# Cybercrime and shifts in opportunities during COVID-19

## A preliminary analysis in the UK

David Buil-Gil[1], Fernando Miró-Llinares[2], Asier Moneva[2], Steven Kemp[3] and Nacho Díaz-Castaño[2]

[1]Department of Criminology, University of Manchester, UK

[2]Crímina Research Centre, Miguel Hernandez University, Spain

[3]Department of Public Law, University of Girona, Spain

## Corresponding author

David Buil-Gil. G18 Humanities Bridgeford Street Building, Oxford Road, M13 9PL, Manchester, UK. Email: david.builgil@manchester.ac.uk

## Abstract

The COVID-19 outbreak and the far-reaching lockdown measures are having direct and indirect effects on complex social domains, including opportunities for crime offline and online. This paper presents preliminary analyses about the short-term effect of COVID-19 and lockdown measures on cyber-dependent crime and online fraud in the UK. Time series analyses from data about crimes known to police between May 2019 and May 2020 are used to explore the extent to which cybercrime has been affected by the COVID-19 outbreak. More specifically, we examine whether cybercrime has suffered an increase during the months with the strictest lockdown restrictions, as an effect of the displacement of crime opportunities from physical to online environments. Results indicate that reports of cybercrime have increased during the COVID-19 outbreak, and these were remarkably large during the two months with the strictest lockdown policies and measures. In particular, the number of frauds associated with online shopping and auctions, and the hacking of social media and email, which are the two most common cybercrime categories in the UK, have seen the largest increases in the number of incidents. The increase in cyber-dependent crimes has mainly been experienced by individual victims rather than organisations.

## Keywords

Crime trends, Internet, cyber security, fraud, police statistics, routine activities

## Full reference

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., Díaz-Castaño, N. (2020). Cybercrime and Shifts in Opportunities during COVID-19: A Preliminary Analysis in the UK. *European Societies*. https://doi.org/10.1080/14616696.2020.1804973

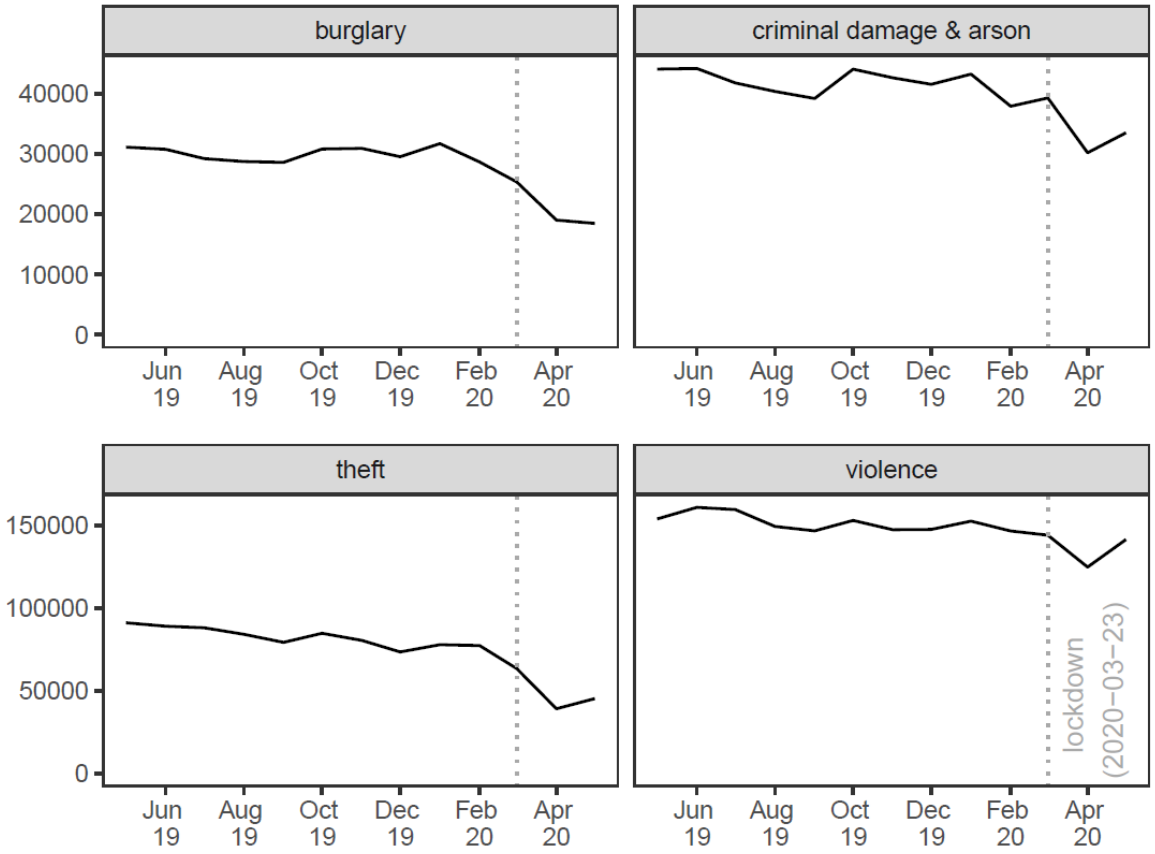
# Introduction

This paper analyses the extent to which cybercrimes known to police have been affected by the COVID-19 outbreak and the lockdown measures imposed by governments to prevent the spread of the virus. More specifically, we analyse if police-recorded cyber-dependent and cyber-enabled crimes have suffered an increase in the UK during the months with the strictest lockdown restrictions, as an effect of the displacement of crime opportunities from physical to online environments. Cyber-dependent crimes are offences that can only be committed using some form of computer systems or networks, such as hacking, computer viruses and denial of service attacks; while cyber-enabled crimes refer to traditional offences that have increased in scale and reach due to the use of computer systems, for example, online frauds and phishing scams (Wall, 2007).

The COVID-19 pandemic is causing extensive harmful consequences on the lives of millions of people. As of 29th June 2020, 10 million cases of COVID-19 have been reported globally, and almost 500 thousand deaths have been confirmed, according to data from the European Union Centre for Disease Prevention and Control. This global pandemic and the far-reaching lockdown measures imposed by governments worldwide are having wide-ranging effects on complex social domains such as working patterns, mobility, consumption, social cohesion and suicide (Kawohl and Nordt, 2020; Lianos, 2020). The pandemic has also fostered support for wealth redistribution and welfare policies (Matthewman and Huppatz, 2020).

Moreover, the COVID-19 crisis is associated with drastic, unprecedented changes in crime opportunities. Many have noted that most street crimes have decreased during lockdown due to reduced opportunities for physical convergence between offenders and targets (Ashby, 2020a; Mohler et al., 2020), as has also been shown in the UK (see Figure 1), while domestic abuse may increase since perpetrators and victims are required to remain confined in the same space for long periods of time (Piquero et al., 2020). Some argue that the massive move towards home working and online shopping during the outbreak may also contribute to a displacement of crime opportunities from offline to online environments (Collier et al., 2020; Hawdon et al., 2020; Payne, 2020; Payne et al., 2020). In other words, as persons spend more time connected to the Internet, and less time on the streets, opportunities for street violent and property crimes decrease while Internet crimes may increase (Miró-Llinares and Moneva, 2019). In this sense, this is one of the first papers to empirically examine the effects of the COVID-19 crisis on cybercrime, but it is also one of the first papers to analyse the potential impact that spending more time at home (and on the Internet) may have on cybercrime. This paper presents key information to gain understanding about the immediate effect of lockdown measures on cybersecurity risks faced by individuals and organisations, which can be essential for government agencies and companies to anticipate threats, design prevention strategies and outline cybersecurity recovery plans, and for researchers to further understand the impact of rapid social changes on crime online and offline. Cybercrime has important financial, emotional and psychological impacts on those who suffer it (Cross, 2018).

**Figure 1.** Count of crimes (violent crimes, burglary, theft and shoplifting, and criminal damage and arson) known to police in the UK (excluding Scotland) from May 2019 to May 2020.




Source: own elaboration (data from DATA.POLICE.UK)

# Lockdown, routine activities and cybercrime

Since, in 1979, Cohen and Felson (1979) explained that crime rates in the US were going up due to a series of societal transformations that had affected people's routine activities, many have studied how rapid social changes impact opportunities for offenders to converge with potential targets under the absence of guardians that are capable of protecting these targets (Felson and Eckert, 2018; Nieuwbeerta et al., 2003). Cohen and Felson (1979) studied how the increased use of electronic durables and motor vehicles facilitated access to new valuable goods and made criminals more mobile, and how increasing female labour participation, growing urban population and access to holidays reduced citizens' capacity to watch over each other and act as 'guardians' to reduce criminal opportunities. This triple convergence between offenders, targets and (lack of) guardians described by Cohen and Felson (1979) to explain opportunities for crime is known as Routine Activities Approach (RAA). Although RAA has been applied to cybercrime research to identify online risks and factors associated with various forms of cyber-victimisation (Holt and Bossler, 2008; Leukfeldt and Yar, 2016), few researchers have examined how the generalisation of Internet use in society may have affected opportunities for online and offline crime, and more specifically how the shift in societal activities from physical places to the Internet may have increased opportunities for crime in cyberspace (Miró-Llinares and Moneva, 2019; Wright et al., 2017). It seems probable that social transformations experienced during the COVID-19 outbreak have had substantial

impacts on the illegitimate opportunity structures that facilitate cyber-dependent and cyber-enabled crimes.

Of all the effects of the pandemic on people's everyday activities, perhaps the natural experiment produced by lockdown measures, the closure of businesses and education centres and the move towards home working is what has affected the greatest number of people. These changes have obvious consequences for citizens' offline and online routine activities and are likely to affect illegitimate opportunity structures for the convergence between targets, offenders and guardians offline and online (Felson et al., 2020). For instance, many use their personal computers to access business information, web conferencing substitutes in-person meetings, online shopping grows as a way to purchase products and services, and businesses remain empty for weeks while households are occupied most of the time. If the pandemic-related lockdown measures are multiplying the use of computer networks for business and leisure, and the number of e-commerce users is growing rapidly (Office for National Statistics, 2020a), it is also likely that new opportunities for the convergence described by RAA will arise on the Internet (Hawdon et al., 2020). In this sense, Payne (2020) analysed data from the US Federal Trade Commission and observed that reports of most types of fraud increased during the first months of 2020 compared to the same period in 2019; Lallie et al. (2020) noted that known cyber-attacks reported globally increased during the outbreak; and Collier et al. (2020) observed an increase in denial of service attacks in the UK. More specifically, since many businesses temporarily stopped their activity due to lockdown (Office for National Statistics, 2020b), we expect that the short-term increase in cybercrime primarily affected individual victims rather than organisations.

# Hypotheses

Based on the previous review of literature, we pose the following hypotheses:

> **H1.** Opportunities for cyber-dependent and cyber-enabled crimes have increased during the COVID-19 crisis.
> **H2.** The growth of cyber-dependent and cyber-enabled crimes has primarily affected individual victims.

# Data and methods

Action Fraud, the UK National Fraud and Cybercrime Reporting Centre, created a data dashboard in June 2020 to publish monthly statistics about fraud and cybercrime known to the police (https://www.actionfraud.police.uk/data). Crime statistics are published from May 2019 for various types of fraud and cybercrime. Data about regions where victims reside are also available, as well as whether victims are individuals or organisations. This paper analyses data about online frauds and cyber-dependent crimes recorded between May 2019 and May 2020 in order to explore potential effects of COVID-19 on cybercrimes reported to the authorities before and during the pandemic. More specifically, we will analyse the following forms of cybercrime:

- *Computer virus/malware/spyware:* A computer virus is a software that can replicate itself and spread from one computer to another, causing computer system failure or corrupting or stealing data. Malware refers to code scripts or computer software designed to disrupt or deny computer operations.

- *Denial of Service attacks* (with and without extortion): Attempts to make a computer or server unavailable to its users by bombarding it with thousands of hits, malware or mails, frequently using 'bots' to perform these attacks, to overload the system.
- *Hacking - Server:* Unauthorised use of, or access into, a computer server.
- *Hacking - Personal:* Unauthorised use of, or access into, a personal computer that is not a server.
- *Hacking - Social media and email:* Unauthorised use of, or access into, individual social media or email accounts.
- *Hacking - PBX/Dial Through:* Unauthorised use of, or access into, telephone systems that contain features such as 'call forwarding', 'voicemail' and 'divert'. This crime is mainly experienced by organisations.
- *Hacking combined with extortion:* Threats (blackmail) connected to computer hacking.
- *Online fraud* (including online shopping and auctions)*:* This category includes a variety of frauds enabled by digital technologies, such as online banking fraud, Internet-enabled card-not-present fraud, fraudulent sales through online auction or retail sites, consumer scams, phishing scams, pharming and so-called 'online romance' scams. All previous categories classify cyber-dependent crimes, while online fraud is a type of cyber-enabled offence.

In the UK, lockdown measures were announced on March 23, and new restrictions were added in April. April and May were the two months with the strictest lockdown restrictions. We aim to compare cybercrime statistics recorded in May 2019, prior to the pandemic, and May 2020, during lockdown. We calculate the percentage relative change between the count of crimes in May 2019 and May 2020 and make use of Poisson Mean Tests to analyse if the difference between the two crime counts is statistically significant (at 95% confidence level). We also examine trends in online frauds and cyber-dependent crimes from May 2019 until May 2020.

We note, however, that data published by Action Fraud may suffer from measurement error arising from victims' non-reporting to the police, and the loss amounts due to cybercrime, which are also briefly described here, are based on the victims' reports and are not verified by the police. Thus, data analysed in this paper include cyber-dependent crimes and online shopping frauds known to the authorities in the UK, and these are reliable indicators of police-recorded offences, but it is yet unknown if lockdown measures may have impacted crime reporting rates alongside crime victimisation (Caneppele and Aebi, 2017). The accuracy of these data as indicators of cybercrime incidence will be checked in further research using survey data. In addition, monthly data on crime counts have inherent limitations already highlighted elsewhere (i.e., not every month has the same number of days, nor weekends; Ashby, 2020b), which will be considered when analysing the results.

# Results

Table 1 compares cyber-dependent crimes and online frauds recorded in May 2019 and May 2020, and calculates the relative change between the two values for each crime type. We observe that most cyber-dependent and cyber-enabled crimes have experienced an increase between both years, and this increase is remarkably large and statistically significant in the case of hacking of personal computers, hacking of social media and email, and online fraud. Online fraud and hacking of social media and email are also the categories with the largest

frequency of offences. Thus, we observe that the overall number of cybercrimes is markedly larger in May 2020 than May 2019. We note, nevertheless, that three types of cybercrime have seen a decrease between May 2019 and May 2020. In the case of hacking of PBX/Dial Through, this decrease may be affected by the small number of cases registered and is not statistically significant, but the decreases observed in the count of computer viruses and hacking combined with extortion deserve further scrutiny.

The number of reports of computer viruses appears to be slightly larger in May 2019 than May 2020, but it should be noted that the figure for computer viruses recorded in May 2019 (742 reports) was the largest in 2019 and it was notably large compared to the average monthly count of computer viruses in 2019 ($\bar{x} = 615.6, sd = 72.7$). Moreover, the highest number of computer viruses since April 2019 was recorded in April 2020 (818), when strict lockdown measures were already in place. Similarly, the month with the largest number of reports of hacking combined with extortion was April 2020 (1,058 offences). In the case of hacking combined with extortion, we also note that the reported value of financial losses due to this crime was much greater in May 2020 (£86,7K) than May 2019 (£10.2K). Thus, although Table 1 appears to indicate that some cybercrime categories may not have increased during the COVID-19 outbreak, we need to provide some context by presenting time series analyses to examine the evolution of police-recorded crimes over time.

**Table 1.** Cyber-dependent crime and online fraud recorded in May 2019 and May 2020.

| | Count in May 2019 | Count in May 2020 | Relative change (%) |
|---|---|---|---|
| Computer virus/malware/spyware | 742 | 648 | -12.67* |
| Denial of Service attack | 14 | 18 | 28.57 |
| Hacking - Server | 24 | 25 | 4.17 |
| Hacking - Personal | 270 | 479 | 77.41*** |
| Hacking - Social media and email | 939 | 1,449 | 54.31*** |
| Hacking - PBX/Dial Through | 9 | 7 | -22.22 |
| Hacking combined with extortion | 313 | 251 | -19.81* |
| Online fraud - online shopping and auctions | 5,619 | 8,482 | 50.95*** |
| All cybercrimes | 7,930 | 11,359 | 43.24*** |

***p-value < 0.001, **p-value < 0.01, *p-value < 0.05

Source: own elaboration (data from Action Fraud UK)

It should be highlighted that some of the cybercrime categories with a less evident increase during the outbreak refer to crimes more commonly experienced by organisations (as opposed to individuals). In order to examine if the increasing trend in cybercrimes is observed for both individual victims and organisations, we present Table 2. While reports of cyber-dependent crimes against individual persons were higher in May 2020 than May 2019, and online frauds were substantially higher in May 2020, the frequency of cyber-dependent crimes against organisations was smaller in May 2020 than 2019 and such difference is not statistically significant. The apparent increase in police-recorded cybercrimes seems to be experienced mainly by individuals, whereas the frequency of cyber-dependent crimes reported by organisations shows different temporal patterns depending on each crime type (i.e., computer viruses appear to increase slightly, denial of service attacks remain stable, and hacking attacks decrease).

**Table 2.** Cyber-dependent crimes and online frauds suffered by individuals and organisations in May 2019 and May 2020.

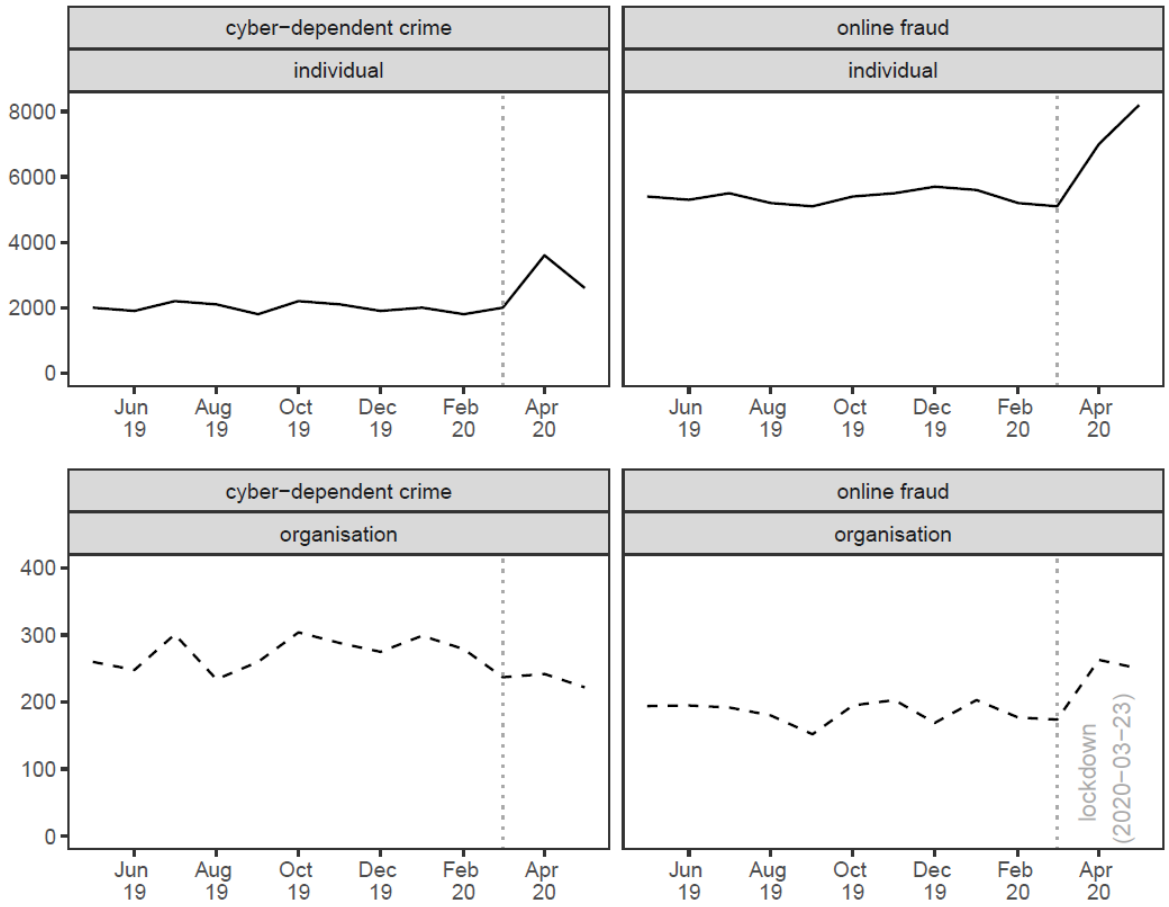
| | | Count in May 2019 | Count in May 2020 | Relative change (%) |
|---|---|---|---|---|
| Cyber-dependent crimes | Individuals | 2,300 | 2,643 | 14.91*** |
| | Organisations | 260 | 222 | -14.62 |
| Online fraud - online shopping and auctions | Individuals | 5,408 | 8,220 | 51.99*** |
| | Organisations | 194 | 250 | 28.87** |
| All cybercrimes | Individuals | 7,708 | 10,863 | 40.93*** |
| | Organisations | 454 | 472 | 3.96 |

***p-value < 0.001, **p-value < 0.01, *p-value < 0.05

Source: own elaboration (data from Action Fraud UK)

However, comparing crime counts between two months may be misleading if it is not contextualised by comparing these with the overall temporal pattern. Figure 2 shows the number of offences known to police by crime category (cyber-dependent crimes and online fraud) and type of victim (individuals and organisations) between May 2019 and May 2020. Figure 2 clearly indicates that the number of cyber-dependent crimes against individuals peaked in April 2020 and was markedly high in May 2020 compared to other months. This distribution is observed for most types of cyber-dependent crimes. The number of cyber-dependent crimes experienced by organisations appears to decrease during the outbreak. Similarly, we can observe that the number of frauds associated with online shopping and auctions peaks in April and May 2020, the months when the strictest lockdown measures were in place, but in this case, offences against both individual victims and organisations show an increase.

**Figure 2.** Count of cyber-dependent crimes and online frauds (online shopping and auction) known to police by victim type from May 2019 to May 2020.




Source: own elaboration (data from Action Fraud UK)

# Conclusions and word of caution

Our results suggest that reports of cyber-dependent crime and online fraud have increased during the COVID-19 outbreak, and rates of cybercrimes have been particularly high during months with the strictest lockdown policies. Lockdown measures and social distancing policies imposed by governments worldwide to prevent the spread of the virus have caused unprecedented effects on the way people interact, consume, conduct business, deliver services and find opportunities for crime (Felson et al., 2020; Payne et al., 2020). The everyday routine activities of millions of individuals have moved from physical to online environments, and opportunities for crime appear to have shifted towards cyber-dependent or cyber-enabled crime. Miró-Llinares and Moneva (2019) argued that the generalisation of Internet use may be associated with a displacement of crime opportunities from offline to online environments, and it is plausible that the rapid societal transformations experienced during the outbreak, which have increased the frequency and variety of activities that users conduct online, have created new illegitimate opportunity structures online (Hawdon et al., 2020; Lallie et al., 2020).

We have also observed that while there is an increase in police-recorded online shopping frauds against individuals and organisations, the increase in cyber-dependent crimes has mainly affected individual victims, and most types of cyber-dependent offences suffered by

organisations appear to have decreased. We can only speculate about the explanation for this observation, but it is plausible that opportunities to target organisations online have decreased given the amount of businesses who have ceased their activity during the outbreak (the Office for National Statistics [2020b] estimates that around 20% of businesses temporarily or permanently closed in May 2020). It is also possible, however, that some organisations will discover that they have suffered cyber-attacks when lockdown measures are lifted and organisations' IT services are back online. Further research should investigate if the volume of cyber-dependent crimes reported by organisations increases after lockdown measures are relaxed. Future studies should also investigate if some of the social changes experienced during the outbreak remain after lockdown measures are lifted, thus meaning that the rise in cybercrime may not be temporary, and establish comparisons between trends in online and offline offences.

These results, however, are subject to the limitations associated with the use of police-recorded data, which depend on the victim's willingness to report crimes to police and may vary across time and space (Caneppele and Aebi, 2017; Kemp et al., 2020). Estimates obtained from the Crime Survey for England and Wales 2018/19 indicate that 63% of all annual crimes in which the Internet is related in one form or another are never known to the police (Office for National Statistics, 2020c). In other words, only 27% of cybercrimes are known to the police, and it is yet unknown the extent to which the outbreak may have impacted not only illegitimate opportunity structures, but also the way in which people report crimes to police services. Future work should look into the effect of COVID-19 on crime reporting patterns.

This paper has presented preliminary analyses about the short-term effect of the COVID-19 outbreak on cybercrime opportunities, and results appear to show a clear increase in cybercrime incidents, but data used in the paper are subject to limitations and further research may analyse victimisation surveys to complement data about police-recorded crimes.

# References


Ashby, M. (2020a) 'Initial evidence on the relationship between the coronavirus pandemic and crime in the United States', *Crime Science* 9(6). https://doi.org/10.1186/s40163-020-00117-6

Ashby, M. (2020b) 'Why you can't identify changes in crime by comparing this month to last month', *Social Research Association*, 13 May.

Caneppele, S. and Aebi, M. (2017) 'Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes', *Policing: A Journal of Policy and Practice* 13(1): 66-79. https://doi.org/10.1093/police/pax055

Cohen, L. and Felson, M. (1979) 'Social change and crime rate trends: A routine activity approach', *American Sociological Review* 4: 588-608.

Collier, B., Horgan, S., Jones, R. and Shepherd, L. (2020) *The implications of the COVID-19 pandemic for cybercrime policing in Scotland: A rapid review of the evidence and future considerations*, The Scottish Institute for Policing Research, Research Evidence in Policing.

Cross, C. (2018) '(Mis)understanding the impact of online fraud: Implications for victim assistance schemes', *Victims & Offenders*, 13(6): 757-776. https://doi.org/10.1080/15564886.2018.1474154

Felson, M. and Eckert, M. (2018) *Crime and everyday life. Sixth edition*, Thousand Oaks: SAGE.

Felson, M., Jiang, S. and Xu, Y. (2020) 'Routine activity effects of the Covid-19 pandemic on burglary in Detroit, March, 2020', *Crime Science*. https://doi.org/10.1186/s40163-020-00120-x

Hawdon, J., Parti, K. and Dearden, T. (2020) 'Cybercrime in America amid COVID-19: The initial results from a natural experiment', *American Journal of Criminal Justice*. https://doi.org/10.1007/s12103-020-09534-4

Holt, T. and Bossler, A. (2008) 'Examining the applicability of lifestyle-routine activities theory for cybercrime victimization', *Deviant Behavior* 30(1): 1-25. https://doi.org/10.1080/01639620701876577

Kawohl, W., and Nordt, C. (2020) 'COVID-19, unemployment, and suicide', *The Lancet Psychiatry* 7(5): 389-390. http://doi.org/10.1016/S2215-0366(20)30141-3

Kemp, S., Miró-Llinares, F. and Moneva, A. (2020) 'The dark figure and the cyber fraud rise in Europe: Evidence from Spain', *European Journal on Criminal Policy and Research*. https://doi.org/10.1007/s10610-020-09439-2

Lallie, H., Shepherd, L., Nurse, J., Erola, A., Epiphaniou, G., Maple, C. and Bellekens, X. (2020) 'Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic', *arXiv*.

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

Lianos, M. (2020) 'The welfare state: where hope and fear meet', *European Societies* 22(3): 291-292. https://doi.org/10.1080/14616696.2020.1771861

Matthewman, S. and Huppatz, K. (2020) 'A sociology of Covid-19', *Journal of Sociology*. https://doi.org/10.1177/1440783320939416

Miró-Llinares F. and Moneva A. (2019) 'What about cyberspace (and cybercrime alongside it)? A reply to Farrell and Birks "Did cybercrime cause the crime drop?"', *Crime Science* 8(2). https://doi.org/10.1186/s40163-019-0107-y

Mohler, G., Bertozzi, A., Carter, J., Short, M., Sledge, D., Tita, G., Uchida, C. and Brantingham, P. J. (2020) 'Impact of social distancing during COVID-19 pandemic on crime in Los Angeles and Indianapolis', *Journal of Criminal Justice*. https://doi.org/10.1016/j.jcrimjus.2020.101692

Nieuwbeerta, P., De Geest, G. and Siegers, J. (2003) 'Street-level corruption in industrialized and developing countries', European Societies 5(2): 139-165. https://doi.org/10.1080/1461669032000072265

Office for National Statistics (2020a) *Retail sales, Great Britain: May 2020*, Office for National Statistics, https://www.ons.gov.uk/businessindustryandtrade/retailindustry/bulletins/retailsales/latest#stores-selling-online.

Office for National Statistics (2020b) *Coronavirus and the economic impacts on the UK: 4 June 2020*, Office for National Statistics, https://www.ons.gov.uk/businessindustryandtrade/business/businessservices/bulletins/coronavirusandtheeconomicimpactsontheuk/4june2020.

Office for National Statistics (2020c) *Crime Survey for England and Wales, 2018-2019*. [dataset]. UK Data Service. Available from: http://doi.org/10.5255/UKDA-SN-8608-1 [Accessed 25 June 2020].

Payne, J. (2020) 'Criminals work from home during pandemics too: A public health approach to respond to fraud and crimes against those 50 and above', *American Journal of Criminal Justice*. https://doi.org/10.1007/s12103-020-09532-6

Payne, J., Morgan, A. and Piquero, A. (2020) 'COVID-19 and social distancing measures in Queensland, Australia, are associated with short-term decreases in recorded violent crime', *Journal of Experimental Criminology*. https://doi.org/10.1007/s11292-020-09441-y

Piquero, A., Riddell, J., Bishopp, S., Narvey, C., Reid, J. and Piquero, N. (2020) 'Staying home, staying safe? A short-term analysis of COVID-19 on Dallas domestic violence', *American Journal of Criminal Justice*. https://doi.org/10.1007/s12103-020-09531-7

Wall, D. (2007) *Cybercrime. The transformation of crime in the Information Age*, Cambridge: Polity Press.

Wright, R., Tekin, E., Topalli, V., McClellan, C., Dickinson, T. and Rosenfeld, R. (2017) 'Less cash, less crime: Evidence from the electronic benefit transfer program', *Journal of Law and Economics* 60: 361-383. https://doi.org/10.3386/w19996