowledge the various inputs and inspiration of my interdisciplinary colleagues on the various research projects I am working on: the CeRes, CRITiCal, TAKEDOWN and BITCOIN projects. First are the many co-Is who are mentioned on the proposals and also the research assistants who came along later, more specifically, those who were with me at Durham; Ladan Cockshut, Noura Al-Moubayed, and those at Leeds, Laura Connelly, Yanna Papadodimitraki, Alena Connolly, Roberto Musotto and Maria Porcedda. I also value greatly my many conversations with members of the National Crime Agency who are both a strategic partner and also stakeholder on the CRITiCal project and also the members of the police forces who helped with the CeRes project (please note that the views expressed here are my own).

There are also a number of authors in my field of study who I would like to acknowledge and who have over the years helped me develop my thinking on the subject in my particular area of the field (Criminology and Criminal Justice) and I apologize to those whom I have accidentally omitted. There are the old school who are still writing and refining their work. They are Susan Brenner, Rod Broadhurst, Dorothy Denning, Andrew Goldsmith, Peter Grabosky, Yvonne Jewkes, Mike Levi, Sam McQuade, Russell Smith, Maggie Wykes, Majid Yar. There is also an exciting new school of scholars such as Adam Bossler, Tom Holt, Mike McGuire and Matt Williams. Plus on the horizon there is an emerging inter-disciplinary cadre of authors such as Russell Brewer, Lennon Chang, Raymond Choo, Alice Hutchings, Natalia Garcia, Grainne Kirwan, Rutger Leukfeldt, Anita Livorgna, Jonathan Lusthaus, Fernando Miro, Anna Sergi, Lisa Sugiura, Michael Yip and others. I recommend that you Google their names along with the term ‘cybercrime’.

References

Wall, D.S.: Policing the virtual community: the internet, cyber-crimes and the policing of cyberspace. In: Francis, P., Davies, P., Jupp, V. (eds.) Policing Futures, pp. 208–236. Macmillan, London (1997)

Wall, D.S.: Insecurity and the policing of cyberspace. In: Crawford, A. (ed.) Crime and Insecurity, pp. 186–209. Willan, Cullompton (2002)

Wall, D.S.: Cybercrime: The Transformation of Crime in the Information Age. Polity, Cambridge (2007)

Wall, D.S.: The devil drives a lada: the social construction of hackers as cybercriminals. In: Gregoriou, C. (ed.) Constructing Crime: Discourse and Cultural Representations of Crime and ‘Deviance’, pp. 4–18. Palgrave Macmillan, London (2012)

Wall, D.S.: Dis-organized crime: towards a distributed model of the organization of cybercrime. Eur. Rev. Organ. Crime **2**(2), 71–90 (2015)

Wall, D.S.: Crime, security and information communication technologies: the changing cybersecurity threat landscape and implications for regulation and policing. In: Brownsword, R., Scotford, E., Yeung, K. (eds.) The Oxford Handbook on the Law and Regulation of Technology. Oxford University Press, Oxford (2017)