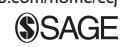
Article

Journal of Contemporary Criminal Justice
2021, Vol. 37(4) 480–501

DOI: 10.1177/10439862211027986
journals.sagepub.com/home/ccj



Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19

Steven Kemp[1,2,3], David Buil-Gil[3], Asier Moneva[4,5], Fernando Miró-Llinares[2], and Nacho Díaz-Castaño[2]

Abstract

The unprecedented changes in routine activities brought about by COVID-19 and the associated lockdown measures contributed to a reduction in opportunities for predatory crimes in outdoor physical spaces, while people spent more time connected to the internet, and opportunities for cybercrime and fraud increased. This article applies time-series analysis to historical data on cybercrime and fraud reported to Action Fraud in the United Kingdom to examine whether any potential increases are beyond normal crime variability. Furthermore, the discrepancies between fraud types and individual and organizational victims are analyzed. The results show that while both total cybercrime and total fraud increased beyond predicted levels, the changes in victimization were not homogeneous across fraud types and victims. The implications of these findings on how changes in routine activities during COVID-19 influenced cybercrime and fraud opportunities are discussed in relation to policy, practice, and academic debate.

Keywords

crime trends, coronavirus, ARIMA, cybersecurity, victims, crime statistics

[1]University of Girona, Spain
[2]Miguel Hernández University of Elche, Spain
[3]University of Manchester, UK
[4]Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), The Netherlands
[5]Center of Expertise Cyber Security, The Hague University of Applied Sciences, The Netherlands

Corresponding Author:
Steven Kemp, Faculty of Law, Carrer Universitat de Girona, 12, 17071 Girona, Spain.
Email: steven.kemp@udg.edu

Introduction

At the beginning of the COVID-19 pandemic, several sources warned of possible increases in cybercrime and fraud (especially cyber-enabled frauds[1]). In March 2020, Europol alerted about new ways in which cybercriminals were benefiting from the pandemic and associated lockdown measures (Europol, 2020b), and in October 2020, Europol's (2020a) Internet Organized Crime Threat Assessment stated that "COVID-19 caused an amplification of existing [cybercrime] problems" (p. 6) and noted an increase in fraud against businesses "as a result of the global outbreak of COVID-19" (p. 47). Similarly, Interpol's (2020) report entitled "Cybercrime: Covid-19 impact," published in August 2020, affirmed that there had been "a sharp increase in cybercriminal activities" (p. 4) related to the virus. As a preventive measure against such threats, U.K. law enforcement agencies used Twitter to raise public awareness, devoting 57.2% of their messages to fraud schemes and 16.9% to cybercrime problems (Nikolovska et al., 2020).

From an opportunity perspective (Newman & Clarke, 2003), it seems obvious to expect an increase in cybercrime and fraud when more people use the internet and converge in cyberspace. However, both these umbrella categories encompass a very diverse range of conducts (e.g., not all frauds are a form of cyber-enabled crime), and it is unlikely that trends are identical for all types of cybercrime and fraud. Furthermore, detected fluctuations may be very short term and may simply bounce back to the initial trend, or they could even be within normal crime variability. In fact, literature on traditional street crime in the United States, such as serious assaults, indicates that the relationship between lockdown measures and crime is not always as expected (Ashby, 2020), while preliminary analysis on cybercrime and COVID-19 in the United Kingdom indicated that individual and organizational victims may not be affected in the same manner (Buil-Gil et al., 2021b).

In this context, the main aim of this article is to provide further understanding of the relationship between the changes in daily activities brought about by the COVID-19 pandemic and cybercrime and fraud in the United Kingdom. To this end, the article begins by describing the changes in routine activities in the United Kingdom and how these may have influenced cybercrime and fraud opportunities. Subsequently, a brief overview of the existing literature on the relationship between crime and COVID-19 is provided. Next, the data and the methods are introduced. A detailed description of the results comprises the penultimate section of the article. Finally, discussion and conclusions are provided with regard to the implications of the findings for policy, practice, and academic debate.

COVID-19 and Shifts in Crime Opportunities

COVID-19 and Routine Activities in the United Kingdom

The unprecedented rapid changes in routine activities brought about by COVID-19 and the associated lockdown measures have been evidenced around the globe. In the

United Kingdom, the first national lockdown came into force on March 26, 2020, and most national-level restrictions were lifted on June 23 and eased further on August 14. Local lockdowns were announced for areas with high levels of COVID-19 cases from July 4 onwards (local restrictions were later renamed under a three-tier system from December 2). The second national lockdown took place from November 5 until December 2, and the third national lockdown was announced on January 6, 2021. Figure 1 visualizes the changes in mobility as documented by Google (2020) in their "UK COVID-19 Community Mobility Reports," based on user location data between mid-February and the end of July 2020, which is the period analyzed in this research. In this regard, Figure 1a, 1b, and 1d highlight the notable drop in work, recreation and retail, and transit mobility, respectively, in comparison to baseline measurements of the median value for the corresponding day of the week, during the 5 weeks between January 3 and February 6, 2020. On the contrary, Figure 1c illustrates a clear rise in mobility trends for places of residence. As can be observed in the plots, the most pronounced changes occurred around March 23, which was the date the United Kingdom announced the first strict lockdown measures.

The Office for National Statistics (ONS) provides support for these trends. They found that in April 2020, over 40% of U.K. workers did some work from home as a result of the coronavirus pandemic (ONS, 2020a). They also found that in the period between April and June, the total hours worked in the United Kingdom was approximately 20% less than in the previous 3 years (ONS, 2020b). These findings indicate a reduction in mobility, a rise in teleworking, and an increase in leisure time. Similarly, the ONS highlighted a change in retail activities with many physical retail stores reporting decreased footfall but online sales showing a 46.8% increase between February and April 2020 (ONS, 2020d). This ties in with data on United Kingdom and global internet use. Ofcom (2020) found a notable increase in the time adults spend online in April 2020 in comparison to September 2019. The London Internet Exchange showed a pronounced spike in internet traffic between March 11 and March 28, far greater than any spike in the upward trend of previous years (see original data from https://portal.linx.net/stats/lans). Traffic decreased from April to August 2020 but generally remained above the levels found before coronavirus. Finally, Datavault's Broadband Insights reports for 2020 (OpenVault, 2020) and their COVID-19 Broadband Impact Tracker (available from https://openvault.com/trusted/) detail increases in global broadband use by both individuals and businesses that were above the general rising trend found in previous periods, especially in the months of March and April 2020.

COVID-19, Routine Activities, and Traditional Crime

For several decades, criminologists have studied trends in routine activities and how these can shape criminal opportunities. Cohen and Felson (1979) formulated this as the Routine Activity Approach and stated that crime occurs when likely offenders and

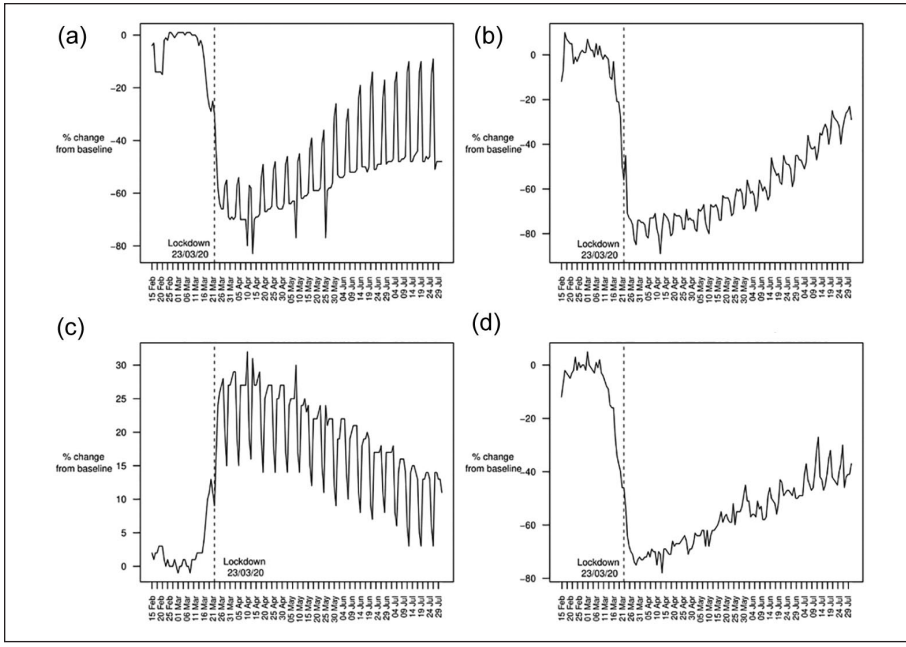


Figure 1. Changes in U.K. mobility February to July 2020: (a) workplace mobility, (b) retail and recreation mobility, (c) residential mobility, and (d) transist stations mobility.
Source. Produced by authors with data from Google Community Mobility Reports.

suitable targets converge in both space and time in the absence of capable guardians. Employing longitudinal data from the 1950s to the 1970s, these authors identified that changes in household structures and activities after World War II, such as the increasing proportion of females in the workforce or the greater number of single-adult households, reduced people's capacity to serve as capable guardians and correlated positively with homicide, forcible rape, aggravated assault, robbery, and burglary. They postulated, for example, that the increase in ownership of valuable and movable goods combined with the increase in the time homes were unattended during the day increased the opportunities for burglary. In Europe, the Routine Activity Approach, often combined with lifestyle theory (Hindelang et al., 1978), has been used to explain crime trends since the 1990s, putting special emphasis on how the development of the internet led to a shift from offline to online and hybrid crimes (Aebi & Linde, 2010, 2014; Caneppele & Aebi, 2019).

Given the huge changes in routine activities in the United Kingdom detailed in the previous section, it was not surprising that criminal opportunities saw marked changes during 2020 (Stickle & Felson, 2020). In this sense, several authors have examined the effects of COVID-19 and related containment measures on traditional crime around

the globe using a variety of statistical techniques (e.g., Felson et al., 2020; Gerell et al., 2020; Piquero et al., 2020). Many studies employing time-series analysis techniques, such as Autoregressive Integrated Moving Average (ARIMA) models, have found an overall reduction in crime but notable differences in trends between crime types (e.g., Ashby, 2020; Campedelli & Favarin, 2021; Estévez-Soto, 2020; Hodgkinson & Andresen, 2020; Langton et al., 2021; Mohler et al., 2020; Payne et al., 2020). Even the prison population rates in European countries that introduced lockdowns were affected by a decrease in the number of entries of remand detainees and sentenced prisoners (Aebi & Tiago, 2020).

COVID-19, Routine Activities, and Cybercrime and Fraud

Prior to COVID-19, academic research had already noted how changes in offline and online routine activities are associated with a shift in crime opportunities from physical space to cyberspace (Miró-Llinares & Moneva, 2019; Newman & Clarke, 2003; Pyrooz et al., 2015). The popularization of the internet has changed work and leisure activities meaning criminals may dedicate more time to online crimes, such as certain types of cyber-enabled fraud. Indeed, studies have found that overall increases in fraud are being driven by pronounced upward trends in fraud with a "cyber" element (Kemp et al., 2020). Given the already existing association between the expansion of the internet and digital platforms and the growth in online criminal opportunities, it seems likely that the boost in online activity since March 2020 is correlated with a similar boost in online crime.

Researchers started exploring this relationship after the first lockdown measures were announced in March 2020. For example, Collier et al. (2020) described an increase in certain cybercrimes such as denial of service attacks and an increase in opportunities for fraud globally. They observed that cybercriminals were mainly adapting already existing attack strategies to exploit psychological effects of the pandemic, for example, higher levels of fear. Similarly, Vu et al. (2020) examined underground cybercrime markets during the pandemic, finding a significant increase in the volume of products involved, but they studied no notable differences in the types of transactions, users, or behaviors in the markets. Payne (2020) used data from the U.S. Federal Trade Commission to identify an overall increase in reported fraud cases in the first 3 months of 2020 in comparison to the same period in 2019. A significant increase in losses from fraud in the same period was also highlighted. However, the growth was not the same across all fraud types or all age groups, with the author noting marked upticks in frauds connected to the internet, such as imposter businesses, fraudulent text messages, online shopping complaints, counterfeit checks, and romance scams. Disparities between crime victims were also found by Buil-Gil et al. (2021b) in their preliminary analysis of reported cybercrime and fraud in the United Kingdom. Despite detailing statistically significant changes between May 2019 and May 2020 in most

fraud and cybercrime categories as well as for the total number of reports, they highlighted differences in trends between organizational victims (a slight nonsignificant decrease in cyber-dependent crime and a slight increase in online fraud) and individual victims (an overall significant increase). This may be related to distinct variations in routine activities or reporting practices between these types of victims (see also Department for Digital, Culture, Media and Sport, 2021). Finally, Hawdon et al. (2020) employed online panel surveys to measure cybercrime victimization during the pandemic. Surprisingly, they found little change between the pre-COVID and COVID samples; however, the overlapping question periods between the two samples mean these results should be interpreted with caution.

The Present Research

Despite the existing research primarily indicating an increase in cybercrime and fraud during the pandemic, there is a lack of time-series analysis as found in the literature on COVID-19 and more traditional crime types. This study aims to start filling this gap by applying ARIMA models, which are explained in greater detail in section "Analytic Strategy," to analyze trends in cybercrime and fraud known to the police in the United Kingdom. In the review of the literature set out in section "COVID-19 and Shifts in Crime Opportunities," it was identified that many crime types have been significantly affected by the mobility restrictions associated with COVID-19, and it was noted that cybercrime and fraud are generally believed to have increased during the pandemic. However, pre-COVID literature on fraud has shown that offline variants of fraud appear to be declining in recent years, while cyber-enabled fraud types are increasing (Kemp et al., 2020; Levi, 2017; Tcherni et al., 2016). In addition, law enforcement, government agencies, and academic studies have highlighted that the changes in routine activities during the pandemic have not had identical effects on cybercrime and fraud victimization of individuals and organizations (Buil-Gil et al., 2021b; Department for Digital, Culture, Media and Sport, 2021; Interpol, 2020). Based on these conclusions from prior research, the following hypotheses have been formulated for this study:

Hypothesis 1 (H1). Changes in cybercrime and fraud during the first months of the COVID-19 pandemic were greater than expected crime variability.
Hypothesis 2 (H2).Traditional offline fraud decreased during the first months of the COVID-19 pandemic while cyber-enabled fraud increased.
Hypothesis 3 (H3). Increases in victimization by cybercrime and cyber-enabled fraud during the first months of the COVID-19 pandemic were greater for individuals than for organizations.

Data

Crime data. The data on cybercrime and fraud used in this study were obtained via a freedom of information request to the City of London Police who, alongside the

National Fraud Intelligence Bureau, run *Action Fraud*, the United Kingdom's national reporting center for fraud and cybercrime. Data on individual and organizational victims were received for each month from April 2017 to July 2020. It was not possible to choose another date for the beginning of the analyses because records disaggregated by victim type and month are only available from April 2017. Due to resource limitations and the provisions of the Freedom of Information Act, the City of London Police were unable to provide data for reports for all crime types recorded by Action Fraud, thus, the following six types were obtained:

- Total cybercrime: In accordance with the Home Office Counting Rules (Home Office, 2020), this category comprises computer virus/malware/spyware; denial-of-service attacks (with or without extortion); hacking of personal computer; hacking of social media and email; hacking of PBX/dial through; and hacking combined with extortion.
- Total fraud: This includes all 46 of the fraud types in accordance with the aforementioned Home Office Counting Rules.
- Online shopping and auction fraud: The Home Office defines this category as "fraud attributable to the misrepresentation of a product advertised for sale through an internet auction site or the non-delivery of products purchased through an internet auction site." This fraud was chosen as one of the individual fraud types for two reasons. On one hand, as illustrated by its name, the internet plays an essential role in its commission. On the other hand, it was considered that online shopping and auction fraud is a crime that should affect both individuals and organizations, thereby permitting comparisons between them.
- Dating fraud: In this type of fraud "the intended victim is befriended on the internet and eventually convinced to assist their new love financially by sending them money for a variety of emotive reasons." This was also requested because the internet plays an essential role in its commission, especially when the typical physical places for meeting a potential partner, such as pubs or nightclubs, are closed or restricted during lockdown.
- Ticket fraud: This category "involves the victim purchasing tickets remotely e.g., over the phone or internet." Data on this fraud were solicited because although often cyber-enabled, the opportunity to commit ticket fraud is created by the desire to carry out activities in the physical world. This crucial link to the physical world allows analysis of the connection between activities in physical space and crime in cyberspace.
- Door-to-door sales and bogus tradesmen fraud: This is one of the only crimes in the *Action Fraud* data that they consider not cyber-enabled and that is committed in relatively large numbers (more than 1,000 cases per year).

Data on crime reports submitted to *Action Fraud* which contain a valid postcode address in England, Wales, Scotland, or Northern Ireland were received by authors and will be used in this research.[2]

Routine activities data. To further explore the influence of COVID-19 on crime opportunities, it was considered relevant to examine whether routine activities that are potentially linked to fraud opportunities followed a similar trend to reported fraud. Although historical data are scarce, some sources were identified that could be analyzed with the same methods as the crime data to show the potential impact of the pandemic on activities potentially related to crime opportunities. First, the ONS (2020c) collects data on retail activities; in particular, data on the value of sales conducted via the internet. Shopping online has been identified as a potential predictor of online fraud victimization (e.g., Leukfeldt & Yar, 2016; Reyns & Henson, 2016). On the contrary, some sources publish information regarding ticket sales, which is likely related to ticket fraud. In this sense, data from the Civil Aviation Authority (2020) show the number of air passengers that pass through U.K. airports, which provides an indication of the effects of COVID-19 on air ticket sales in the United Kingdom. In addition to this evidence of changes in tickets related to mobility, monthly cinema admissions provided by the UK Cinema Association (2020a, 2020b) serve as an indication of changes in leisure activities.

Analytic Strategy

To test the three hypotheses posed at the beginning of section "The Present Research," univariate ARIMA models were applied to the *Action Fraud* data described in the previous section. ARIMA models are a method for time-series data analysis that employs past observations of one variable to predict its own future values. They are one of the most common approaches to time-series analysis (Hyndman & Athanasopoulos, 2018) and, as described in the review of the literature in section "COVID-19 and Shifts in Crime Opportunities," they have already been used to study the effects of COVID-19 on crime. To apply the ARIMA modeling approach in this article, the values were selected for crime reports each month up until lockdown was introduced in March 2020, that is, April 2017 to March 2020. This allowed computation of 95% prediction intervals for the time period up to March 2020, and subsequently, parameters obtained from ARIMA models were used to forecast 95% prediction intervals for crime from April 2020 to July 2020. This allowed the known values of crime for April to July 2020 to be compared to the 95% prediction intervals to identify whether the known values of crime fall within the 95% prediction intervals given by the parameters from pre-COVID models.

To select the ARIMA model with the best goodness-of-fit for each variable under study (i.e., crime types and types of victims), we followed a variation of the Hyndman–Khandakar algorithm (see Hyndman & Khandakar, 2008) that automates the selection of the components p (i.e., the order of the auto-regressive model), d (i.e., the order of differencing), and q (i.e., the order of the moving average) of each ARIMA model estimated for each variable. This approach uses a stepwise search to

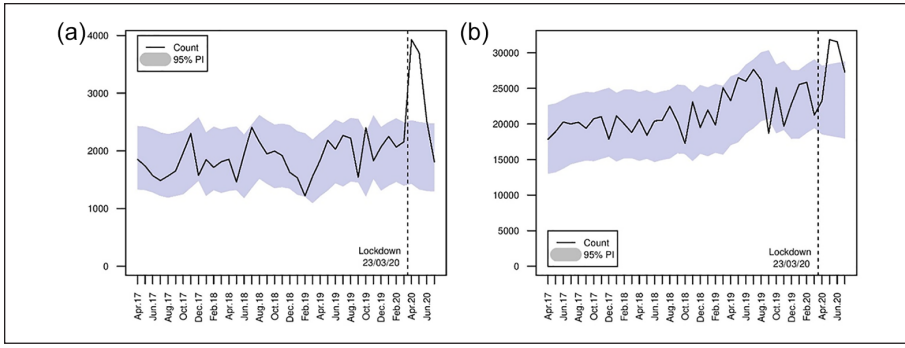


Figure 2. ARIMA forecast and actual count of recorded cybercrime and fraud in the United Kingdom, April 2017 to July 2020: (a) recorded cybercrime and 95% prediction intervals and (b) recorded fraud and 95% prediction intervals.

select the model with the lowest AICc, a bias-corrected version of the Akaike Information Criterion (AIC) for small sample sizes, in each case. This is done to effectively select the best model for each variable in our data, and in turn improve the forecast accuracy of the ARIMA models. The auto.arima() function from the "forecast" package (Hyndman, 2020) in *R* (R Core Team, 2020) was used to implement the Hyndman–Khandakar algorithm to estimate a univariate time-series ARIMA model for each of the crime types described above. *R* codes used in this research can be found in the Supplemental Material. Moreover, an interactive data visualization tool has been created to allow readers to visualize bivariate associations between crimes known to the police and changes in routine activities in the United Kingdom (see: https://asiermoneva.shinyapps.io/trends_app/).

Results

Total Cybercrime and Fraud

Figure 2 plots the 95% prediction interval for total cybercrime and total fraud from the corresponding ARIMA models as well as the actual count of recorded offenses for the period April 2017 to July 2020. As can be observed in Figure 2a, in March, April, and May 2020, total recorded cybercrime was markedly greater than the levels forecast based on the data from the previous 3 years. This 3-month period witnessed a sharp spike in recorded cybercrime that dropped back to within the 95% confidence interval in June and July. Similarly, though with a slight delay in comparison to cybercrime, Figure 2b shows total recorded fraud also increased clearly beyond the bounds of the prediction interval in May and June 2020 and then bounced back to the original trend in July.

With regard to H1, based on the application of the ARIMA models to historical data of recorded cybercrime and fraud in the United Kingdom, we can reject the null hypothesis and conclude that the changes in cybercrime and fraud during the first months of the COVID-19 pandemic were greater than the crime variability that would have been expected given historical trends.

Fraud Types

As set out in section "The Present Research," H2 posits that trends for different types of fraud were unlikely to be homogeneous during the first months of the pandemic; in particular, it states that online types are likely to have increased, and offline types are likely to have decreased. Figure 3 visualizes the range of values forecast from the historical series as well as the known count rates for the four individual fraud types analyzed in this research. First, Figure 3a shows a steep increase in recorded online shopping and auction fraud in March, April and May 2020 that is far beyond the values that would be expected 95% of the time in accordance with the ARIMA prediction intervals. The number of recorded offenses then dropped back down in June and July but remained outside the range of predicted values. Figure 3b indicates a similar trend with regard to dating fraud: a pronounced increase immediately subsequent to the introduction of lockdown measures in the United Kingdom. However, in contrast to online shopping fraud, this is followed by what appears to be a return to the less steep historical upward trend in June and July. In Figure 3c, we can discern that the trend for ticket fraud is the inverse of that observed for the previous two fraud types. Ticket fraud appears to have a seasonal pattern, with higher levels of recorded crime in spring and summer than in winter and autumn in the 3 years prior to 2020. However, recorded ticket fraud during the first months of the COVID-19 pandemic was reduced to close to zero. In April, May, June, and July 2020, it was below the prediction interval and far below the numbers recorded in the spring and summer of 2017, 2018, and 2019. Finally, as shown in Figure 3dp, door-to-door frauds were on a downward trend from April 2017. This trend appears to have continued during the pandemic with a notable drop in April 2020; however, the reduction in this fraud type was within the prediction interval forecast by the ARIMA model.

Thus, based on the analysis of these four individual fraud types, the null hypothesis with regard to H2 is not rejected because even though the cyber-enabled online shopping fraud and dating fraud did increase, ticket fraud, which is also cyber-enabled but dependent on events that take place in physical spaces, decreased. As such, it appears not all cyber-enabled frauds have been affected in the same manner by the mobility restrictions associated with the pandemic. Furthermore, the decline in door-to-door sales fraud identified in this study follows the pre-COVID downward trend and the variability during the first months of the pandemic is not beyond the 95% prediction intervals.

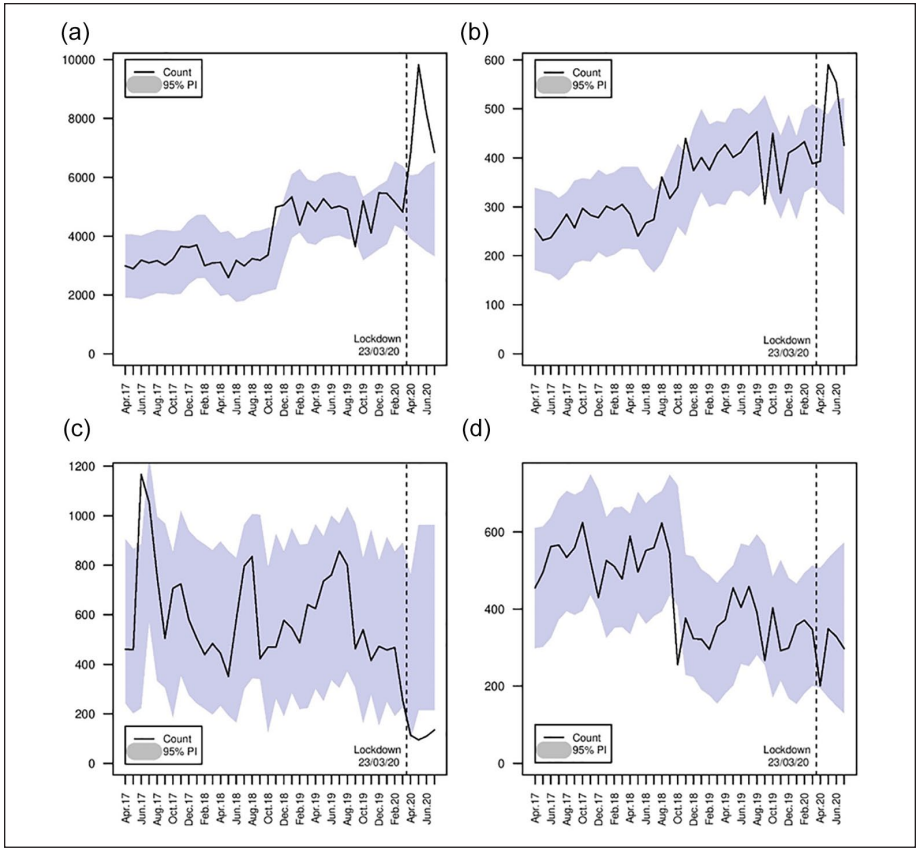


Figure 3. ARIMA forecast and actual count of four fraud types in the United Kingdom, April 2017 to July 2020: (a) online shopping fraud, 95% PI, (b) dating fraud, 95% PI, (c) ticket fraud, 95% PI, and (d) door-to-door fraud, 95% PI.

Some data sources offer support for routine activities explanations regarding the disparities in the direction of certain fraud trends. For example, as can be identified in Figure 4a, the value of internet retail sales (ONS, 2020c) followed a markedly similar trend to online shopping and auction fraud from March 2020. There was a sharp increase in the value of sales that were conducted online, far beyond the forecast values based on historical data, and sales may have been beginning to return to closer to the original trend in July. Similarly, regarding ticket sales, data from the Civil Aviation Authority (2020) plotted in Figure 4b demonstrate the drastic effects of COVID-19 on air travel as the number of passengers passing through U.K. airports plummeted

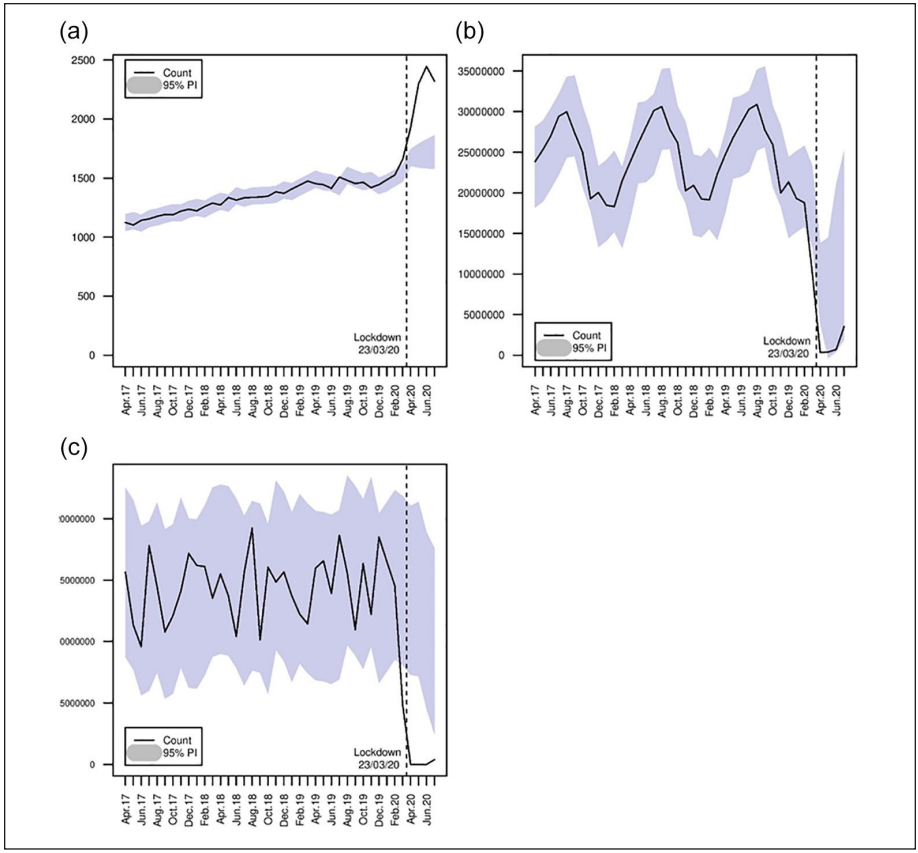


Figure 4. ARIMA forecast and actual count of routine activities, April 2017 to July 2020: (a) mean internet weekly sales in GBP million, 95% PI, (b) .passengers from all U.K. airports, 95% PI, and (c) U.K. monthly cinema admissions, 95% PI.

between March and April. However, since the number of passengers began to drop before lockdown measures were launched in the United Kingdom, ARIMA prediction intervals were able to capture the observed values of air passengers in May, June, and July. This reduction in passengers at U.K. airports before the introduction of lockdown measures in United Kingdom may be due to the fact other regions of the world introduced restrictions before the United Kingdom and/or owing to U.K. passengers reducing air travel as a consequence of the already rising threat of the pandemic. In any case, the air passenger data serve as an indication of changes in tickets sales related to mobility for the period under analysis. In addition, monthly cinema admissions provided by the UK Cinema Association (2020a, 2020b) indicate enormous changes in ticket sales related to leisure activities. Figure 4c shows cinema admissions reached zero for the months with the strictest lockdown measures. In short, both these data

sources that are related to ticket sales show very steep declines between March and April 2020, similar to that identified in recorded ticket fraud victimization. The relationship between shifts in routine activities and shifts in crime opportunities is discussed in greater detail in section "Conclusion."

Cybercrime and Fraud Suffered by Individuals and Organizations

To test whether increases in victimization by cybercrime and cyber-enabled fraud during the first months of COVID-19 were greater for individuals than for organizations, as outlined in H3, this article also enquires about potential divergences between individual and organizational victims. In this sense, the *Action Fraud* data appear to indicate certain contrasts. Figure 5 details the prediction intervals and known counts of reported victimization for total cybercrime, total fraud, as well as online shopping and auction fraud (abbreviated as online shopping fraud in Figure 5e and f). Before proceeding to examine the results, three points should be noted. First, City of London Police stated that disaggregated data for the two victim types are unavailable for October and November 2018. This can be observed by the gap in the time-series plots. Second, the ARIMA models were not applied to dating fraud, ticket fraud, and door-to-door sales fraud because the sample size of organization victims was so small that the ARIMA models could not be correctly estimated. Third, data about crimes suffered by organizations show unusual, very small values in December 2018, and January and February 2019. This is likely to be due to inconsistencies in recording, rather than actual changes in crime, but this does not have a major impact on the ARIMA models' forecast accuracy.

With regard to cybercrime, Figure 5a and b shows a difference in reported offenses between individuals and organizations. The spike found in individual cybercrime victimization is not present in the results for organizational victims, which remain firmly within the 95% prediction intervals for the period after the introduction of lockdown measures. There is a similar discrepancy in relation to total fraud in Figure 5c and d. The post-lockdown jump in fraud reported by individuals is not found for organizational victims in terms of values greater than the forecast prediction intervals. In this sense, while there was an increase in reported fraud in May and July 2020, this did not go beyond the ARIMA prediction intervals. Finally, Figure 5e and f show both a concordance and a divergence with respect to online shopping and auction fraud. On one hand, reported victimization climbs steeply for both individuals and organizations after the onset of the COVID-19 pandemic. On the other hand, the rise in cases reported by individuals took place in April and May 2020 and then dropped back, while reports by organizations rose slowly from April to June and then rocketed in June and July.

As a consequence of the aforementioned results for individual and organizational cybercrime and fraud victims, H3 cannot be rejected and it can be stated that cybercrime and fraud victimization trends for individuals exceeded the upper limits of the expected volume as opposed to victimization trends for organizations, which only exceeded the prediction in the case of online shopping fraud.

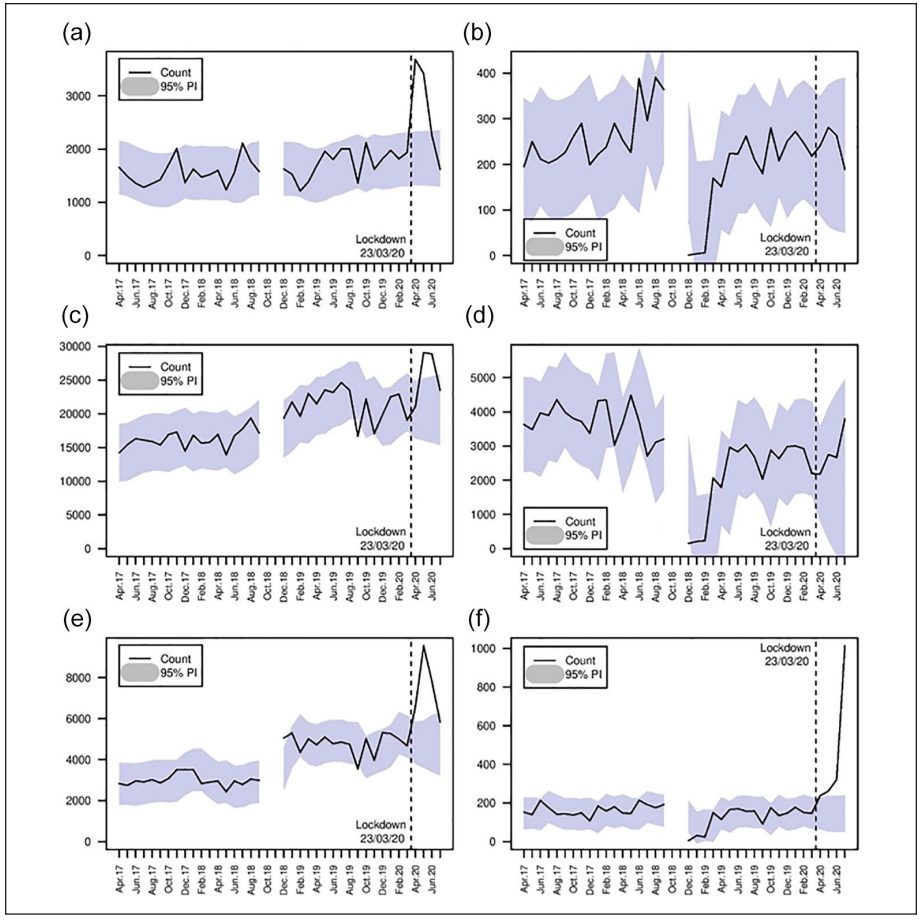


Figure 5. ARIMA forecast and known count of individual and organization cybercrime and fraud victims in the United Kingdom, April 2017 to July 2020: (a) cybercrime (individual victims), (b) cybercrime (organization victims), (c) fraud (individual victims), (d) fraud (organization victims), (e) online shopping fraud (individual victims), and (f) online shopping fraud (organization victims).

Discussion

In his address to the Annual Meeting of the American Society of Criminology 2017, Rosenfeld (2018) advocated research on the impact of exogenous shocks on crime rates with the aim of testing theoretical expectations in criminology. In contemporary times, there has been no event that has affected crime opportunities as greatly in such a short period of time as the COVID-19 pandemic. While its devastating impacts have been felt by millions, criminologists have been presented with an unprecedented situation to study how short-term shocks to society affect crime trends.

Changes in mobility are arguably one of the most important variables to explain the convergence of the minimum elements of crime, as stated in the Routine Activity Approach (Cohen & Felson, 1979). However, it is also among the most difficult variables to control for. National lockdowns in response to the pandemic created a natural experiment to capture this variable through time spent at home (Stickle & Felson, 2020). Building on previous research (Aebi & Linde, 2010, 2014; Caneppele & Aebi, 2019; Newman & Clarke, 2003; Pyrooz et al., 2015), Miró-Llinares and Moneva (2019) stressed the importance of time spent at home as an explanatory factor in the shift of criminal opportunities from physical space to cyberspace. In that piece, emphasis was placed on the growing adoption of online forms of entertainment, such as online shopping, streaming content, TV series, or computer games, to the detriment of traditional leisure in parks, bars, and streets. Yet the result regarding the convergence of offenders, targets, and guardians is the same as that caused by lockdowns: more time at home and less time on the street. In other words, empty streets and a busy internet.

This article has shown, however, that the opportunity structures for fraud are nuanced and that the reductions in offline routine activities during the pandemic are associated with disparate effects on distinct cyber-enabled fraud types. As we have seen, less offline retail activity appears related to more online activity and, consequently, more online shopping fraud. On the contrary, less ticket-related offline leisure and transport activities led to a decrease in ticket fraud. In this sense, ticket fraud provides an interesting example of online opportunity structures being affected by offline changes in routine activities; it demonstrates how a decline in activities in the physical world can also reduce opportunities for cyber-enabled frauds. Crime science (Clarke, 2010) and problem-oriented policing (Goldstein, 1979) have promoted the benefits of crime specificity for crime analysis since long before the current health crisis (e.g., Andresen & Linning, 2012; O'Connor & Grant, 1998; Read & Tilley, 2000), and recent research has urged the study of particular offenses with respect to crime patterns and the pandemic (Stickle & Felson, 2020). As a consequence of the discrepancies found in this study, a crime-specific approach to fraud and cybercrime research and prevention appears more urgent than ever.

Similarly, reported cybercrime and fraud evolved differently for organizational and individual victims. The reduced activity in the physical world was associated with marked effects on the general trends for the latter but had little effect on the former. This raises at least three pertinent yet distinct possibilities. First, it could be that with many businesses closed, opportunities to attack organizations were in fact reduced rather than increased. It has been widely stated that attacks against organizations have risen during COVID-19 (Europol, 2020a; Interpol, 2020), but it may be that such a general statement is overly simplistic and greater crime, victim, or country, specificity is required when researching trends in cybercrime and fraud against organizations. In fact, academic literature has begun to examine the organizational characteristics related to cybercrime and fraud victimization (Buil-Gil et al., 2021a; Rantala, 2008; Williams et al., 2019) and future research could examine this within the context of COVID-19. Second, it is unclear to what extent the divergences in individual and

organizational victimization during the pandemic are the result of differences in reporting. It seems plausible that with many organizations experiencing great changes to their daily functioning, many attacks went undetected and, thus, unreported (Department for Digital, Culture, Media and Sport, 2021). The move to teleworking in many industries may have impeded organizations' ability to detect and respond to cybercrime and fraud events. This would highlight the crucial role of teleworking individuals as "guardians" for their organizations with regard to cybercrime and fraud. In this sense, the peak in online shopping fraud in July 2020 may be due to IT services reporting all undetected offenses from previous months. Or, third, could it be that the difference in victimization rates found in this article is evidence of increased homeworking shifting risk onto the individual and away from the organization (e.g., spam and computer viruses being received in personally owned laptops instead of business computers)? Is a target being placed on under-protected individuals as opposed to organizations with IT support? This seems unlikely, given the potentially greater spoils available to criminals who target organizations, but nevertheless further research is required.

Finally, further discussion is also necessary on the apparent return to longer-term trends identified in many of the general and specific crime types analyzed in this article. This coincides with the Google Mobility Data discussed in section "COVID-19 and Shifts in Crime Opportunities" and the internet retail sales data in "Results" section, which seem to show a slow return to routine activities that are closer to pre-COVID levels. This is an indication of the potentially fundamental role of crime opportunities even in the short-term and compels future research on the criminal actors that are taking advantage of the changes in opportunity structures. Was it already existing offenders who simply increased their offending during spring and early summer 2020 or did new actors enter the market inspired by the new opportunities? Given the partial return to the general trend rather than sustained increases, as well as the prior research that has highlighted adaptations of existing attack vectors to take advantage of the social and psychological turmoil created by COVID-19 (Collier et al., 2020; Europol, 2020b), it appears that the first option is more likely. Nevertheless, further analysis in this sense could add to wide-ranging theoretical debates on cybercrime, fraud, and opportunity approaches.

Conclusion

This article contributes to the growing body of research on the impact of COVID-19 on crime by showing that, in the United Kingdom, overall counts of reported cybercrime and fraud in the period immediately after the introduction of lockdown measures were notably higher than predicted by the time-series technique applied in this research. However, and importantly for policy and practice, these general trends were not homogeneous throughout all fraud types or when comparing individual and organizational victims. Many spikes in cybercrime and fraud identified at the beginning of the pandemic appear to have later dropped back to the longer-term gentler upward

trend. All these conclusions open the door to future research as discussed in the previous section.

In reaching these conclusions, the present research is not without limitations. Notably, the secondary data used are the result of cybercrime and fraud offenses reported to the relevant law enforcement body and collated by *Action Fraud*. On one hand, the low levels of fraud and cybercrime reporting (Correia, 2019; Kemp, 2020; ONS, 2020c) mean that there may be a significant dark figure that is not accounted for in these figures. On the other hand, the methods for registering crime may vary across time, which could distort historical analysis. Despite these rather typical limitations with the official crime data, the results and conclusions contained herein can help inform future research and practice with regard to changes in routine activities and the consequent shifts in crime opportunities.

Acknowledgments

The authors would like to thank the City of London Police and U.K. Action Fraud for sharing the data used in this study.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Supplemental Material

Supplemental material for this article is available online. (file:///C:/Users/GDhonsi/OneDrive%20-%20SAGE%20Publishing/Desktop/1_EmptyStreetsBusyInternet_Appendix.html.html).

Notes

1. "Cyber-enabled" fraud refers to fraud types that existed before the internet but that are now mainly committed via information and communication technologies as this allows them to increase in scale and reach (McGuire & Dowling, 2013). For example, online shopping fraud.
2. Authors received no information about the proportion of reports associated with invalid or unknown postcode addresses (which *Action Fraud* removed before sharing the data). Thus, it is not known how many reports were removed from the data set due to not containing a valid address. To ensure that using data with removed reports does not have a large impact on our results, we accessed the *Action Fraud* open data dashboard for crimes recorded in the last 13 months (https://www.actionfraud.police.uk/data), downloaded available monthly records of cyber-dependent crime, fraud, and online shopping fraud from May 2019, and calculated the percentage difference and the Pearson's correlation coefficient

between the open data published by *Action Fraud* and data received via freedom of information request. The average difference between cyber-dependent crimes reported in the open-data portal and cyber-dependent crimes received was −6.07%, while this difference was −8.73% for total fraud and −9.98% for online shopping fraud. Correlation coefficients between the monthly aggregates of crime based on data received and data available from the open-data portal were significant and moderate/large in all three cases (i.e., cyber-dependent crime: $r = .87$, p value $< .001$; total fraud: $r = .51$, p value $< .05$; online shopping fraud: $r = .87$, p value $< .001$), showing that monthly aggregates of crime before and after removing reports with invalid addresses are linearly related and defined by a very similar distribution and rank. This was further analyzed using visualizations. The moderate correlation coefficient observed for total fraud is likely to be explained by the small number of months examined in this sensitivity analysis (15 months). Thus, data received allow analysis of trends of crimes reported to *Action Fraud*.

References

Aebi, M. F., & Linde, A. (2010). Is there a crime drop in Western Europe? *European Journal on Criminal Policy and Research*, *16*(4), 251–277. https://doi.org/10.1007/s10610-010-9130-y

Aebi, M. F., & Linde, A. (2014). The persistence of lifestyles: Rates and correlates of homicide in Western Europe from 1960 to 2010. *European Journal of Criminology*, *11*(5), 552–577. https://doi.org/10.1177/1477370814541178

Aebi, M. F., & Tiago, M. M. (2020). *Prisons and prisoners in Europe in pandemic times: An evaluation of the medium-term impact of the COVID-19 on prison populations*. Council of Europe and University of Lausanne. https://wp.unil.ch/space/files/2020/06/Prisons-and-the-COVID-19_200617_FINAL.pdf

Andresen, M. A., & Linning, S. J. (2012). The (in)appropriateness of aggregating across crime types. *Applied Geography*, *35*(1–2), 275–282. https://doi.org/10.1016/j.apgeog.2012.07.007

Ashby, M. P. J. (2020). Initial evidence on the relationship between the coronavirus pandemic and crime in the United States. *Crime Science*, *9*(1), Article 6. https://doi.org/10.1186/s40163-020-00117-6

Buil-Gil, D., Lord, N., & Barrett, E. (2021a). The dynamics of business, cybersecurity and cyber-victimization: Foregrounding the internal guardian in prevention. *Victims & Offenders*, *16*(3), 286–315. https://doi.org/10.1080/15564886.2020.1814468

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021b). Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK. *European Societies*, *23*(S1), 47–59. https://doi.org/10.1080/14616696.2020.1804973

Campedelli, G. M., Aziani, A., & Favarin, S. (2021). Exploring the effects of COVID-19 containment policies on crime: An empirical analysis of the short-term aftermath in Los Angeles. *American Journal of Criminal Justice*, *46*, 704–727. https://doi.org/10.1007/s12103-020-09578-6

Caneppele, S., & Aebi, M. F. (2019). 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

Civil Aviation Authority. (2020). *Airport data 2020* [Data file]. https://www.caa.co.uk/Data-and-analysis/UK-aviation-market/Airports/Datasets/UK-Airport-data/Airport-data-2020-01/

Clarke, R. V. (2010). Crime science. In E. M. McLaughlin & T. Newburn (Eds.), *The SAGE handbook of criminological theory* (pp. 271–283). Sage. https://doi.org/10.4135/9781446200926

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588–608. https://doi.org/10.2307/2094589

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

Correia, S. G. (2019). Responding to victimisation in a digital world: A case study of fraud and computer misuse reported in Wales. *Crime Science*, *8*, Article 4. https://doi.org/10.1186/s40163-019-0099-7

Department for Digital, Culture, Media and Sport. (2021). *Cyber Security Breaches Survey 2021*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/972399/Cyber_Security_Breaches_Survey_2021_Statistical_Release.pdf

Estévez-Soto, P. R. (2020). Crime and COVID-19: Effect of changes in routine activities in Mexico City. *Socarxiv*. https://doi.org/10.31235/osf.io/3jfwu

Europol. (2020a). *Internet Organised Crime Threat Assessment (IOCTA)*. https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

Europol. (2020b). *Pandemic profiteering. How criminals exploit the COVID-19 crisis*. https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis

Felson, M., Jiang, S., & Xu, Y. (2020). Routine activity effects of the Covid-19 pandemic on burglary in Detroit, March, 2020. *Crime Science*, *9*(1), Article 10. https://doi.org/10.1186/s40163-020-00120-x

Gerell, M., Kardell, J., & Kindgren, J. (2020). Minor covid-19 association with crime in Sweden. *Crime Science*, *9*(1), 19. https://doi.org/10.1186/s40163-020-00128-3

Goldstein, H. (1979). Improving policing: A problem-oriented approach. *Crime and Delinquency*, *25*(2), 236–258. https://doi.org/10.1177/001112877902500207

Google. (2020). *COVID-19 community mobility report. United Kingdom, 23 October 2020*. https://www.gstatic.com/covid19/mobility/2020-10-23_GB_Mobility_Report_en-GB.pdf

Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amid COVID-19: The initial results from a natural experiment. *American Journal of Criminal Justice*, *45*, 546–562. https://doi.org/10.1007/s12103-020-09534-4

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization*. Ballinger.

Hodgkinson, T., & Andresen, M. A. (2020). Show me a man or a woman alone and I'll show you a saint: Changes in the frequency of criminal incidents during the COVID-19 pandemic. *Journal of Criminal Justice*, *69*, 101706. https://doi.org/10.1016/j.jcrimjus.2020.101706

Home Office. (2020). *Home office counting rules for recorded crime: Fraud*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/881505/count-fraud-apr2-2020.pdf

Hyndman, R., Athanasopoulos, G., Bergmeir, C., Caceres, G., Chhay, L., O'Hara-Wild, M., Petropoulos, F., Razbash, S., Wang, E., & Yasmeen, F. (2020). *forecast: Forecasting functions for time series and linear models* (R package version 8.13). https://pkg.robjhyndman.com/forecast/

Hyndman, R. J., & Athanasopoulos, G. (2018). *Forecasting: Principles and practice* (2nd ed.). OTexts. https://Otexts.com/fpp2/

Hyndman, R. J., & Khandakar, Y. (2008). Automatic time series forecasting: The forecast Package for R. *Journal of Statistical Software*, *27*(1), 1–22. https://doi.org/10.18637/jss.v027.i03

Interpol. (2020). *Cybercrime: COVID-19 impact*. https://www.interpol.int/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf. Accessed 09/10/2020

Kemp, S. (2020). Fraud reporting in Catalonia in the Internet era: Determinants and motives. *European Journal of Criminology*. Advance online publication. https://doi.org/10.1177/1477370820941405

Kemp, S., Miró-Llinares, F., & Moneva, A. (2020). The dark figure and the cyber fraud rise in Europe: Evidence from Spain. *European Journal on Criminal Policy and Research*, *26*, 293–312. https://doi.org/10.1007/s10610-020-09439-2

Langton, S., Dixon, A., & Farrell, G. (2021). Six months in: Pandemic crime trends in England and Wales. *Crime Science*, *10*(6). https://doi.org/10.1186/s40163-021-00142-z

Leukfeldt, E. R., & 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

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: Overview and issues. *Crime, Law and Social Change*, *67*(1), 3–20. https://doi.org/10.1007/s10611-016-9645-3

McGuire, D. M., & Dowling, S. (2013). *Cyber-enabled crimes-Fraud and theft (Cyber crime: A review of the evidence Research Report 75)*. Home Office.

Miró-Llinares, F., & 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*(1), Article 12. https://doi.org/10.1186/s40163-019-0107-y

Mohler, G., Bertozzi, A. L., Carter, J., Short, M. B., Sledge, D., Tita, G. E., Uchida, C. D., & Brantingham, P. J. (2020). Impact of social distancing during COVID-19 pandemic on crime in Los Angeles and Indianapolis. *Journal of Criminal Justice*, *68*, 101692. https://doi.org/10.1016/j.jcrimjus.2020.101692

Newman, G. R., & Clarke, R. V. (2003). *Superhighway robbery*. Willan Publishing.

Nikolovska, M., Johnson, S. D., & Ekblom, P. (2020). "Show this thread": Policing, disruption and mobilisation through Twitter. An analysis of UK law enforcement tweeting practices during the Covid-19 pandemic. *Crime Science*, *9*, Article 20. https://doi.org/10.1186/s40163-020-00129-2

O'Connor, T., & Grant, A. C. (1998). *Problem-oriented policing: Crime-specific problems, critical issues and making POP work*. Police Executive Research Forum.

Ofcom. (2020). *Online Nation 2020—Summary report*. https://www.ofcom.org.uk/__data/assets/pdf_file/0028/196408/online-nation-2020-summary.pdf

Office for National Statistics. (2020a). *Coronavirus and homeworking in the UK: April 2020*. https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/bulletins/coronavirusandhomeworkingintheuk/april2020#measuring-the-data

Office for National Statistics. (2020b). *Labour market overview, UK: October 2020*. https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/bulletins/uklabourmarket/october2020#coronavirus-and-measuring-the-labourmarket

Office for National Statistics. (2020c). *Nature of fraud and computer misuse in England and Wales: year ending March 2019*. https://www.ons.gov.uk/peoplepopulationandcommu-

nity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2019

Office for National Statistics. (2020d). *Retail sales, Great Britain: August 2020*. https://www.ons.gov.uk/businessindustryandtrade/retailindustry/bulletins/retailsales/august2020

OpenVault. (2020). *Broadband Insights Report (OVBI)* (2Q 2020). https://telecompetitor.com/clients/openvault/2020/Q2/LP/index.html#:~:text=OpenVault%20Broadband%20Insights%20Report%20(OVBI)&text=The%20OVBI%20gains%20this%20insight,new%20normal'%20may%20look%20like

Payne, B. K. (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*, *45*, 563–577. https://doi.org/10.1007/s12103-020-09532-6

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

Piquero, A. R., Riddell, J. R., Bishopp, S. A., Narvey, C., Reid, J. A., & Piquero, N. L. (2020). Staying home, staying safe? A short-term analysis of COVID-19 on Dallas domestic violence. *American Journal of Criminal Justice*, *45*(4), 601–635. https://doi.org/10.1007/s12103-020-09531-7

Pyrooz, D. C., Decker, S. H., & Moule, R. K., Jr (2015). Criminal and routine activities in online settings: Gangs, offenders, and the Internet. *Justice Quarterly*, *32*(3), 471–499. https://doi.org/10.1080/07418825.2013.778326

Rantala, R. R. (2008). *Cybercrime against Businesses, 2005*. Bureau of Justice Statistics. https://www.bjs.gov/index.cfm?ty=pbdetail&iid=769

R Core Team. (2020). *R: A language and environment for statistical computing*. *R Foundation for Statistical Computing*. https://www.r-project.org/

Read, T., & Tilley, N. (2000). *Not rocket science? Problem solving and crime reduction. Crime Reduction Research Series Paper 6.* Home Office.

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International Journal of Offender Therapy and Comparative Criminology*, *60*, 1119–1139. https://doi.org/10.1177/0306624X15572861

Rosenfeld, R. (2018). Studying crime trends: Normal science and exogenous shocks. *Criminology*, *56*(1), 5–26. https://doi.org/10.1111/1745-9125.12170

Stickle, B., & Felson, M. (2020). Crime rates in a pandemic: The largest criminological experiment in history. *American Journal of Criminal Justice*, *45*(4), 525–536. https://doi.org/10.1007/s12103-020-09546-0

Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2016). The dark figure of online property crime: Is cyberspace hiding a crime wave? *Justice Quarterly*, *33*(5), 890–911. https://doi.org/10.1080/07418825.2014.994658

UK Cinema Association. (2020a). *Monthly admissions 2010-2019* [Data file]. https://www.cinemauk.org.uk/the-industry/facts-and-figures/uk-cinema-admissions-and-box-office/monthly-admissions

UK Cinema Association. (2020b). *Monthly admissions 2020* [Data file]. https://www.cinemauk.org.uk/the-industry/facts-and-figures/latest-uk-cinema-statistics/monthly-admissions/

Vu, A., Hughes, J., Pete, I., Collier, B., Chua, Y. T., Shumailov, I., & Hutchings, A. (2020, October 27–29). *Turning up the dial: The evolution of a cybercrime market through set-up,*

stable, and Covid-19 eras [Conference session]. ACM Internet Measurement Conference (IMC '20). https://doi.org/10.1145/3419394.3423636

Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2019). Under the corporate radar: Examining insider business cybercrime victimization through an application of routine activities theory. *Deviant Behavior*, *40*(9), 1119–1131. https://doi.org/10.1080/01639625.2018.1461786

Author Biographies

Steven Kemp is assistant lecturer in Criminology at the University of Girona and Miguel Hernández University of Elche, Spain, and research associate at University of Manchester, United Kingdom. His research focuses on fraud, cybercrime, white-collar crime, and crime reporting.

David Buil-Gil is lecturer in quantitative criminology at the University of Manchester, United Kingdom. His primary research interests are in crime data modeling, victimization surveys, measurement error in crime data, new methods for data collection, and cybercrime.

Asier Moneva is postdoctoral researcher at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), and The Hague University of Applied Sciences, Netherlands. His research focuses on cybercrime analysis and prevention from a situational perspective.

Fernando Miró-Llinares is professor of criminal law and criminology at Crímina at Miguel Hernández University of Elche, Spain. His research interests cover cybercrime, crime trends, environmental criminology, deterrence, and criminal law.

Nacho Díaz-Castaño is researcher at Crímina Research Center for the Study and Prevention of Crime at Miguel Hernández University of Elche, Spain. His primary research interests are in transnational crime.