Trends in Organized Crime
https://doi.org/10.1007/s12117-022-09450-5

Criminal markets and networks in Cyberspace

Anita Lavorgna[1] · **Georgios A. Antonopoulos**[2]

Accepted: 4 March 2022

Abstract
This is an introduction to the special issue of *Trends in Organized Crime* on 'criminal markets and networks in cyberspace'. All the contributions to this special issue, even if from different standpoints and focuses, help us understand how cyberspace is (re)shaping offenses and offenders.

Keywords Cyberspace · Online · Networks · Criminal markets

In our hyper-connected world, digital technologies and social media are so embedded in our everyday lives that we are increasingly part of a 'digital society' (Castells 2001; Lupton 2014; Stratton et al. 2017). Cyberspace per se is simply a social space connecting people and facilitating commerce. However, some of its characteristics (for instance, being virtually unlimited, and enabling both instantaneous and asynchronous communication) make it particularly prone to exploitation, and to the carrying out of countless illicit and malicious behaviours in very effective ways. Academic literature on crime and deviance in cyberspace has boomed in recent years, with most studies (think, for instance, of the seminal works of Wall 2007; Holt and Bossler 2015) focusing on so-called 'cybercrimes in a narrow sense' (such as hacking, spamming, copyright infringements) and, more recently, on a broader range of other computer-content crimes and deviant behaviours (Yar and Steinmetz 2019; Lavorgna 2020). Yet, there is still much unknown when it comes to cybercrimes.

✉ Anita Lavorgna
A.Lavorgna@soton.ac.uk

[1] Sociology, Social Policy and Criminology, University of Southampton, SO17 1BJ Southampton, United Kingdom

[2] Department of Social Sciences, Northumbria University, NE1 8ST Newcastle, United Kingdom

Published online: 01 April 2022

From an academic perspective, one preliminary issue to be addressed is that 'cybercrime' is still too often used as a hodgepodge for diverse criminal and/or harmful activities and behaviours, occurring (fully or partially) online being their main discerning factor. However, with the blurring of online and offline in our daily lives, it makes probably less and less sense to think of 'cyber' as something that can be easily kept apart from our 'real' routines in the physical world (Lavorgna 2020). Rather, in cyberspace – as in the physical space – we have very different types of activities and behaviours, each one deserving specific attention. This observation, of course, does not intend to deny the specific features of the digital (see, for instance, Powell et al. 2019).

As criminologists, we are mostly interested in all those activities and behaviours that can produce negative psychological, physical or financial effects on individuals and society alike (Agrafiotis et al. 2018). From this perspective, it is important to remember that there are still problems in fully recognising many of the harms occurring via digital means, with the exception of the financial harms broadly recognised by studies on profit-driven cybercrimes. It has been suggested that this might be due to the narrative that has traditionally surrounded cyberspace – a narrative whose roots come from a tradition of early techno-optimists stressing the utopic possibilities offered by new technologies, which emphasizes transcendence and a sort of disembodied vision of the relationship between humans and machines (Brydolf-Horwitz 2018). An effect of this narrative is that cyberspace is often assumed to be not (or less) 'real', because the body is not directly involved. This perception, unfortunately, is far from realistic. Rather, research suggests that -through cyberspace- certain harms can be even worsened and enhanced (see, for instance, Powell and Henry 2017), and in any case many cyber harms spill over into the physical space, having direct repercussions on individuals' mundane existence.

Moreover, cyberspace provides a socio-legal context that evolves extremely fast, with legal frameworks on and social perceptions of cyber threats and risks yet to be settled (Lavorgna 2020). Such ongoing evolution depends not only on the emergence of technological innovations, but also on power relationships in society (Adler and Adler 2006), and on the changes taking place in the political and economic arenas of our 'information age', which have important legal and ethical implications (Boyle 1996).

In this complex and developing context, a major challenge for researchers, and criminologists and sociologists in particular, is both to empirically study materializing manifestations of criminal, deviant or otherwise harmful activities and behaviours occurring through or facilitated by cyberspace, and to re-think and re-discuss their conceptualizations in cyberspace, pondering whether our current paradigms can properly capture emerging trends and patterns. Especially considering that much research on cyberspace is carried out nowadays by techno-epistemic networks of experts (such as computer and data scientists, both in academia and in cybersecurity companies), who have great digital capital (van Dijk 2005; Ballo 2015) but might lack sufficient intellectual (subject-matter) and critical capital on these matters, it is of fundamental importance for criminologists, and social scientists in general, to retain a role in these debates, both within their disciplines and in inter- and multi-disciplinary endeavours. After all, the challenges posed by cyberspace are of socio-

technical nature, and we need to be careful not to lose sight of the 'social'. Otherwise, we risk losing sight of the fundamental question behind all this – 'what kind of cyberspace do we want to live in?' – which requires understanding, defining and evaluating the trade-offs that our societies are willing to accept between, for instance, 'convenience' and 'security'.

In cybercrime research, some of the core research puzzles that still need many answers pivot around the evolving nature of criminal markets and networks. At the heart of this, is the (often implicit) assumption that, within and through cyberspace, the patterns of relationships of both activities and behaviours, and among individuals, change as a response to changes in the environmental factors in which relevant actors operate, creating new opportunities as well as new constraints. In other words, the social organization of both cybercrimes and cyber-criminals, as in all forms of crime, evolves in response to societal changes (see, among the classics, McIntosh 1975; Best and Luckenbill 1982). In cyberspace settings, however, these changes can be particularly quick and radical.

All the contributions to this special issue, even if from different standpoints and focuses, help us understand how cyberspace is (re)shaping offenses and offenders – a necessary starting point to imagine, develop and implement appropriate responses. The first article focuses on a "traditional" venue for cybercriminals – that is cryptomarkets, pseudonymous criminal marketplaces located in the so-called dark web –, shedding light on offender specialization. Past empirical research on offender specialization has focused on offline criminal endeavours, suggesting that most offenders engage in different forms of offenses during their criminal trajectories, while they generally fail to specialize in a specific crime. In the article *Diversification of tobacco traffickers on cryptomarkets*, by looking at original data from eight cryptomarkets, Rasmus Munksgaard, David Décary-Hétu, Vincent Mousseau and Aili Malm further this line of inquiry with reference to the offender specialization of tobacco traffickers in digital spaces – a very interesting case study because, as discussed by the authors, the barriers to become poly-traffickers are lower in cyberspace due to the readily available supply of illicit goods. Keeping in mind that cryptomarkets are not the preferred distribution channel for the illicit trade of tobacco, which mostly seems to rely on other already established distribution channels, the analysis confirms the diversification of offenders involved in online criminal marketplaces, with counterfeit products, psychedelics and cannabis being other common products trafficked by tobacco vendors online. The study also extends past research by quantifying the degree to which these offenders are diversified and by estimating the global sales of tobacco products on cryptomarkets.

The second article focuses on vendors in digital criminal market, but of a different kind. In the contribution *More Amazon than Mafia: analysing a DDoS stresser service as organised cybercrime*, Roberto Musotto and David S. Wall contribute to the literature by debating the opportunity to consider certain forms of cybercrime as 'organised crime' or even 'mafia' by focusing on a DDoS (Distributed Denial of Service) stresser (that is, an IT service which, for a fee, enables its clients to mobilise attacks and that can be used in both legal and criminal ways) in a context of cybercrime-as-a-service. Using Social Network Analysis, the authors demonstrate a clear organisation in the market, but they also show that this organisation is distributed

(rather than hierarchical), adaptive and, as the overall income yield is relatively low, further organisational activity is needed to make the service pay. As stressed by the authors themselves, this is in line with recent empirical research suggesting that most current cybercrime organizations are quite fluid and ephemeral in nature, and even if the involvement of more structured group might change with new, high impact cybercrimes, evidence still points to the direction that crime groups operating online are unlikely to imitate 'traditional' organized crime groups (operating mainly offline) in their structures and scopes.

Moving to the clear web, and to digital networks comprising both sellers and buyers, Anita Lavorgna and Gopala Sasie Rekha, in their contribution titled *From horticulture to psychonautics: an analysis of online communities discussing and trading plants with psychotropic properties* discuss a very peculiar and understudied aspect of internet-facilitated wildlife trafficking at the intersection of environmental crimes, illegal online trades, and drug use – that is, online forums dedicated to the discussion and the trades of endangered plant species that are sought after for their psychotropic properties. The article offers a better understanding of the socio-demographic and subcultural characteristics of these peculiar online communities, acknowledging that this is a necessary step to design and implement prevention or harm-reduction approaches. Most importantly, the study offers further evidence on the role of cyberspace in the creation and development of subcultures, stressing its role in identity formation and social learning. On the one hand, cyberspace allows for otherwise dispersed individuals with "niche" interests to find a common place that leads to communal spirit and social bonding and learning; on the other hand, it also facilitates the entrance into deviant and illegal spheres of new actors, often moving easily between legal, semi-legal and illegal spheres.

The last two articles rely on a similar approach – that of crime scripts – to systematically investigate two diverse types of widespread cybercrimes: phishing and computer frauds, respectively. In their contribution titled *Unravelling the crime scripts of phishing networks: an analysis of 45 court cases in the Netherlands*, Joeri Loggen and Rutger Leukfeldt examine Dutch court transcripts to unpack the *modus operandi* of phishing for information (aimed either at the theft of ATM or credit cards and pin numbers, or to transfer funds directly from the victims' bank accounts). Building on previous research on this topic, the authors clarify – among other things – some nuances in the script models and the pivotal role of money mules. Loggen and Leukfeldt also provide a number of suggestions for situational crime prevention, including through awareness-raising approaches.

Finally, in the article *The modus operandi of transnational computer fraud: a crime script analysis in Vietnam*, Trong Van Nguyen relies on data from criminal profiles and interviews with investigators analysed through a crime script approach to shed light on the characteristics and methods used by cyber fraudsters in the Vietnamese context. This is a topic of great international relevance as Vietnam is considered an emerging operational base for both domestic and foreign cybercriminals. The findings of this study, as stressed by the author, remind us of the importance of international cooperation when it comes to policing matters, but also – consistently with the previous article – the importance of preventive and awareness-raising approaches, targeting not only potential victims but also those who could get involved in criminal

networks (for instance, as money mules) without being fully aware of the severity of their actions.

Despite the heterogeneity of the criminal markets and networks considered, all the articles presented help us to emphasise some key aspects that are increasingly emerging in cybercrime research as pivotal, such as the *glocalization* of cybercrimes (that is, the permanent intertwining of the global and local dimensions, which coexist as two sides of the same coin, see also Lavorgna 2020), with its obvious implications in terms of: the need for both international cooperation and the improvement of local capacities; the fluid and transient nature of many relevant networks, with *some* of the individuals involved lacking a serious commitment towards a specific form of criminality, or towards criminality at all; the need to move beyond rigid and fictional distinctions when we study the relationship between the online and the offline, with the physical and digital dimensions of crimes being different in their manifestations, but also entangled.

We hope that that these themes will be further unpacked in new empirical research, and that this special issue will generate new discussions and debates around cybercriminality. We take this chance to thank all the authors and the anonymous reviewers for their precious insights and critical perspectives.

Compliance with ethical standards

Conflict of interest Anita Lavorgna and Georgios A. Antonopoulos declare that they have no conflicts of interest.

Human and animal participants This article does not contain any studies with human participants or animals performed by any of the authors.

References

Adler PA, Adler P (2006) 'The deviance society'. Deviant Behav 27(2):129–114

Agrafiotis I, Nurse JRC, Goldsmith M, Creese S, Upton D (2018) 'A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate'. J Cybersecur 4(1). doi:https://doi.org/10.1093/cybsec/tyy006

Ballo IF (2015) 'Imagining energy futures: Sociotechnical imaginaries of the future smart grid in Norway'. Energy Res Social Sci 9:9–20

Best J, Luckenbill DF (1982) Organizing deviance. Prentice-Hall, Englewood Cliffs, NJ

Boyle J (1996) Shamans, software, and spleens: Law and the construction of the information society. Harvard University Press, Cambridge

Brydolf-Horwitz R (2018) 'Embodied and entangled: Slow violence and harm via digital technologies'. Environ Plann C: Politics Space. doi:https://doi.org/10.1177/2399654418791825
Castells M (2001) The Internet galaxy: Reflections on the Internet, business and society. Oxford University Press, Oxford
Holt TJ, Bossler AM (2015) Cybercrime in progress. Theory and prevention of technology-enabled offences. Routledge, New York
Lavorgna A (2020) Cybercrimes: Critical issues in a global context. Palgrave Macmillan/Red Press, London
Lupton D (2014) Digital sociology. Routledge, London
McIntosh M (1975) The organization of crime. The Macmillan Press, London
Powell A, Henry N (2017) Sexual violence in digital age. Palgrave, London
Powell A, Straton G, Cameron R (2019) Digital Criminology. Crime and Justice in Digital Society. Routledge, London
Stratton G, Powell A, Cameron R (2017) 'Crime and justice in digital society: Towards a 'digital criminology'? Int J Crime Justice Social Democracy 6(2):17–33
van Dijk J (2005) The Deepening Divide: Inequality in the Information Society. Sage, Thousand Oaks, Ca.
Wall DS (2007) Cybercrime: The transformation of crime in the information age. Polity, Cambridge
Yar M, Steinmetz KF (2019) Cybercrime and society. Sage, London