Assessing the Effects of COVID-19 on Online Routine Activities and Cybercrime: A Snapshot of the Effect of Sheltering in Place

Troy Smith
The University of Trinidad and Tobago
E-Mail: *mr_t_smith@ymail.com*

Abstract

The study examined the changes in online routines, cybercrime rates and the applicability of the Routine Activities Theory (RAT) resulting from the COVID-19 pandemic. The RAT proposes that, upon the spatiotemporal convergence of an offender and target, a crime event results from an offender's rational but subjective assessment of a target's suitability and level of guardianship. The study used cybercrime victimisation data collected with a self-administered survey pre- and post-COVID-19 (N = 149 Facebook users of varying ages, ethnicities, and geographic locations within The Republic of Trinidad and Tobago). The change in online routine, cybercrime rate and their relationship to COVID-19 were assessed using Bayesian t-tests, χ^2-tests and Propensity Score Matching. Additionally, pre-and post-COVID-19 classification models were compared to identify any change in the utility of the RAT. The study found that there was a general increase in online routine activities particularly those resulting in increased time spent online and accessing pornographic content. Further, the predictors of victimisation changed, and the predictive accuracy of the classification model decreased. However, it was determined that cybercrime victimisation rates decreased post-COVID-19 and that the change had a causal dependence on the implementation of guardianship measures. The study concluded that increased use of technical guardianship measures such as the use of protective software and implementation of browser security protocols led to the decreased rate of victimisation, particularly as cybercrime shifted from interpersonal crimes to techno-centric cybercrimes. However, the study was limited due to the use of chain referral sampling and the fact that a control group could not be used because this was a global 'treatment'. The findings suggest that increased focus by policymakers on targeting hardening and removal measures through the implementation of technical guardianship and cyber-safety awareness and education can help reduce cybercrime victimisation. This study highlights the need for further research into motivations for protective online behaviour and the role of exogenous shocks in changing crime and behavioural patterns.

Keywords: COVID-19, cybercrime, online routines, guardianship

Dr Troy Smith *is a graduate of the Doctor of Philosophy programme offered by the Institute of Criminology and Public Safety, The University of Trinidad and Tobago. He is a scholar with multiple peer-reviewed articles and*

ongoing international projects focusing on the areas of cybercrime, problematic social media use and the effect of exogenous shocks on crime patterns. He also actively seeks to enhance research within the social sciences through the use of alternative statistical methods where appropriate; for example, the use of Bayesian analysis and Rasch measurement. He has over fourteen years of experience working in the area of national security in various specialty areas within Trinidad and Tobago. He is currently one of the directors of Research Analysis Inquiry and Development, a research non-profit entity focused on producing quality multidisciplinary research within the Caribbean.

Introduction

Based on the Routine Activities Theory (RAT), any phenomenon such as COVID-19 that leads to increased time at home, restricted access to public places, and increased dependency on online services will increase victimisation. When vaccines were still in the trial phase and infection in some cases increased exponentially, countries issued 'shelter in place' or 'stay at home' orders to control the spread of the virus (Gallagher, 2020; Smith & Teague, 2020; Stickle & Felson, 2020). While the COVID-19 pandemic is not believed to be a permanent state, it appears to be long-lasting with an undefined end state. Therefore, it is important to understand the effect it has had or is having on society. This study focuses on one aspect of its effect, which is cybercrime victimisation patterns.

There is empirical evidence presented by the extant literature which suggests that activities that increased time spent online intensifies the risk of cybercrime victimisation (Álvarez-García et al., 2019; Mesch & Dodel, 2018; Reyns et al., 2011; Rodriguez et al., 2017; Wick et al., 2017). Further, the RAT, which has been used to demonstrate the importance of online routine activities in predicting cybercrime risk, also dictates that routine activities are constrained by social and situational conditions (Cohen & Felson, 1979). Such a social or situational condition change is undoubtedly created by the COVID-19 pandemic, which has forced self- and government-imposed restrictions and changes in social domains such as social cohesion, communication, working patterns and mobility (Buil-Gil et al., 2020). Initial evidence suggests that crimes associated with being at home or extended personal contact have increased, such as domestic violence, intra-familial assaults, nuisance complaints and private parties with illegal drugs (Campedelli et al., 2020; Mohler et al., 2020). However, the recorded changes in other crimes have been inconsistent across categories, types, places, and timeframes (Stickle & Felson, 2020). Stickle and Felson (2020) highlighted the fact that a review of the post-COVID-19 literature shows that many criminological theories are struggling to explain the abrupt and often sweeping changes in crime patterns. Note that in this study 'post-COVID-19' refers to the period after the start of the pandemic rather than its cessation.

This study seeks to add to the extant literature by examining the pandemic's effect(s) on cybercrime victimisation and its relationship to human-centric factors as explained by the theoretical framework of the RAT. This study employs Bayesian methodologies given its advantages with smaller datasets, lack of dependence on the Central Limit Theorem, congruent performance between balanced and unbalanced datasets and the limited role of randomisation (Berchialla et al., 2019; Rudner, 2016). This research is significant as it adds to the lone study into the effect of a pandemic and specifically stay-at-home orders on cybercrime victimisation done by Hawdon et al., (2020), while adding additional statistical analysis. More importantly, it also adds to the limited data available on cybercrime victimisation within the Caribbean.

Literature Review

Routine Activities Theory (RAT)

The RAT has emerged as the prevailing theory in cybercrime research (Hsieh & Wang, 2018; Bossler & Berenblum, 2019). The theory proposes that crime occurs based on routine activities, which result in the spatio-temporal convergence of a suitable target, a motivated offender and a lack of capable guardianship (Cohen & Felson, 1979; Wick et al., 2017). Further, the theory provides a macro perspective of the relationship between social and situational conditions with the probability of a crime event (Howell et al., 2019; de Jong et al., 2019; Smith & Stamatakis, 2020). This study at the core examines the effect of the social and situational conditions resulting from the response to the COVID-19 pandemic, an exogenous shock, on the probability of a crime event. Therefore, the RAT's perspective on the relationship between social and situational factors with crime can provide a relevant theoretical framework for the examination of this phenomenon.

Researchers have applied RAT to a range of cybercrimes including unauthorised access, malware, romance scams, harassment, and cyber dating abuse (Bossler & Holt, 2013; Reyns, Henson & Fisher 2015; van Ouytsel, Ponnet & Walrave, 2018; Hawdon et al., 2019). Studies using the RAT have had mixed results as it relates to the selection, strength, and effect of predictors (Rodriguez et al., 2017; Choi, 2018; Sarre et al., 2018; Smith & Stamatakis, 2021). Although studies have shown some inconsistency, researchers have found that there are specific behaviours that increase the risk of victimisation (Logan, Walker, Jordan & Leukefeld, 2006; Turanovic, Pratt & Piquero, 2018; Hawdon et al., 2020). In general, routine activities that increase the time spent online, and those associated with risky/deviant behaviour and low self-control, increase the risk of victimisation (Hinduja & Patchin, 2009; Navarro & Jasinski, 2012; Leukfeldt & Yar, 2016; Reyns, Henson & Fisher, 2015; Rodriguez et al., 2017; Mesch & Dodel, 2018).

COVID-19 Potential to Constrain Routine Activities

The stay-at-home orders introduced to reduce the spread and 'flatten the curve' during the pandemic have had an irrefutable effect on citizens' routines. Citizens have been limited in when,

how often, and where they can go daily. As a result, human interaction, traditional leisure activities, and entertainment have been greatly reduced. Therefore, the world has been forced to seek new ways to connect and entertain themselves (Brathwaite, 2020; Buil-Gil et al., 2020). Market research indicates that since COVID-19 social media usage, online gaming and e-commerce increased dramatically from 0.4 million in January and 1.6 million in February to 20.3 million in March (Balram, 2020; Beech, 2020; Brathwaite, 2020; Hawdon et al., 2020; Koeze & Popper, 2020). Increases in cybercrime activity post-COVID-19 have been reported from various sectors (Brathwaite, 2020; Buil-Gil et al., 2020). However, reports by Interpol suggest that there has been a significant target shift from individuals to corporations, governments, and critical infrastructure (INTERPOL General Secretariat, 2020).

Cybercrime studies have relied heavily on traditional theories such as the RAT, which identify situations and opportunities as triggers of crime (Mesch & Dodel, 2018; Rodriguez et al., 2017). The routine activities that lead to situations or opportunities for a crime event are dependent on social and situational factors, which may include those resulting from the COVID-19 pandemic. Therefore, even before empirically assessing the framework, a researcher should be able to use the theory to explain the expected outcome given observed changes (Campedelli et al., 2020).

Researchers have demonstrated that the lifestyle of individuals, which are constrained by spatial factors define the probability of the spatio-temporal convergence of a motivated offender, suitable target and absence of capable guardianship required for a crime event to occur (Castells, 2002; Kitchin, 1998; Stein, 2011; van Wilsem, 2003; Yar, 2005). Hence, in theory, the COVID-19 pandemic's effect on routine activities due to social and societal changes has the potential to, directly and indirectly, change the probability of the spatio-temporal convergence of a motivated offender, suitable target and absence of capable guardianship in cyberspace (Hawdon et al., 2020). The following sections examine each tenet of the RAT and the possible effect that the COVID-19 stay-at-home measures may have on cybercrime victimisation.

Motivated Offender

As highlighted by Hawdon et al. (2020) increased unemployment rates associated with temporary or permanent closures resulting from COVID-19 can act as a push factor for offending. Further, cybercriminals who are also sheltering in place may have more time to engage in criminality. They will also undoubtedly see the increased usage of the Internet as being correlated with a greater number of potential victims, driving them to increase efforts and develop new methods to exploit current vulnerabilities (Anderson & Selck, 2020).

Target Suitability

As it relates to increasing target suitability, COVID-19 has done three main things: created a society desperate to obtain information on the pandemic; pushed the society to a greater

dependency on the Internet for business; and modified commerce, education, socialization and entertainment. It also forced persons into limited movement with the majority of time spent at home (Brathwaite, 2020; Koeze & Popper, 2020). Firstly, these factors increase target suitability as persons may tend to be less circumspect when scams are wrapped in the guise of COVID-19 updates or information (Mahamba, 2020). Secondly, the dependence on technology for daily activities leads to increased time online, hence increasing their 'visibility' (Yar, 2005). As, previously mentioned research shows that increased time online, particularly if combined with risky or deviant behaviour, increases the risk of victimisation (Kokkinos & Saripanidis, 2017; Lee et al., 2019; Lee & Downing, 2019). Thirdly, research into the spatial dimension of cybercrime has identified that persons have higher levels of engagement in behaviours that increase the risk of cybercrime victimisation such as online shopping and banking when at home (Ren et al., 2013; Saravanan & Thilagaraj, 2014; Song et al., 2016). This implies that persons using the Internet at home may expose themselves to a greater risk of victimisation through the increased time spent engaging in risky online activity. Overall, COVID-19 measures have the potential to increase target exposure, accessibility, and attractiveness as they shift routine activities by moving individuals online and increasing the time that must be spent using technology.

Capable Guardianship

In the initial stages of COVID-19, it was indeed evident that organisations did not fully assess the risk associated with services such as Zoom. Users of Zoom worldwide, including the University of the West Indies' Caribbean Sociological Society and the University of the Bahamas experienced 'zoombombing' as it has been coined (Brathwaite, 2020). The activity of 'zoombombing', which plagued users in the early stages of the transition due to COVID-19 refers to unwanted intrusions by Internet trolls and hackers on the Zoom platform, which included racial slurs and pornographic material (Lorenz & Alba, 2020). However, with time the surge in Internet usage drew greater attention to vulnerabilities and risks associated with online usage, which has resulted in upgrades by service providers (Heaven, 2020). For example, after growing cries to ban the use of Zoom because of 'zoombombing', the company released its 5.0 version in April 2020 with security features that include AES 256-bit encryption and several other security measures (Lyons, 2020; O'Flaherty, 2020). Further, there is a growing drive to encourage public awareness and provide guidance on the importance of online security and the steps that can be taken to mitigate cybercrime risk (International Chamber of Commerce, 2020; Interpol, 2020; Sharton, 2020). One demonstration of the effectiveness of these recent campaigns are reports showing that antivirus software searches saw a drastic increase of up to 357% since the implementation of stay-at-home orders due to the COVID-19 pandemic (Brathwaite, 2020; Winter, 2020).

Methods

This study is based on a natural experiment resulting from the presence of the COVID-19 pandemic and the resulting changes instituted to reduce its spread. The study uses a between-group design to assess the effect of COVID-19 on cybercrime rates and patterns. Given that this was a global 'treatment', it would not be feasible to identify a control group within the country or the region. Therefore, the researcher used data from a group that was already collected before COVID-19 as the control group. For the post treatment group, the same collection mechanism and survey instrument were used to collect the data. To limit the concerns related to possible selection bias and randomization, Bayesian statistics and Propensity Score Matching (PSM) are used in this study. Table 2 shows a guide to the interpretation of Bayes Factors as it relates to the level of evidence in support of the alternative hypothesis H_1.

Sampling

The pre- and post-COVID-19 samples were collected using a self-administered survey, which was disseminated using snowball sampling via Facebook to users over the age of 18 residing in The Republic of Trinidad and Tobago. The initial seed consisted of 450 Facebook users of varying ages, ethnicities, and geographic locations within Trinidad and Tobago. The survey was run during the period June 6, 2019 to August 17, 2019 with a 92% completion rate, which resulted in a dataset of 104 usable submissions with missing data imputed for 14 responses using the Multivariate Imputation by Chained Equations (MICE) (van Buuren & Groothuis-Oudshoorn, 2011) package for R (version 3.6.2, R Core Team, 2019). The post-COVID-19 sample was collected using the same method as in the pre-COVID-19 study, which targeted Facebook users in Trinidad and Tobago. The survey was made available for the period July 25, 2020 to August 27, 2020 and resulted in 149 participants completing the survey, which was a completion rate of 98%.

An analysis of the learning curves for logistic regression and Naïve Bayes classification (not shown here) showed that the sample size was sufficient to reach a point of irreducible error using both algorithms. This is in line with findings by Rudner (2016) who examined fifteen datasets and found that a sample as small as 50 data points had an accuracy of 79% and a Root Mean Square Error (RMSE) or 0.083. Further, Myllymaki et al. (2002) found that for B-Course v2.0.0 a network with 5 - 15 nodes required as little as 100 data points to construct the network regardless of its complexity.

An initial assessment of the data was performed by comparing the demographics of the participants in the pre-COVID-19 and post-COVID-19 samples using a Bayesian t-test, which is given in Table 2. The results show that there are no statistical differences between the two samples based on the three demographic factors assessed. This inference is based on the association test (t-test)

producing a log BF_{10} < -2 (extreme evidence, Table 1) in all instances in favour of H_0 (the composition of the pre- and post- COVID-19 samples are statistically equivalent).

Table 1

A Descriptive and Approximate Classification Scheme for the Interpretation of Bayes Factors BF_{10} and Log BF_{10} (adjusted from Lee & Wagenmakers, 2013)

Bayes factor (BF_{10})	Log Bayes factor (BF_{10})	Evidence category
> 100	> 2	Extreme evidence for H_1
30 - 100	1.477 to 2	Very strong evidence for H_1
10 - 30	1 to 1.477	Strong evidence for H_1
3 - 10	0.477 to 1	Moderate evidence for H_1
1 - 3	0 to 0.477	Anecdotal evidence for H_1
1	0	No evidence
1/3 - 1	0 to -0.477	Anecdotal evidence for H_0
1/10 – 1/3	-0.477 to -1	Moderate evidence for H_0
1/30 – 1/10	-1 to -1.477	Strong evidence for H_0
1/100 – 1/30	-1.477 to -2	Very strong evidence for H_0
< 1/100	< -2	Extreme evidence for H_0

Data Collection

To measure victimisation, the respondents were asked to indicate if they had been victims of four types of cybercrime (Unauthorized Access, Malware, Cyberbullying and Unsolicited Content). To provide a point of comparison the specific cybercrimes chosen for the study were those prevalent in the jurisdiction of interest and for which there is substantial peer-reviewed literature (Inter-American Development Bank & Organization of American States, 2016; Jessop, 2019; Taitt, 2018; Reyns, Fisher, Bossler, & Holt, 2019; Leukfeldt & Yar, 2016; Rodriguez et al., 2017). The response was dichotomous and given as either 'Yes' or 'No'. The results were calculated and recorded both separately and summarily as an overall cyber-victimisation variable.

Table 2

Demographic Comparison of Pre- and Post-COVID-19 Samples Using Bayesian t-test

Online Routine Activities	Pre-COVID-19 Sample	Post-COVID-19 Sample	Log BF_{10} (t-test)
Sex			-2.495
Female	47	79	

Male	57	70	
Age			-2.274
15-24	25	18	
25-34	27	46	
35-44	32	57	
45-54	12	16	
> 55	8	12	
Ethnicity			-2.880
African	37	76	
East Indian	36	32	
Chinese	0	3	
Syrian/Lebanese	0	0	
White/Caucasian	1	0	
Mixed	27	38	
Other	3	0	

Note. For all *t*-test the alternative hypothesis is that Group 1 is not equal to Group 2

Analysis of the individual cybercrimes would allow insight into the nature of the effect, if any, of COVID-19 measures on specific cybercrimes; that is, an overall effect on cybercrime victimisation may not translate equally to all forms of cybercrime. The summated variable was also dichotomous and represented whether the respondent was a victim of any form of cybercrime victimisation. Given the nature of the data collection, an attempt to create a count variable would not give an accurate perception of the frequency of victimisation but rather how many types. Further, such an attempt could obfuscate the results as these individual cybercrimes may be linked, either as correlated or causal relationships, or it may magnify any misclassification of the crime event by the respondent.

The construct variables of target accessibility, target exposure, and capable guardianship were measured using Likert-type scales with 5, 3 & 6 items respectively. Target accessibility was measured by the time in hours spent per day engaging in the online activities of browsing the Internet, shopping online, using social media, watching adult content or pornography, and downloading music or videos. Target exposure was measured by the degree of self-disclosure of personal information in various online settings. It included nonverbal communication, such as posting pictures of oneself online, posting personal information, and sharing one's location openly online. Capable guardianship denotes software applications developed to guard/protect computer systems and networks from offenders, which in this study were antivirus, pop-up blockers, and anti-malware. Capable guardianship can also include nontechnical methods, which were measured with three items that assessed the potential target's skill level and knowledge with computers, technology, and awareness of victimisation risk.

Limitations

As with all studies there were limitations, which in some cases were inescapable given that this was a natural experiment and that it required replication of the initial data collection methods. Firstly, although the statistical analyses add some confidence in the representativeness of the Facebook sample, it is still a convenience sample and may not be generalisable to the general population. Secondly, the pretest and posttest groups used different respondents, in what is essentially a quasi-experimental design. Although this design is frequently used in social science and healthcare research, it comes with potential limitations (Harris et al., 2006).

The main limitation is the potential reduction in internal validity; however, this is minimised by instituting controls such as consistency in sample sources and methods. Further, Bayesian statistics is useful in this sense as it provides a measurement of the support for the hypothesis; that is, the statistical 'evidence' is only slightly better than chance or substantial. Further, by testing the similarity between the data sets based on demographics and by propensity score matching concerns related to selection bias were mitigated.

Results

This section outlines the results of all the statistical analyses performed on the datasets to determine the effect of the stay-at-home measures implemented due to the COVID-19 pandemic on online routine activities and cybercrime. All t-tests, χ^2-tests and logistic regression analyses were conducted using JASP statistical software (version 0.13.1; JASP Team, 2020) and unless otherwise stated default parameter values were used. The Bayesian classification and dependency modelling were done using the B-Course platform (version 2.0.0; Complex Systems Computer Group, 2002), a web-based tool for Bayesian and causal dependence data analysis (Myllymaki et al., 2002).

Next, the online routine activities assessed in pre/post-COVID-19 samples were compared using t-tests. Also, the effect of COVID-19 measures on the online routine activities are presented based on χ^2- tests. The results of the two analyses are given in Table 3. The tests of association produced logarithm Bayes factor of < -2 (extreme evidence, Table 1) in favour of a statistically significant increase in online activities related to target exposure from the pre-COVID-19 period to the post-COVID-19 period.

Concerning target accessibility, the results were mixed, with strong evidence for increased time spent engaging in Internet browsing and watching adult content. Interestingly, the results showed that time spent shopping online, downloading music and video, and using social media or social networking sites decreased. Surprisingly the tests showed that there were increases in usage of

physical guardianship measures and personal guardianship activities post-COVID-19. Of all the variables measured, only the physical guardianship measures of using antivirus, spam filters and pop-up blockers were found to be related to COVID-19. However, the level of evidence for the relationship of COVID-19 with the use of antivirus and spam filters was anecdotal (log BF_{10} 0 – 0.477), while the evidence for the relationship between COVID-19 and the use of pop-up blockers was extreme (log BF_{10} > 2). For all t-tests, the alternative hypothesis specifies that the level of engagement in the routine activities decreased after the onset of COVID-19 related measures at the 0.05 level. And for all chi-squared tests, the alternative hypothesis specified that there was insufficient evidence to reject the null hypothesis of no relationship between COVID-19 and the change in routine activities at the 0.05 level.

Table 3

Bayesian t-test and χ^2 of Online Routines Activities Comparing Pre-and Post-COVID-19 Samples

Online Routine Activities	Log BF_{10} (t-test)	Log BF_{10} (χ^2)
Target Exposure (Frequency of engaging in the activity per week)		
Posting pictures online	-2.418	-4.707
Posting personal information online	-2.701	-6.178
Posting location online	-3.122	-2.369
Target Accessibility (No. of hours engaging in the activity per day)		
Internet Browsing	-1.343	-2.540
Shopping Online	1.296	-1.747
Using Social Media (Social Networking Sites)	1.028	-0.114
Watching adult content	-1.719	-5.120
Downloading videos and music	1.926	-2.543
Capable Guardianship (Physical or Personal)		
Use of antivirus software	-1.330	0.424
Use of spam filters	-2.433	0.011
Use of pop-up blockers	-2.666	6.301
Setting social networking/media accounts to 'Private'	-2.068	-2.118
Skill level and knowledge with computers and technology	-1.865	-2.005
Knowledge of victimisation risk/awareness of cybercrime	-1.642	-1.864

To assess the effect of COVID-19 measures on cybercrime victimisation the data was analysed using three statistical methods. In the first instance χ^2 - tests were used to assess the relationship/effect of COVID-19 measures on the four cybercrimes measured in the survey instrument, the results of which are shown in Table 4. For all t-tests, the alternative hypothesis specifies that the prevalence of the specified cybercrime decreased after the onset of COVID-19 related measures at the 0.05 level. For all chi-squared tests, the alternative hypothesis specified that there was insufficient evidence to reject the null hypothesis of no relationship between COVID-19 and the change in the prevalence of cybercrime at the 0.05 level.

Table 4
Results of χ^2- tests Comparing Pre- and Post-COVID-19 Samples

Types of Victimisation	Pre-COVID-19 Sample	Post-COVID-19 Sample	Log BF_{10} (t-test)	Log BF_{10} Poisson (χ^2)
Unauthorized Access	66%	16%	-4.376	20.212
Malware	40%	33%	-1.878	-0.587
Cyberbullying	81%	12%	-5.140	40.596
Unsolicited Content	54%	28%	-3.363	4.855
Cybercrime Victimisation (overall)	96%	55%	-4.614	19.101

The results shown in Table 4 suggest that all forms of cybercrime have decreased in prevalence after the COVID-19 pandemic. However, the χ^2 test suggests that while the overall decrease in cybercrime victimisation is related to the COVID-19 pandemic, not all cybercrimes were affected in the same way. While the decreases in the prevalence of victimisation for unauthorised access, cyberbullying and unsolicited content are related to the pandemic, the decrease in victimisation using malware is not related to the pandemic.

Given the results in the initial analysis suggesting that changes in victimisation patterns have indeed occurred post-COVID-19 pandemic, the Naïve Bayes algorithm was used to develop a predictive model to further assess the phenomenon. Naïve Bayes allows effective visualisation of interrelationships and the cumulative effect of predictors on the responses; i.e., the strength of the relationship of the covariates with the response variable is measurable. To facilitate the analysis, the pre- and post-COVID-19 datasets were merged and a COVID-19 indicator variable added (pre-COVID-19 = 0; post-COVID-19 = 1).

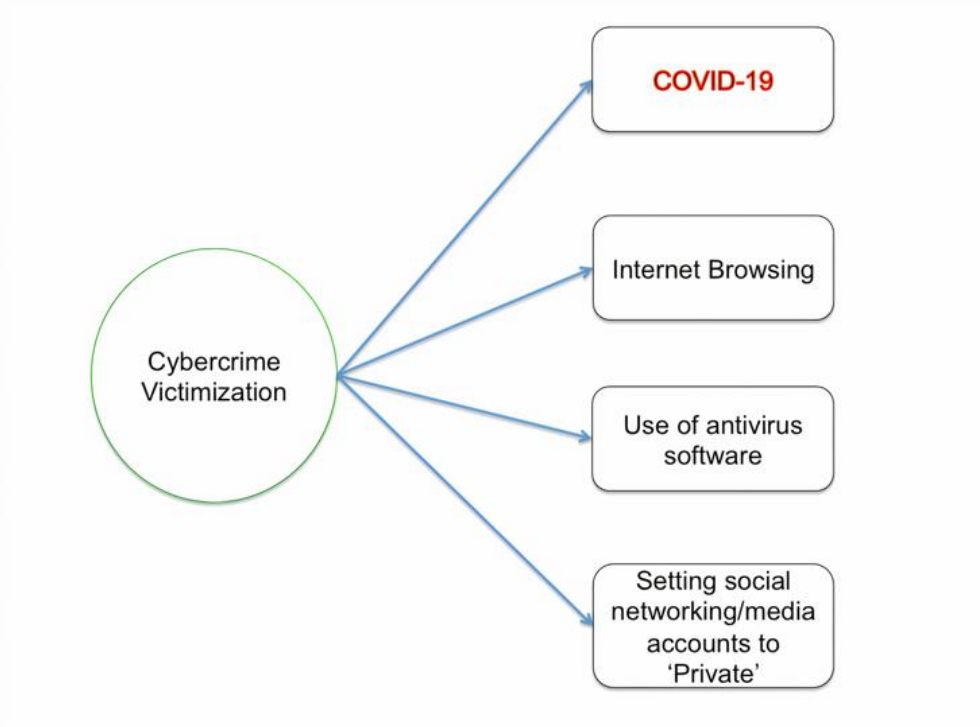
The results of the Naïve Bayes algorithm (prediction of overall cyber-victimisation variable) are provided in Figure 1. The classification model suggests that the variables of Internet browsing hours, Use of Antivirus software, and Setting Social Media Accounts to Private are statistically

related to cybercrime victimisation. Further, and specifically important to this study, the model also shows that the COVID-19 variable is statistically related to cybercrime victimisation. Therefore, adding further evidence that the COVID-19 pandemic is affecting the prevalence of cybercrime.

However, Naïve Bayes does not indicate the size or direction of the effect. To fill the gap, logistic regression was used to determine the direction/sign of the effect of COVID-19 measures and how it changed the outcome, that is, the odds of becoming a victim. The results of the logistic regressions (not shown) indicated that COVID-19 measures result in a decrease in the risk of victimisation with odds ratio of 0.017. Notably, the COVID-19 variable had a p-value of <0.001 (strong statistical significance), with the overall model having a Nagelkerke R^2 of 0.536.

Figure 1

Naïve Bayes Directed Acyclic Graphical Model for Cybercrime Victimisation (Pre/Post-COVID-19)



Given the nature of the natural experiment being done with different groups, the ability to compare the outcomes can be questioned. However, to demonstrate the validity of the results, propensity score matching (PSM) was also performed. PSM is a quasi-experimental method where statistical techniques are used to construct an artificial control group by matching each treated unit with a non-treated unit of similar characteristics to artificially remove selection bias (Ali et al., 2019;

Rosenbaum & Rubin, 1983; Schneider & McDonald, 2010). To obtain an artificial control, PSM pairs datapoints as 'treatment' and 'control' units based on the similarity of covariates (the characteristics of participants) and discards all unmatched units. PSM obtained a point estimate mean of -0.42 for the matched difference (pre vs. post-COVID-19) with a paired t-test indicative of a significant difference between cybercrime victimisation pre and post-COVID-19 ($t = -6.6377$, $df = 68$, $p < 0.001$). The results suggest that there was a 42% smaller chance of victimisation post-COVID-19.

To further define the role or dependence of cybercrime victimisation on COVID-19 pandemic measures, Bayesian dependency modeling was done using the summated victimisation data. The results of this are presented in Figure 2. This will identify the possible causal relationship that may exist between the COVID-19 pandemic and cybercrime victimisation and our online routine activities.

Figure 2

Dependency Model for Cybercrime Victimisation

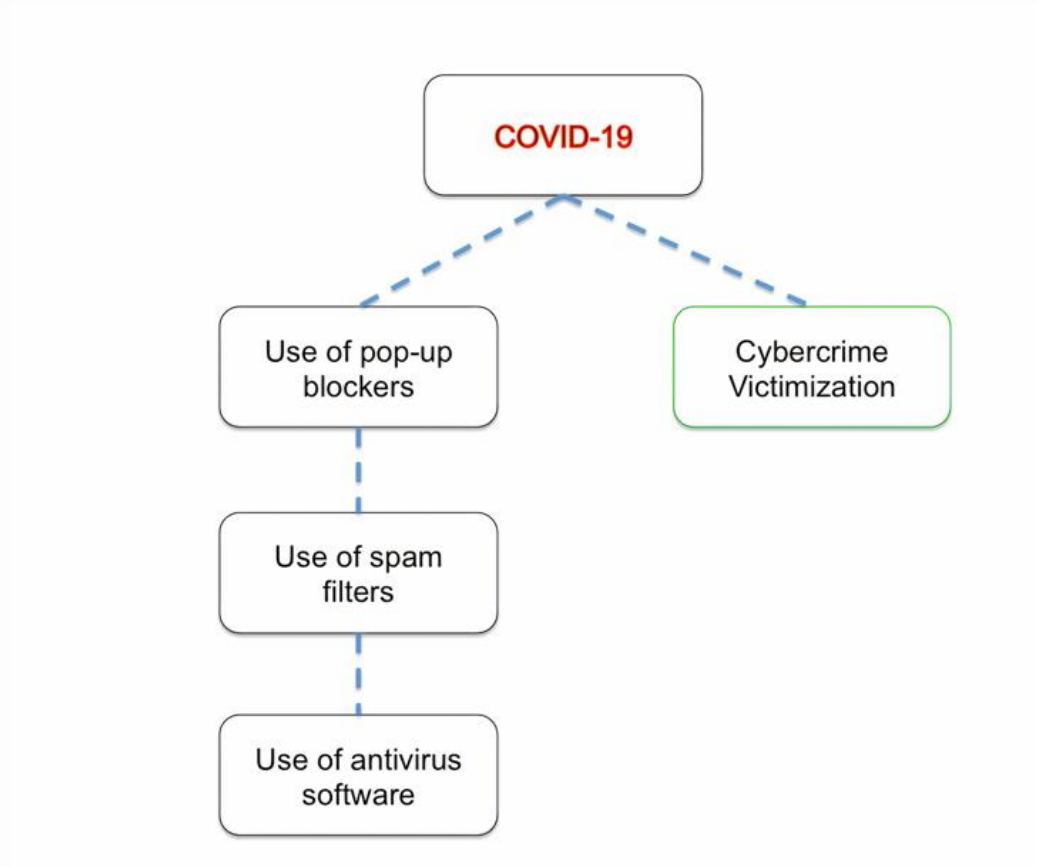


Figure 2 shows that COVID-19 is linked to the use of physical guardianship and cybercrime victimisation. However, the information is not sufficient to determine the nature of the

dependencies; that is, the direction of the dependency or if a latent variable interaction exists – indicated by the broken lines. However, it can be proposed that COVID-19 caused increased use of physical guardianship measures. As stated in the introduction, there has been increased education and initiatives to increase awareness of cybercrime and online safety practices by both government and private entities (Anant et al., 2020; Arnold et al., 2020). Increased awareness may have led to increased implementation of these physical guardianship measures.

Lastly, the classification models produced using Naïve Bayes for overall cybercrime victimisation pre- and post-COVID-19 are compared to determine if the measures implemented had any possible effect on the performance of the RAT relative to cybercrime; specifically, changes in the predictors of cybercrime. The comparison of the two samples is given in Table 5 and Table 6.

Table 5

Comparison of Predictors of Cybercrime Victimisation Identified Pre- and Post-COVID-19

Online Routine Activities	**Pre-COVID-19**	**Post-COVID-19**
Target Exposure (Frequency of engaging in the activity per week)		
Posting pictures online		
Posting personal information online		
Posting location online	X	X
Target Accessibility (No. of hours engaging in the activity per day)		
Internet Browsing	X	X
Shopping Online		
Using Social Media (Social Networking Sites)		
Watching adult content		X
Downloading videos and music	X	
Capable Guardianship (Physical or Personal)		
Use of antivirus software	X	
Use of spam filters	X	
Use of pop-up blockers	X	
Setting social networking/media accounts to ‘Private’		
Skill level and knowledge with computers and technology		X
Knowledge of victimisation risk/awareness of cybercrime		
Demographics		
Age	X	
Ethnicity		
Sex	X	

Table 6

Comparison of Predictive Model Performance (Explanatory Power of the RAT) Pre- and Post - COVID-19

	Pre-COVID-19	Post-COVID-19
Scaler performance metric		
General classification Accuracy	*95.70%*	*72.06%*
Combination performance metrics		
F1-Score	*0.9778*	*0.7246*
Matthews Correlation Coefficient (MCC)	*0.4374*	*0.4565*

Note: The positive class is coded as 1

Tables 5 and 6 show a decrease in the importance of given predictors and the overall explanatory power of the RAT post-COVID-19. The number of predictors has been cut in half with a corresponding drop in model performance in the post-COVID-19 model. The only exception is the minor increase in the MCC; however, closer examination indicates that this was because while the overall accuracy of the model and the model's ability to predict the positive class decreased, there was a minor increase in the ability to predict the negative class. However, overall the results suggest both a change in user behaviours and a decrease in the importance of the spatio-temporal convergence required by the RAT for a crime event to occur.

Researchers have suggested that such outcomes are correlated to the dominance of crimes that occur as random events that cannot be explained within an opportunity framework, which is supported by the collected data in the post-COVID-19 sample (Bossler & Holt, 2009; Yucedal, 2010; Ngo & Paternoster, 2011; Bossler & Holt, 2013, Reyns, 2015). In the post-COVID-19 sample, the crime with the highest prevalence is Malware as compared to Cyberbullying dominating before COVID-19. Where in the latter case the crime tends to be less human-centric, also explaining the absence of demographic factors in the post-COVID-19 predictive model. Bossler and Holt (2013) specifically suggest that the RAT has limited usability with Malware related victimisation due to its random nature. Notably, the shift to higher occurrences of malware-related victimisation corresponds to reports of spikes in phishing attempts, which has seemingly become one of the primary tools employed by cyber-threat actors post-COVID-19.

Discussion

This study found that reports of increases in cyberattacks (Brathwaite, 2020; Mahamba, 2020; Shaver, 2020) or increased time spent online do not necessarily translate into increases in cybercrime victimisation as indicated by the observed decrease in cybercrime, although there was a positive change in online activities such as Internet browsing. This study and the research done by Hawdon et al., (2020) indicate that although cyberattacks are increasing, there is not a

commensurate increase in cybercrime victimisation. It also suggests that although increased time spent online is associated with higher cybercrime victimisation risk, the threat can be mitigated by the implementation of sufficient guardianship measures such as the use of antivirus software and web browser protective software including pop-up blockers and spam filters.

Shifts in cybersecurity priorities and budgets by both the private and public sectors have led to increased media attention and cyberawareness initiatives to reduce online risk and increase cybersafe practices (Anant et al., 2020; Arnold et al., 2020; Brathwaite, 2020; Ghouralal, 2020; World Health Organization, 2020; Superville, 2020). Further, reports show that antivirus software searches saw a drastic increase of up to 357% since the implementation of stay-at-home orders due to the COVID-19 pandemic (Winter, 2020). In essence, the results of this study support an inference that these measures are having a positive impact on users' cyber-safe practices and hence the prevalence of cybercrime.

The effect of COVID-19 relative to online routines and victimisation rates in this study differed from a previous study. While Hawdon et al. (2020) reported no significant difference in cybercrime rates and online routines, this study identified increased rates of online activity and decreased cybercrime rates. The outcome of the increased online routine activity is in line with theoretical expectations given the limited mobility and increased dependency on cybersystems due to the stay-at-home orders. However, the fact that cybercrime rates decreased seems impractical. However, this may be explained by the increase in the use of self-protection measures, which was shown to be statically associated with the COVID-19 changes (Table 3). This aspect of increased use of self-protection was also reported by Hawdon et al. (2020). It suggests that physical guardianship measures once implemented are effective protective factors against cybercrime victimisation, even with the increased exposure and accessibility that is associated with greater time spent online.

Another observation which was not previously discussed in the literature but seen in this study was a shift in the most prevalent cybercrime (Table 4). There was a shift from the cyber-enabled crime of cyberbullying (81% to 12%)) to the cyber-dependent crime of malware infection (40% to 33%). This was a result of an 85.2% decrease in the prevalence of cyberbullying compared to a 17.5%. This corresponds to reports of spikes in phishing and online scams, which can be deemed random events as the attacker sends out thousands of attacks with no specific target (Reyns, 2015; Oduber et al., 2017). Conversely, stay-at-home orders correspond to decreased interpersonal relations, which can lead to cyberbullying; therefore, making this observation a logical change in cybercrime trends.

This study found that similar to the research by Hawdon et al. (2020) the RAT retained explanatory power for cybercrime post-COVID-19. However, its overall explanatory power may have changed and so too the predictors of cybercrime. Through a comparative analysis, this study discovered a

25% decrease in the accuracy of the predictive model (Table 6) derived from the rate for cybercrime victimisation, given the indicators examined. Further, demographic factors were no longer predictors of victimisation in the post-COVID-19 sample. In addition, the post-COVID-19 sample indicated that risky/deviant behaviour such as watching pornography was not a predictive factor. The former's change relative to the demographic factors is possibly related to the shift from interpersonal cybercrime, where the attacker is likely to show preference to a specific type of target – aligned with target congruence and victim precipitation theories – to a crime that takes a 'whoever falls into the net' approach (Bossler & Holt, 2013; Reyns, 2015).

For pornography, reports have indicated a spike in usage of pornographic content occurring immediately after the implementation of social distancing measures (Grubbs, 2020; Mestre et al., 2020). Research has shown that psychological distress, feelings of loneliness, depression, stress and anxiety often predict high levels of pornography use (Grubbs, et al., 2019; Mestre et al., 2020). All of these predictors are factors associated with the emergence of the pandemic and the feelings of dread and uncertainty it brings.

The role of COVID-19 in the increase in pornography viewership is supported by the χ^2- test, which was reported in Table 3. The role of risky/deviant behaviour such as watching pornography in increasing cybercrime victimisation risk is well reported throughout the extant literature (e.g. Akdemir & Lawless, 2020; Hinduja & Patchin, 2009; Kranenbarg et al., 2019; Marcum et al, 2010; Navarro & Jasinski, 2012). Therefore, the overall linkage between COVID-19, watching pornography and increased risk aligns well with the literature.

It is important to note that the observations on the RAT are limited to overall cybercrime occurrence since, as highlighted, the change is likely associated with the shift in prevalence of interpersonal crimes to more random cybercrimes. Therefore, the utility of the RAT may have remained unchanged relative to specific forms of cybercrimes.

Conclusion

The stay-at-home measures implemented due to the COVID-19 pandemic have indeed affected cybercrime victimisation prevalence and patterns. However, the effect is contrary to expectation based on the premise that increased time online would result in an increased prevalence of cybercrime victimisation. While there was a general increase in online routine activities, there was a decrease in both cyber-dependent and cyber-enabled crimes post-COVID-19. The χ^2-tests and causal analysis are done in this study suggest that the decrease may be due to the indirect effect of COVID-19 leading to the increased usage of physical guardianship measures.

The decrease in cybercrime prevalence was also accompanied by a shift in the dominant form of victimisation moving from the cyber-enabled crime of cyberbullying to the cyber-dependent crime of malware infection. The comparative analysis between the predictive models of overall cybercrime victimisation pre- and post-COVID-19 using the RAT also elucidated a change in the theory's explanatory power. The roughly 24% decrease in model accuracy coincides with the shift in the most prevalent cybercrime moving from cyberbullying to malware infection. The latter is associated with a random event that cannot be explained within an opportunity framework.

The observed changes in cybercrime victimisation suggest that this form of crime may be modelled as a complex adaptive system that is subject to change due to social/environmental factors, such as the exogenous shock caused by the sudden onset of COVID-19 and its associated governmental and societal response. The importance of routine activities in cybercrime is dependent on the type of cybercrime, but overall an equilibrium exists between the risk factors and the protective factors. Therefore, the prediction of changes to cybercrime victimisation rates requires that all factors be considered, including motivation, target routines, target behavioural patterns, and protective measures adopted by individuals or third parties. However, the decrease in cybercrime which is correlated to guardianship bodes well for policymakers as it suggests that investment in technical guardianship measures and public safety awareness can have an adequate impact on cybercrime victimisation rates.

This study highlights the need for further research into the human factor in cybercrime in the Caribbean cultural context; specifically, motivations for protective online behaviour and the role of exogenous shocks in changing crime and behavioural patterns. A longitudinal study can potentially provide a deeper understanding of factors that determine changes in online behaviours in a society where increased use and dependence on digital platforms seem inescapable, and decreasing time spent online is not a practical approach to cybercrime reduction. Therefore, the situation necessitates an increased focus on the effectiveness of protective behaviour by individuals and the motivation to engage in these behaviours. Overall, additional targeted research will provide policymakers not only with greater situational awareness, but also a foundation for policy development targeting cybercrime reduction.

References

Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Research, 30*(6), 1665–1687. https://doi.org/10.1108/INTR-10-2019-0400

Ali, M. S., Prieto-Alhambra, D., Lopes, L. C., Ramos, D., Bispo, N., Ichihara, M. Y., Pescarini, J. M., Williamson, E., Fiaccone, R. L., Barreto, M. L., & Smeeth, L. (2019). Propensity score methods in health technology assessment: Principles, extended applications, and

recent advances. *Frontiers in Pharmacology*, *10*, 973. https://doi.org/10.3389/fphar.2019.00973

Álvarez-García, D., Nunez, J., Gonzalez-Castro, P., Rodriguez, C., & Cerezo, R. (2019). The effect of parental control on cyber-victimization in adolescence: the mediating role of impulsivity and high-risk behaviors. *Frontiers in Psychology*, *10*. https://doi.org/10.3389/fpsyg.2019.01159

Anant, V., Caso, J., & Schwarz, A. (2020). COVID-19 crisis shifts cybersecurity priorities and budgets. Retrieved July 29, 2020, from McKinsey & Company website: https://www.mckinsey.com/business-functions/risk/our-insights/covid-19-crisis-shifts-cybersecurity-priorities-and-budgets

Anderson, M., & Selck, E. (2020). Cyber crime increases as netwroks grow more vulnerable in the wake of COVID-19. Retrieved July 27, 2020, from Security Boulevard website: https://securityboulevard.com/2020/06/cyber-crime-increases-as-networks-grow-more-vulnerable-in-the-wake-of-covid-19/

Arnold, B., Azam, U., & Sivasothy, K. (2020). Authorities step up cyber awareness efforts for COVID-19. Retrieved August 1, 2020, from Gowling WLG website: https://gowlingwlg.com/en/insights-resources/articles/2020/authorities-step-up-cyber-awareness-efforts-for-co/

Balram, S. (2020). Covid-19 Impact: Social media activity in the country grew 50X in early March, says Nielsen. Retrieved July 29, 2020, from The Economic Times website: https://economictimes.indiatimes.com/tech/internet/covid-19-impact-social-media-activity-in-the-country-grew-50x-in-early-march-says-nielsen/articleshow/74833596.cms

Beech, M. (2020, March 25). COVID-19 Pushes up internet use 70% and streaming more than 12%, first figures reveal. *Forbes*. https://www.forbes.com/sites/markbeech/2020/03/25/covid-19-pushes-up-internet-use-70-streaming-more-than-12-first-figures-reveal/#23cf4af53104

Berchialla, P., Gregori, D., & Baldi, I. (2019). The role of randomization in bayesian and frequentist design of clinical trial. *Topoi*, *38*(2), 469–475. https://doi.org/10.1007/s11245-018-9542-8

Bossler, A., & Berenblum, T. (2019). Introduction: New direction in cybercrime research. *Journal of Crime and Justice*, *42*(5), 495-499. https://doi.org/10.1080/0735648X.2019.1692426

Bossler, A. M., & Holt, T. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, *30*(1), 1–25.

Bossler, A. M., & Holt, T. (2013). Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice*, *29*(4). 420-436. doi: 10.1177/1043986213507401

Brathwaite, C. (2020, June 4). OP-ED | COVID-19 is exposing cyber security vulnerabilities. *Guyana Chronicle*. https://guyanachronicle.com/2020/06/04/op-ed-covid-19-is-exposing-cyber-security-vulnerabilities/

Buil-Gil, D., Miro-Llinares, F., Moneva, A., Kemp, S., & Diaz-Castano, N. (2020). Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK. *European Societies*, *23*(1), S47-S59. https://doi.org/10.1080/14616696.2020.1804973

Campedelli, G., Aziani, A., & Favarin, S. (2020). *Exploring the effect of 2019-nCoV containment policies on crime: The case of Los Angeles*. arXiv:2003.11021 [stat.OT]. https://arxiv.org/abs/2003.11021v1

Castells, M. (2002). *The Internet galaxy: Reflections on the Internet, business and society*. Oxford University Press.

Choi, S. (2018). A Lifestyle-Routine Activity Theory (LRAT) Approach to Cybercrime Victimization: Empirical Assessment of SNS Lifestyle Exposure Activities (Seoul National University). Seoul National University. Semantic Scholar. Retrieved from https://www.semanticscholar.org/paper/A-Lifestyle-Routine-Activity-Theory-(LRAT)

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

de Jong, E., Bernasco, W., & Lammers, M. (2019). Situational correlates of adolescent substance use: An improved test of the routine activity theory of deviant behavior. *Journal of Quantitative Criminology*. *36*, 823–850. https://doi.org/10.1007/s10940-019-09433-w

Gallagher, J. (2020, May 28). *Covid vaccine update: Those that work - and the others on the way* [BBC] https://www.bbc.com/news/health-51665497

Ghouralal, D. (2020, March 13). *Rowley: Schools, universities to be closed for one week*. LoopTT. https://www.looptt.com/content/rowley-schools-universities-be-closed-one-week

Grubbs, J. (2020, April 8). *Porn use is up, thanks to the pandemic*. The Conversation. https://theconversation.com/porn-use-is-up-thanks-to-the-pandemic-134972

Grubbs, J., Wright, P., Braden, A., Wilt, J., & Kraus, S. (2019). Internet pornography use and sexual motivation: A systematic review and integration. *Annals of the International Communication Association*, *43*(2), 117-155.

Harris, A. D., McGregor, J. C., Perencevich, E. N., Furuno, J. P., Zhu, J., Peterson, D. E., & Finkelstein, J. (2006). The use and interpretation of quasi-experimental studies in medical informatics. *AMIA Journal of the American Medical Informatics Association*, *13*(1), 16–23. https://doi.org/10.1197/jamia.M1749

Hawdon, J., Bernatzky, C., & Costello, M. (2019). Cyber-Routines, political attitudes, and exposure to violence-advocating online extremism. *Social Forces*, *98*(1), 329–354. https://doi.org/10.1093/sf/soy115

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

Heaven, W. (2020, April 7). *Why the coronavirus lockdown is making the Internet stronger than ever*. MIT Technology Review Retrieved July, 2020, from https://www.technologyreview.com/2020/04/07/998552/why-the-coronavirus-lockdown-is-making-the-internet-better-than-ever/

Hinduja, S., & Patchin, J. W. (2009). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying*. Corwin Press.

Howell, C. J., Burruss, G. W., Maimon, D., & Sahani, S. (2019). Website defacement and routine activities: Considering the importance of hackers' valuations of potential targets. *Journal of Crime and Justice*, *42*(5), 536–550. https://doi.org/10.1080/0735648X.2019.1691859

Hsieh, M., & Wang, S. (2018). Routine activities in a virtual space: A Taiwanese case of an ATM hacking spree. *International Journal of Cyber Criminology*, *12*(1), 333–352.

Inter-American Development Bank, & Organization of American States. (2016). *Cybersecurity: Are we ready in Latin America and the Caribbean?: 2016 Cybersecurity Report*. Inter-American Development Bank.

International Chamber of Commerce. (2020). *COVID-19 cyber security threat to MSMEs*. International Chamber of Commerce. https://iccwbo.org/content/uploads/sites/3/2020/05/2020-icc-sos-cybersecurity.pdf

Interpol. (2020). *Global landscape on COVID-19 cyberthreat* (pp. 1–2). Interpol. https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats

INTERPOL General Secretariat. (2020). *Cybercrime: COVID-19 impact*. INTERPOL.

JASP Team. (2020). *JASP* (0.13.1) [Computer software]. https://jasp-stats.org/}

Jessop, D. (2019). *The Caribbean's cybersecurity response must evolve*. The Caribbean Council. https://www.caribbean-council.org/caribbeans-cybersecurity-response-must-evolve/

Kitchin, R. (1998). Towards geographies of cyberspace. *Progress in Human Geography*, *22*(3), 385–406.

Koeze, E., & Popper, N. (2020, April 7). *The virus changed the way we Internet*. The New York Times. https://www.nytimes.com/interactive/2020/04/07/technology/coronavirus-internet-use.html

Kokkinos, C. M., & Saripanidis, I. (2017). A lifestyle exposure perspective of victimization through Facebook among university students: Do individual differences matter? *Computers in Human Behavior*, *74*, 235–245.

Kranenbarg, M., Holt, T., & van Gelder, J. (2019). Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. *Deviant Behavior*, *40*(1), 40–55.

Lee, J., & Downing, S. (2019). An exploratory perception analysis of consensual and non-consensual image sharing. *Journal of Cybersecurity Intelligence & Cybercrime, 2*(2), 23–43.

Lee, M. D., & Wagenmakers, E. J. (2013). Bayesian cognitive modeling: A practical course. http://dx.doi.org/10.1017/CBO9781139087759

Lee, S. S., Choi, K., Choi, S., & Englander, E. (2019). A test of structural model for fear of crime in social networking sites. *International Journal of Cybersecurity Intelligence & Cybercrime, 2*(2), 5–22.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263-280.

Logan, T. K., Walker, R., Jordan, C. E., & Leukefeld, C. G. (2006). *Women and victimization: Contributing factors, interventions, and implications*. American Psychological Association.

Lorenz, T., & Alba, D. (2020, April 3). *"Zoombombing" becomes a dangerous organized effort*. The New York Times. https://www.nytimes.com/2020/04/03/technology/zoom-harassment-abuse-racism-fbi-warning.html

Lyons, K. (2020, May 25). *Zoom has temporarily removed Giphy from its chat feature*. the Verge. https://www.theverge.com/2020/5/25/21269506/zoom-disables-giphy-gifs-chat-security-facebook

Mahamba, C. (2020, June 24). *Banking Risk Information Centre says cybercrime on the rise during COVID-19 pandemic*. Independent Online. https://www.iol.co.za/the-star/news/banking-risk-information-centre-says-cybercrime-on-the-rise-during-covid-19-pandemic-49835906

Marcum, C., Ricketts, M., & Higgins, G. (2010). Assessing sex experiences of online victimization: An examination of adolescent online behaviors using routine activity theory. *Criminal Justice Review*, *35*(4), 412–437.

Mesch, G., & Dodel, M. (2018). Low self-control, information disclosure, and the risk of online fraud. *American Behavioral Scientist, 62*(10), 1356–1371.

Mestre, G., Blycker, G., & Potenza, M. (2020). Pornography use in the setting of the COVID-19 pandemic. *Journal of Behavioral Addictions, 9*(2), 181-183.

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. *JCJ Journal of Criminal Justice, 68*.

Myllymaki, P., Silander, T., Tirri, H., & Uronen, P. (2002). B-Course: A web-based tool for Bayesian and causal data Analysis. *International Journal on Artificial Intelligence Tools, 11*(3), 369–387.

Navarro, J. N., & Jasinski, J. L. (2012). Going cyber: Using routine activities theory to predict cyberbullying experiences. *Sociological Spectrum, 32*(1), 81–94.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773–793.

O'Flaherty, K. (2020, April 10). *Zoom security: Here's what zoom is doing to make its service safer*. Forbes. https://www.forbes.com/sites/kateoflahertyuk/2020/04/10/zoom-security-heres-what-zoom-is-doing-to-make-its-service-safer/#7583a80a30fc

R Core Team. (2019). *R: A language and environment for statistical computing*. R Foundation for Statistical Computing. https://www.R-project.org/

Ren, F., Kwan, M.P., & Schwanen, T. (2013). Investigating the temporal dynamics of Internet activities. *Time & Society*, *22*(2), 186–215.

Reyns, B. W. (2015). A routine activity perspective on online victimisation. *Journal of Financial Crime*, *22*(4), 396–411. https://doi.org/10.1108/JFC-06-2014-0030

Reyns, B. W., Fisher, B. S., Bossler, A. M., & Holt, T. J. (2019). Opportunity and self-control: Do they predict multiple forms of online victimization? *American Journal of Criminal Justice*, *44*(1), 63–82. https://doi.org/10.1007/s12103-018-9447-5

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, *38*(11), 1149–1169. https://doi.org/10.1177/0093854811421448

Reyns, B. W., Henson, B., & Fisher, B. S. (2015). Guardians of the cyber galaxy: An empirical and theoretical analysis of the guardianship concept from routine activity theory as it applies to online forms of victimization. *Journal of Contemporary Criminal Justice*, *32*(2), 148–168. https://doi.org/10.1177/1043986215621378

Rodriguez, J. A., Oduber, J., & Mora, E. (2017). Routine activities and cybervictimization in Venezuela. *Latin American Journal of Safety Studies*, *20*, 63–79.

Rosenbaum, P. R., & Rubin, D. B. (1983). The central role of the propensity score in observational studies for causal effects. *Biometrika*, *70*(1), 41–55. https://doi.org/10.1093/biomet/70.1.41

Rudner, L. (2016). *Accuracy of Bayes and logistic regression subscale probabilities for educational and certification tests*. https://doi.org/10.7275/Q7ZZ-D655

Saravanan, M., & Thilagaraj, R. (2014). Cyber crime spatial data analysis. *International Journal of Applied Sciences and Engineering Research*, *3*(2), 2277–8442.

Sarre, R., Lau, L. Y. C., & Chang, L. Y. C. (2018). Responding to cybercrime: Current trends. *Police Practice and Research*, *19*(6), 515–518.

Schneider, B., & McDonald, S. -K. (2010). Methods for approximating random assignment. In *International Encyclopedia of Education* (3rd ed.), (pp.97–103). Elsevier. https://doi.org/10.1016/B978-0-08-044894-7.01689-4

Sharton, B. (2020, March 16). *Will coronavirus lead to more cyber attacks?* Harvard Business Review. https://hbr.org/2020/03/will-coronavirus-lead-to-more-cyber-attacks

Shaver, B. (2020). *Covid-19, Cybercrime, and Capitol Hill*. Center for Strategic and International Studies. https://www.csis.org/blogs/technology-policy-blog/covid-19-cybercrime-and-capitol-hill

Smith, D., & Teague, K. (2020, December 4). When will COVID end? The update on the race for a vaccine. Retrieved August 1, 2020, from https://www.cnet.com/how-to/when-will-covid-end-the-update-on-the-race-for-a-vaccine/

Smith, T., & Stamatakis, N. (2020). Defining cybercrime in terms of routine activity and spatial distribution: Issues and concerns. *International Journal of Cyber Criminology*, *14*(2), 433–459. https://dx.doi.org/10.5281/zenodo.4769989

Smith, T., & Stamatakis, N. (2021). Cyber-victimization trends in Trinidad & Tobago: The results of an empirical research. *The International Journal of Cybersecurity Intelligence and Cybercrime*, *4*(1), 46–63. https://doi.org/10.52306/04010421JINE3509

Song, H., Lynch, M. J., & Cochran, J. K. (2016). A macro-social exploratory analysis of the rate of interstate cyber-victimization. *American Journal of Criminal Justice*, *41*(3), 583–601. https://doi.org/10.1007/s12103-015-9308-4

Stein, R. E. (2011). The contextual variation of routine activities: A comparative analysis of assault victimization. *International Journal of Humanities and Social Science*, *1*(10), 11–24.

Stickle, B., & Felson, M. (2020). Crime rates in a pandemic: The largest criminological experiment in history. *Just American Journal of Criminal Justice*, *45*(4), 525–536.

Superville, S. (2020, August 02). *Regional experts warn: Cyberthreats as dangerous as COVID-19*. Trinidad and Tobago Newsday. https://newsday.co.tt/2020/08/02/regional-experts-warn-cyber-threats-as-dangerous-as-covid19/

Taitt, R. (2018, June 4). Citizens lose $14M to cybercrime: 1,694 reports of bank card fraud in 2017. Trinidad Express. Retrieved from https://trinidadexpress.com/news/local/citizens-lose-m-to-cybercrime/article_f85b01fe-6859-11e8-915b-6b551b4fed14.html Turanovic, J. J., Pratt, T. C., & Piquero, A. R. (2018). Structural constraints, risky lifestyles, and repeat victimization. *Journal of Quantitative Criminology*, *34*(1), 251–274.

van Buuren, S., & Groothuis-Oudshoorn, K. (2011). mice: Multivariate imputation by chained equations in R. *Journal of Statistical Software*, *45*(3), 1–67.

van Ouytsel, J., Ponnet, K., & Walrave, M. (2018). Cyber dating abuse victimization among secondary school students from a lifestyle-routine activities theory perspective. *Journal of Interpersonal Violence*, *33*(17), 2767–2776. https://doi.org/10.1177/0886260516629390

van Wilsem, J. (2003). Crime and Context: The Impact of Individual, Neighborhood, City and Country Characteristics on Victimization (Dissertation, Radboud University Nijmegen). Radboud University Nijmegen, Netherlands. Retrieved from https://hdl.handle.net/2066/63843Wick, S. E., Nagoshi, C., Basham, R., Jordan, C., Kim, Y. K., Nguyen, A. P., & Lehmann, P. (2017). Patterns of cyber harassment and

perpetration among college students in the United States: A test of routine activities theory. *International Journal of Cyber Criminology*. https://doi.org/10.5281/zenodo.495770

Winter, D. (2020, July 24). *Current google search trends reveal coronavirus impacts on SEO*. Noble Studios. https://noblestudios.com/current-google-search-trends-coronavirus/

World Health Organization. (2020, April 23). *WHO reports a fivefold increase in cyber-attacks, urges vigilance*. World Health Organization - Newsroom. https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

Yar, M. (2005). The novelty of "cybercrime": An assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407–427.

Yucedal, B. (2010). Victimization in Cyberspace: An Application of Routine Activity and Lifestyle Exposure Theories (Kent State University). Kent State University, Kent, Ohio. Retrieved from http://rave.ohiolink.edu/etdc/view?acc_num=kent1279290984.