American Journal of Criminal Justice (2020) 45:546–562
https://doi.org/10.1007/s12103-020-09534-4

Cybercrime in America amid COVID-19: the Initial Results from a Natural Experiment

James Hawdon[1] · Katalin Parti[2] · Thomas E. Dearden[2]

Received: 4 May 2020 / Accepted: 29 May 2020 /
Published online: 10 June 2020

Abstract

The COVID-19 pandemic has radically altered life, killing hundreds of thousands of people and leading many countries to issue "stay-at-home" orders to contain the virus's spread. Based on insights from routine activity theory (Cohen & Felson 1979), it is likely that COVID-19 will influence victimization rates as people alter their routines and spend more time at home and less time in public. Yet, the pandemic may affect victimization differently depending on the type of crime as street crimes appear to be decreasing while domestic crimes may be increasing. We consider a third type of crime: cybercrime. Treating the pandemic as a natural experiment, we investigate how the pandemic has affected rates of cybervictimization. We compare pre-pandemic rates of victimization with post-pandemic rates of victimization using datasets designed to track cybercrime. After considering how the pandemic may alter routines and affect cybervictimization, we find that the pandemic has not radically altered cyberroutines nor changed cybervictimization rates. However, a model using routine activity theory to predict cybervictimization offers clear support for the theory's efficacy both before and after the pandemic. We conclude by considering plausible explanations for our findings.

Keywords Cybercrime · Cybervictimization · Routine activity theory · COVID-19 · Natural experiment

✉ James Hawdon
hawdonj@vt.edu

Katalin Parti
kparti@vt.edu

Thomas E. Dearden
tdearden@vt.edu

[1] Department of Sociology and Center for Peace Studies and Violence Prevention, Virginia Tech, Blacksburg, VA, USA

[2] Department of Sociology, Virginia Tech, Blacksburg, VA, USA

The COVID-19 pandemic has radically altered life. At the time of this writing, over 3 million cases had been confirmed and 234,000 people had died of the virus globally, and public health experts warn the pandemic has not yet peaked. In efforts to slow the virus' spread, many countries issued "stay-at-home" orders. In the US, the directives started in California in mid-March, and by mid-April, approximately 316 million people (95% of the population) in 43 states were ordered to stay at home (Mervosh, Lu, & Swales, 2020). Millions of Americans were told to avoid public places, K-12 schools were closed, colleges and universities shifted to online instruction, and millions of people lost their jobs. In short, COVID-19 has radically altered the routine activities of many people.

Given the well-known relationship between routine activities and criminal victimization, it is likely that COVID-19 will influence victimization rates. As people spend more time at home and less time in public, the convergence of motivated offenders, suitable targets, and guardians upon which criminal victimization depends (Cohen & Felson, 1979) is undoubtedly altered. Initial evidence suggests that murders, assaults, robberies, burglaries, and grand larceny thefts are declining, as major cities across the US report decreases ranging from 30% to 42% following the implementation of stay-at-home orders (Lederer, 2020; Coyne, 2020; Jacobs & Barrett, 2020; Shayegh & Malpede, 2020). These decreases are comparable to those of the great crime decline in the 1990s (Zimring, 2007) and similar to those reported in other nations (McDonald & Balkin, 2020). Yet, it is possible that not all crimes have decreased. For example, although it is too early to say with certainty, there is some evidence that domestic violence, intra-familial assaults, targeted violent crimes, as well as nuisance complaints–such as residential noise complaints—may have increased after stay-home orders, at least in some places (Mohler et al., 2020). Thus, the pandemic may affect victimization differently depending on the type of crime. As such, we investigate how COVID-19 has altered cybervictimization. Using datasets designed to track cybercrime, we compare pre-pandemic rates of victimization with post-pandemic rates of victimization. That is, the timing of our surveys vis-à-vis the pandemic create a natural experiment.

We begin by reviewing Cohen and Felson's (1979) routine activity theory (RAT). We then consider how the pandemic and result stay-at-home orders would likely alter people's routine activities and their likelihood of victimization. We then report the results of a negative binomial regression cybervictimization on a number of indicators of routine activities. Included in the model is a time variable (pre/post COVID) that captures the influence of the pandemic on victimization rates. We conclude by considering the implications of our findings. Our research is significant because, to our knowledge, it is the first theoretical consideration of how a pandemic can influence routine activities and the first empirical evidence concerning how cyber routines and cybervictimization have changed after the pandemic.

Literature Review

Routine Activity Theory

Routine activity theory (Cohen & Felson, 1979), which is the most influential theory of victimization (Miró, 2014), argues that for crime to occur, three necessary conditions must spatio-temporarily converge: (1) the presence of motivated offenders, (2) the

presence of a suitable target, and (3) the absence of a capable guardian. Routine activity theory proposes that victimization stems from the "recurrent and prevalent activities" that individuals are involved in, which in turn influence the likelihood that the three necessary factors are present (Cohen & Felson, 1979). Therefore, routines influence an individual's risk of being victimized.

While RAT cannot be directly applied to the online world (see Yar, 2005; Yar, 2013; Tillyer & Eck, 2009), the cyberlifestyle-routine activities perspective (see Reyns, Henson, & Fisher, 2011; Eck & Clarke, 2003) overcomes the primary issue limiting the theory's applicability. Most notably, while offline victimization requires a convergence in time and space of offenders and victims, cybervictims and offenders can come into virtual contact through their networked devices, and this contact can happen asynchronously (Leukfeldt & Yar, 2016; Reyns et al., 2011; Vakhitova, Reynald, & Townsley, 2015). With this modification in mind, online routine activities can increase the likelihood of victimization by bringing potential targets into virtual contact with offenders in environments lacking guardians (see Eck & Clarke, 2003; Reyns et al., 2011). Researchers have now applied RAT to a variety of types of cybervictimization, ranging from fraud and identity theft to harassment and other forms of cyberviolence (e.g., Bossler & Holt, 2009; Bossler, Holt, & May, 2012; Costello, Hawdon, Ratliff, & Grantham, 2016; Hawdon, Bernatzky, & Costello, 2019; Hawdon, Oksanen, & Räsänen, 2015; Hawdon, Oksanen, & Räsänen, 2017; Holt & Bossler, 2008; Holt & Bossler, 2013; Marcum, Higgins, & Ricketts, 2010; Navarro & Jasinski, 2012; Navarro & Jasinski, 2013; Pratt, Holtfreter, & Reisig, 2010; Reyns, 2013; Reyns & Henson, 2015; van Wilsem, 2011).

Studies using RAT to predict cybervictimization generally find that engaging in risky online behaviors such as downloading games and music from unknown websites, using file-sharing programs, instant messaging, opening unknown email attachments, and clicking on pop-up messages increases cyberharassment (Hinduja & Patchin, 2009; Marcum, 2009; Marcum et al., 2010; Navarro & Jasinski, 2012). Similarly, general computer use, anonymously confiding in others online, playing video games, spending time in chatrooms, online shopping, and the use of social networking sites, and adding strangers as friends to the social networking accounts have been reported to increase the likelihood of being a victim of cyberviolence (e.g. Bossler & Holt, 2009; Bossler et al., 2012; Costello et al., 2016; Hawdon, Oksanen, & Räsänen, 2014; Holt & Bossler, 2008; Leukfeldt & Yar, 2016; Navarro & Jasinski, 2012; Reyns et al., 2011; Reyns, Henson, & Fisher, 2016; van Wilsem, 2011). The use of target-hardening devices such as antivirus programs, firewalls, and filtering and blocking software can potentially reduce cybervictimization, although the effect may only apply to economic victimization (e.g., Leukfeldt, 2014; Marcum, 2008; Marcum et al., 2010).

COVID-19 and Changes in Cyber-Routines

As mentioned above, the stay-at-home orders enacted to combat the spread of COVID-19 have radically altered the daily routines or millions of Americans. With decreased mobility due to shelter-in-place orders, people are increasingly teleworking. According to one study, 88% of organizations have encouraged or required their employees to

work from home because of the pandemic (Gartner, 2020). In addition to more people relying on technology to telework, the use of social media sites such as TikTok, Twitter, Facebook, and Instagram are also spiking (Yitzhak, 2020). As we spend more time online, our cyber-routines change, and we would anticipate these changes would alter cybervictimization rates. But how specifically would the COVID-19 pandemic likely alter our proximity to motivated offenders, suitability as a potential target, and online guardianship? Let us speculate on each of these.

COVID-19 and Virtual Proximity to Motivated Offenders First, the unemployment rate has surged above 20% and is expected to reach levels not seen since the Great Depression, millions have lost their jobs, had their hours reduced, or have been furloughed, and the nation's small business owners are struggling to remain in business (Bartash, 2020; Lambert, 2020; Wolfer, 2020). As a revised version of RAT argues (see Bryant & Miller, 1997) areas with large secondary labor markets have high crime rates in part because workers in the secondary sector frequently experience unemployment, which may compel them to find alternative means of support. Thus, the radical shift in the employment structure of the nation to which these dire economic numbers attest has likely led to heightened economic need and increased motivations to steal. Combined with the increase in the number of people going online, we would anticipate an increase in the virtual presence of motivated offenders in cyberspace. *The increased presence of motivated offenders in cyberspace during the pandemic, assuming it is indeed the case, should increase overall rates of cybervictimization.* While this proposition is likely to be true, motivated offenders are a necessary but not sufficient condition for victimization. Indeed, Cohen and Felson (1979) assumed such offenders were omni-present, and this truism is probably even more enhanced in cyberspace because its asynchronous nature allows offenders to be "virtually present" even when they are not personally online. Thus, while more motivated offenders being online is likely to elevate rates of cybervictimization, the overall patterns are likely more affected by changes in target suitability and guardianship that result from the pandemic.

COVID-19 and Target Suitability Independent of the number of offenders prowling virtual space, the online routines of potential victims also shapes their likelihood of being victimized by determining a target's suitability. Suitable targets include any person or object that can fulfill the needs or wants of a motivated offender (Cohen & Felson, 1979), and target suitability is a function of VIVA: the target's *value*, *inertia*, *visibility*, and *access* (Felson & Clarke, 1998). Value is the worth a person or object has in the eyes of a potential offender, inertia is the target's ability to avoid the offender, access is the opportunity for an offender to commit the illegal act, and visibility is the extent to which offenders can see a possible victim. These factors are interrelated and also related to the extent of contact targets have with motivated offenders. It is likely that the pandemic would influence target suitability in several ways.

As noted above, the pandemic has resulted in people spending more time online. All things being equal, spending more time online would increase the potential victim's visibility to likely offenders. Indeed, research indicates that the proportion of users who access the internet only from home is positively related to cybertheft victimization (Song, Lynch, & Cochran, 2016). However, simply spending more time online may not necessarily result in a greatly enhanced probability of being victimized because overall

time spent online is likely less important than the specific online activities in which one engages. For example, spending 8 hours online teleworking is probably not likely to bring one into a virtual space where motivated offenders lurk. In contrast, spending even 1 hour surfing the dark web very well might increase one's exposure to motivated offenders. Thus, online activities that lead one to visit "dangerous virtual spaces" will increase a potential target's visibility and the offender's access more so than those activities that occur in more secure online spaces (see Costello, Barret-Fox, Bernatzky, Hawdon, & Mendes, 2018; Räsänen et al., 2016).

How the COVID-19 pandemic and resulting stay-at-home orders will likely affect target suitability is undoubtedly complex. For example, as previously mentioned, the limited available evidence suggests that some activities known to be related to victimization because they may lead users into dangerous virtual spaces have undoubtedly increased (Yitzhak, 2020). These "dangerous" online routines would include surfing the dark web, playing online video games, online shopping, and visiting social media sites as all of these activities have been reported to increase cybervictimization (Bossler & Holt, 2009; Bossler et al., 2012; Costello et al., 2016; Hawdon et al., 2014; Leukfeldt & Yar, 2016; Navarro & Jasinski, 2012; Reyns et al., 2011; van Wilsem, 2011). *All of these activities would increase the target's visibility and the offender's access, and we would anticipate that increases in these behaviors would result in higher rates of cybervictimization.* However, time spent performing other online routines, such as working online or reading the news, may have also increased due to the pandemic, but *these activities are unlikely to affect cybervictimization since they would not bring one into "dangerous" virtual spaces.*

Another factor that can influence target suitability by decreasing an offender's access and possibly increase the target's ability to avoid an attack (i.e. decrease the target's inertia) is the use of target-hardening devices. Some evidence suggests that the use of antivirus programs, firewalls, and filtering and blocking software can reduce the likelihood of becoming a victim of an economic cybervictimization; however, there is little evidence such devices can protect one from violent cybercrimes (see Holt & Bossler, 2008; Leukfeldt, 2014; Marcum et al., 2010). How the pandemic would influence the use of target-hardening devices is difficult to predict. While one would hope people would be more vigilant in terms of updating their anti-virus software and making sure their firewalls are set, the pandemic has probably not influenced the overall use of computer technology for those with high levels of computer skills since these people were probably frequent users prior to the pandemic. Instead, the pandemic has probably led to more inexperienced and unsophisticated computer users spending more time online. If this is the case, *we would predict that overall rates of economic cybervictimization should increase.* We note here that we would not expect violent cybercrimes to increase since these are reportedly unaffected by target-hardening devices.

COVID-19 and Guardianship Finally, another factor that patterns victimization is guardianship. Guardianship is "the presence of a human element which acts—whether intentionally or not—to deter the would-be offender from committing a crime against an available target" (Hollis, Felson, & Welsh, 2013: 76). The findings with respect to guardianship and cybercrime are inconsistent (e.g., Bossler & Holt, 2009; Leukfeldt &

Yar, 2016; Reyns, 2015), in part due to conceptual uncertainty across both study design and types of victimization (Vakhitova & Reynald, 2014). Yet, as argued by Costello, Hawdon, and Ratliff (2017), the virtual world is a truly socially disorganized community. In cyberspace, actors are truly transient as they come and go regularly, and they do so anonymously. Moreover, many online spaces have no way for anyone even trying to monitor the activity to intervene, and most offenders likely know this. Even sites that closely monitor activity and have policies to censor or delete material struggle to keep pace with the amount of activity that must be monitored. Moreover, online norms that would stimulate intervention on one's behalf tend to be weak and underdeveloped (see Costello et al., 2017). Thus, overall guardianship is always low online and the pandemic is unlikely to have changed that. *As such, we would not anticipate rates of cybervictimization to have changed due to any influence the pandemic would have had on cyber guardianship*.

Taking all of these factors together, we would anticipate an increase in cybervictimization amid the COVID-19 pandemic due to more motivated offenders, a change in some "dangerous" online routines, and perhaps less target-hardening. However, given that many online routines that have likely increased would not necessarily result in increased victimization and the fact that guardianship is likely unchanged by the pandemic (because it is always lacking online), any observed increase is expected to be modest.

The above discussion gives rise to the following hypotheses that will be tested using samples collected pre (November 2019) and post (April 2020) pandemic. First, as stated above, given the anticipated changes in online routines, we hypothesize (H1) *rates of cybervictimization will be modestly higher among post-COVID-19 respondents than they are among pre-COVID-19 respondents.* Next, as explained above, we anticipate the increase in victimization because people were forced to shift their daily activities online and radically enlarge their digital footprint. Thus, we hypothesize that (H2) *the extent to which respondents engage in online activities will be higher in the post-COVID-19 sample than in the pre-COVID-19 sample.* We now turn to our analysis.

Methods

Sample

Data were collected using online panels from *Dynata*. *Dynata* uses random digit dialing, banner ads, and other permission-based techniques to recruit respondents. From this database *Dynata* randomly invites panel members to participate in the survey. The sample was balanced based on US Census data to represent sex, ethnicity, and race. Online proportional sampling has been found to yield similar results as random probability-based samples due to several strategies (Weinberg, Freese, & McElhattan, 2014; Simmons & Bobo, 2015; contrast MacInnis, Krosnick, Ho, & Cho, 2018). First, both repeat participants and individuals who speed through the survey are eliminated to increase sample validity (Wansink, 2001; Evans & Mathur, 2005). In addition, the rewards offered by the panel company have been shown to increase validity of the overall data (see Wansink, 2001).

The first survey was fielded between November 24 and November 30, 2019 (pre-COVID-19 sample), and the second was fielded between April 14 and April 17, 2020 (post-COVID-19 sample). Overall, 1315 respondents began the pre-COVID-19 survey, but 81 respondents completed the survey in less than 3 min and were considered "speeders." They were removed from the sample. In addition, 125 participants did not complete the survey and were eliminated from the analysis. In total, 1109 respondents had usable data and were included in our analysis. In the post-COVID-19 sample, 1120 respondents began the survey, with 58 "speeders" who were dropped from the analysis. Dropping these respondents resulted in a sample of 1021 participants in the post-COVID-19 sample.

A comparison between the pre-COVID-19 and post-COVID-19 sample in terms of demographics can be found in Table 1. Of note was an expected increase in unemployment in the post-COVID-19 sample. In addition, the samples differed in average age and education, but did not differ in terms of racial/ethnic composition or gender.

Results

To examine the first hypothesis, we investigate rates of cybervictimization in the two samples. To measure cybervictimization, respondents were asked if they had been a victim of seven different types of cybercrime (see Table 4 for the types of crimes and survey items used to measure them). We created a summated variable of all victimization behaviors. This count variable reflected the number of different victimization experiences the participants had experienced in the past 12 months.

Even upon visual inspection we noticed that, if anything, victimization was slightly higher in the pre-COVID-19 sample. We examined victimization in relation to the samples using a negative binomial regression because our data are over-dispersed count data. We examined the differences between the samples by regressing victimization on a COVID-19 indicator variable (0 = pre-COVID-19; 1 = post-COVID-19). The COVID-19 indicator variable failed to reach standard levels of statistical significance, and the overall model had extremely low predictive power, with a Pseudo R^2 of <.001. As such, our first hypothesis is not supported, at least when we consider overall cybervictimization.

Given that certain types of cybercrimes may have increased while others decreased, we also examined specific victimization and self-protection behaviors between the pre and post-COVID-19 sample to help understand why we were not seeing a difference between the samples. We utilized χ^2 tests to consider differences between the samples. Types of victimizations tested included scams, identity theft, unknown transactions, notification from organizations about data theft, online bullying, online sexual harassment, and malware/viruses. Only one significant difference was found. The post-COVID-19 sample reported *fewer* notifications by companies that their data had been stolen ($\chi 2 = 7.97(1)$, $p = .005$). In the pre-COVID-19 sample 21% of respondents indicated they had been notified by a company about data loss whereas in the post-COVID-19 sample only 16% indicated they had been notified by a company about data loss.

We also examined differences in self-protection measure use in the pre/post-COVID-19 samples using similar χ^2 tests. Only one significant difference was found. While 70% of the post-COVID-19 sample indicated that they used virus

Table 1 Demographic and RAT Variable Sample Comparison

	Non COVID-19 Sample	COVID-19 Sample
Gender		
Male	49.50%	49.31%
Female	49.05%	50.10%
LGBTQ+	1.45%	0.60%
Education***		
Less than High School	2.71%	2.96%
High School	21.36%	15.48%
Some College	23.98%	21.01%
College Degree	35.02%	38.86%
Masters or Professional or higher	16.92%	21.70%
Race		
White	71.09%	72.09%
Black	14.18%	15.48%
American Indian	1.17%	0.89%
Asian	6.32%	5.72%
Hawaiian or Pacific Islander	0.81%	0.59%
Political Affiliation*		
% Conservative	33.87%	36.21%
% Liberal	29.85%	33.73%
% Moderate	36.28%	30.06%
Unemployment (Looking & Not Looking)***	29.99%	37.38%
Average Age***	42.66 (SD = 13.68)	46.50 (SD = 16.18)
% Who Spend Time on Dark Web in A Week	26.15%	21.90%

*$p < 0.1$; ** $p < 0.05$; ***$p < 0.01$

software or firewalls, only 66% of the pre-COVID-19 reported that they did ($\chi^2 = 3.97(1)$, $p = .046$). We advise caution in interpreting this result as the p value was close to .05 and we ran a total of 11 χ^2 tests, increasing the likelihood of a false positive. All victimization and self-protection difference tests can be found in Table 2.

To test our second hypothesis regarding differences in computer behaviors between the samples, we compared pre-COVID-19 and post-COVID-19 computer-related activities. These activities include playing online games, reading news or other articles online, browsing social media, using a computer while working, and shopping online. As seen in Table 3, only one activity, reading news or other online articles was significantly higher in the post-COVID-19 sample ($t = -4.4(2093)$, $p < .001$). Therefore, our second hypotheses is also not supported.

Given the failure of either of our hypotheses to be supported, we investigate if the RAT model still applies to cybervictimization in the post-COVID-19 world. Given the reported fourfold increase in cybercrimes during the pandemic (Cimpanu, 2020; England, 2020) yet our data not reflecting such an increase, we need to consider if

Table 2 Self-Reported Online Victimization and χ2 tests Comparing Pre and Post-COVID-19 Samples

	Respondents Who Reported Engaging in Past 12 Months		
	Pre- COVID-19 Sample	Post-COVID-19 Sample	χ2
Types of Victimization			
Lost money due to an email, website or other computer scam	122 11.16%	109 10.78%	$\chi2 = 0.07(1)$, $p = .780$
Had your identity used by someone else to start a bank account, credit card or loan	102 9.32%	90 8.91%	$\chi2 = 0.10(1)$, $p = .748$
Had unknown transactions in your bank/investment account, credit card, or other online payment system	199 18.16%	168 16.65%	$\chi2 = 0.82(1)$, $p = .363$
Received notification from a company or organization that your private information, such as name, social security, credit card or password, has been stolen or posted publicly	229 20.89%	163 16.11%	$\chi2 = .7.97(1)$, p = .005
Experienced hurtful comments, pictures or videos about you about posted online	120 10.95%	116 11.51%	$\chi2 = 0.16(1)$, $p = .685$
Experienced unwanted sexual comments or advances online	143 13.02%	127 12.55%	$\chi2 = 0.10(1)$, $p = .745$
Had a computer virus or malware that affected how your computer operated	134 12.20%	110 10.92%	$\chi2 = 0.84(1)$, $p = .359$
Self-Protection Enacted			
Cover your web camera on your camera or laptop	430 39.89%	424 42.44%	$\chi2 = 1.40(1)$, $p = .237$
Use identity theft protection monitoring	458 42.72%	439 44.03%	$\chi2 =0 .36(1)$, $p = .549$
Freeze your credit when you do not plan to use it	240 22.73%	247 24.90%	$\chi2 = 1.33(1)$, $p = .249$
Use virus software and/or firewalls on your computer	696 65.54%	691 69.66%	$\chi2 = 3.97(1)$, p = .046

our earlier theoretical understanding of what patterns victimization remains accurate. To do this, we turn to a test of RAT using our two samples.

To examine if RAT is an adequate predictor of cybervictimization, we included several variables in a negative binomial regression. The model included an index variable of pre/post-COVID-19 sample, time spent in the various online activities mentioned above, computer self-protection behaviors, and demographic variables. Table 4 reports the results of the analysis. Overall the model was significant ($p < .001$). Factors related to increased risk of victimization included dark web use per week (IRR = 1.14; $p < .001$), time reading online news/articles (IRR = 1.08; $p < .001$), time browsing social media (IRR = 1.04; $p < .05$) and age (IRR = 1.02; $p < .001$). Age was the only demographic factor to achieve statistical significance in the model. Factors significantly related to lower risk of victimization included time working on a computer (IRR = 0.95; $p < .005$) and all protective behaviors including covering a webcam (IRR = 0.70; $p < .001$), having identity theft protection (IRR = 0.78;

Table 3 T-Tests of Computer Activities and $\chi 2$ tests Comparing Pre and Post-COVID-19 Samples

In a typical weak how many hours do you spend[a]	Pre-COVID-19		Post-COVID-19		
	M	SD	M	SD	*t*-test
Playing online games	3.18	2.36	3.12	2.38	.6(2113)
Reading news or other articles online	3.33	1.79	3.70	1.95	−4.4(2093) ***
Browsing social media	3.84	2.16	3.99	2.25	−1.5(2104)
On a computer while working	3.62	2.75	3.77	2.84	−1.2(2102)
Shopping online	3.12	1.60	3.01	1.62	1.5(2106)
Other online activities	3.84	2.02	3.86	2.00	−.3(2100)

[a] Scale is nonlinear as hours were represented in increasing increments, 0, <1, 1–2, 2–4, 4–6, 7–8, 8–10, 10 or more

*$p < .05$, **$p < .01$, ***$p < .001$*

$p < .001$), freezing credit (IRR = 0.53; $p < .001$), and having virus protection (IRR = 0.74; $p < .001$). It is worth noting that the COVID index variable was still not significant.

While the COVID-19 indicator was again not significant, almost all of the RAT-specified variables were significant predictors in the model, and all of the relationships between these variables and cybervictimization were in the direction RAT would predict. It is also worth noting that age was the only demographic variable that was significantly related to cybervictimization. This finding is also supportive of RAT's argument that one's routines determine victimization. Finally, we tested to see if any interaction between the COVID-19 indicator variable and the RAT variables were significant to be certain that RAT applied equally well in the pre and post COVID-19 world. Results (not shown here) indicated that no interactions were significant, suggesting that indeed RAT still performs well as an explanation of cybervictimization even during the pandemic.

Discussion

To our knowledge, our study is the first empirical evidence concerning how the COVID-19 pandemic influenced cyber-routines and cybervictimization. We assumed that the pandemic and the results of stay-at-home orders would result in increased online presence, an increased level of routine activities online, and, as such, enhanced levels of target suitability and target proximity to motivated offenders. Consequently, we expected that rates of cybervictimization would be higher in the post-pandemic sample than what was observed in the pre-pandemic sample. The results show that we were clearly wrong. Based on our results, the stay-at-home orders did not radically alter our cyber-routines, and cybervictimization did not increase either. Instead, global levels of cybervictimization were nearly identical pre and post-pandemic, and only one type of victimization (being informed that your identity or private information had been stolen) changed. Moreover, this victimization decreased in the post-COVID-19 sample. Among the indicators of cyber-routine activities, including playing online games,

Table 4 Poisson Regressions predicting cyber-victimization index

Variable	Full Model			
	B	*SE(B)*	*p*	*IRR*
COVID (index)	−.009	.080		0.99
Dark Web Use	.127	.025	***	1.14
Time on Online Video Games	−.009	.020		0.99
Time Reading Online News/Articles	.076	.025	***	1.08
Time Browsing Social Media	.043	.022	*	1.04
Time Working on a Computer	−.056	.018	***	0.95
Time Shopping Online	.053	.031		1.05
Computer Familiarity	−.027	.037		0.97
Cover Webcam	−.362	.089	***	0.70
Use Identity Theft Protection	−.251	.086	***	0.78
Freeze Credit	−.637	.093	***	0.53
Use Virus Protection	−.299	.099	***	0.74
Age	.023	.037	***	1.02
Education	.051	.045		1.05
Male (index)	.117	.088		1.12
White (index)	.011	.092		1.01
Unemployed (index)	−.114	.111		0.89
Income	−.008	.029		0.99
Constant	−45.043	7.217	***	
Pseudo R^2	.09			
LR Chi^2	375 ($n = 1650$)			

*$p < 0.1$; ** $p < 0.05$; ***$p < 0.01$

reading news or other articles online, browsing social media, using a computer while working, and shopping online, only reading news or other online articles increased. One online activity, online shopping, even decreased in the post-COVID-19 sample.

We also wanted to see if specific types of victimization and protection behaviors changed after the pandemic. Among all the specific victimization variables, only one showed a significant difference: there was less notification from companies concerning data theft in the post-COVID-19 sample. In terms of target-hardening behaviors, participants reported using more self-protection (i.e. virus software and a firewall) in the post-COVID-19 sample. Thus, while there were minor differences between the samples, contrary to our expectations and FBI reports (Cimpanu, 2020; England, 2020), our data show that the pandemic has not radically altered our cyber-routines or levels of cybervictimization.

Fearing RAT may not apply in the post-pandemic virtual world, we tested it with a negative binominal regression. Our model showed dark web use, time spent online reading newspapers and other articles, and time using social media significantly increased the likelihood of being a cyber victim. Time spent working on a computer,

protective behaviors such as covering the webcam, having identify theft protection, freezing credit, and having virus protection were all inversely related to the likelihood of victimization. These results clearly support RAT, and the insignificance of the COVID index variable or any interactions between it and the various cyber-routines indicate that the theory applies equally well in the pre and post COVID-19 world.

Although cybervictimization has not changed substantially, our binominal regression model indicates that RAT can account for patterns of cybervictimization in both pre and post-pandemic samples. So why were our expectations so wrong? First, proximity to motivated offenders may have increased as people went online to work, study, and network, but target suitability did not increase as, according to our results, people likely used online platforms similarly to how they had before the pandemic. Most of their online behaviors did not put them at more than average risk of victimization. There was no evidence that dangerous online behaviors such as dark web use, online shopping, or visiting social media platforms changed significantly after the pandemic. Indeed, our data suggest users abandoned online activities such as online shopping that would pose risk to their bank accounts. Instead, it seems that people kept their cyber-routines concentrating on less dangerous routine activities, such as working online and reading news articles. The online routine activity that significantly increased was reading online news, but that activity would not heighten victimization as most traditional online news sites are reputable and do not increase their readers' target suitability.

We also expected that the overall rates of cybervictimization, and especially economic cybervictimization, would increase because of the nation's swift shift to the virtual world likely did not leave time for users to upgrade their computer security measures (e.g. firewalls, anti-virus software, etc.). While more computer savvy users likely have security measures already installed, those with fewer computer skills could be more vulnerable now that they are spending more time online. However, our data indicated that more people engaged in target-hardening measures and cybervictimization was unrelated to computer familiarity. A plausible explanation for this is that workers' relatively unfamiliar with computers were moved online by their companies who provided sufficient IT support. We cannot say this happened, but it is likely that corporations were keenly aware that some of their less-than-tech-savvy employees who were now teleworking needed support and failing to do so could put their company at heightened risk.

Indeed, there is reason to suspect there was heightened concern about cybercrime and possibly greater vigilance practiced to protect oneself from it. For example, the FBI noted how cybercriminals would likely target both companies and individuals working from home via teleworking software, education technology, and business email platforms. On April 15, the US Departments of State, Homeland Security, and Treasury, and the FBI issued an advisory to raise awareness of the cyber threat posed by North Korea's malicious cyber activities, a significant threat to the integrity and stability of the international financial system (US CERT, 2020). On April 20, the FBI Charlotte warned (FBI Charlotte, 2020) social media users to pay attention to trending social media topics (e.g. high school support photo trend, posting a picture of your first car, answering questions about your best friend, providing the name of your first pet, identifying your first concert, etc.), which might collect users' personal information, including passwords to reset accounts and gain access to protected data. Thus, it is possible that these warnings worked. While we lack the data to adequately test if

companies' policies attempted to protect their users or the government warnings worked, this possibility should be further explored by future research.

Our data allows us to say that the relative unchanged nature of our respondents' "dangerous" cyber-routines combined with their use of stronger security measures such as antivirus software and firewalls likely kept cybervictimization low, even if there was elevated motivation among offenders due to souring rates of unemployment and economic struggles. We can also say that our findings contradict recent reports about heightened levels of cybercrime being reported to the FBI (Cimpanu, 2020; England, 2020; IC3, 2020). Like us, the FBI anticipated that virtual environments will be increasingly affected adversely by cybercriminals, and as of March 30, 2020 (IC3, 2020), their data gives credence to their fears. The FBI Internet Crime Complaint Center (IC3) reports receiving more than 1200 complaints related to COVID-19 scams, including phishing campaigns against first responders, DDoS attacks against government agencies, ransomware against medical facilities, and fake COVID-19 websites downloading malware to users' computers. In total, the FBI reports cybercrimes have quadrupled during the COVID-19 pandemic (Cimpanu, 2020; England, 2020).

How do our results showing decreased cybervictimization make sense when cybercrime has an upward trend in the news and in FBI reports? It might just show the usual discrepancies between official crime statistics relying on reporting and victimization surveys. It is well documented how official statistics seriously underestimate crime rates. What we might be seeing is that while rates of crime are actually unchanged, rates of reporting crimes is increasing.

The repeated warnings of federal and state law enforcement and international policing agencies about the expected increase in cyber-offending may alert people and lead them to the dangers of cybercrime. This heightened awareness would then lead them to notice and report these crimes more than they did prior to the pandemic. Another possibility is that the increased rates of reporting to the FBI are more due to attacks on companies than on individual users. Our data focused on individual, not corporate, victimization. Thus, because our survey only included individual level cybervictimization while ignoring attacks on companies and critical infrastructures, we may not be detecting the increase in cybercrimes through our victimization surveys. This possibility should also be investigated by future researchers.

Conclusion

Our lives have been radically altered by a pandemic that is considered to be among the most widespread in history. The change in our daily routines appears to have resulted in an abrupt drop in street crimes. However, the shift to the digital world undoubtedly creates new opportunities and platforms for motivated offenders to engage in various illegal activities. This shift should increase the number of suitable targets, as millions of people are confined to their homes and forced to work, study, and socialize online. The current shift was swift, but, at least according to our data, this shift apparently did not result in people being more affected by cybercrime. They may be reporting more of it, but it is also possible that the pandemic has led to a decrease in most street crimes, an increase in domestic crimes, and no change in cybercrimes.

The reasons of the crime drop experienced all over the world in the 1990s (Pope & Pope, 2012) is still debated (Rosenfeld & Messner, 2012) and is indeed a complex issue. It is likely the current crime trends will be studied and debated for some time too. Our aim here was simply to provide one piece of evidence that will hopefully significantly contribute to that future analysis and debate.

We live in unprecedented times. We did not, nor can we, measure every possible underlying reason why cybervictimization occurs. We cannot predict if cybervictimization will remain low as social distancing continues. However, we can say that routine activities theory appears to still apply. We live in unprecedented times, but we still have theories to help us make sense of them.

Acknowledgements This research was funded by the Center for Peace Studies and Violence Prevention at Virginia Tech (Grant number 025-19), The Institute for Culture, Society, and Environment at Virginia Tech, and The Integrated Security Destination Area at Virginia Tech.

References

Bartash, J. (2020). Unemployment rate could approach great depression-era levels. MarketWatch (April 6, 2020). https://www.marketwatch.com/story/the-soaring-us-unemployment-rate-could-approach-great-depression-era-levels-2020-04-03. Accessed 25 Apr 2020.

Bossler, A. M., & Holt, T. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology, 3*(1), 400–420.

Bossler, A. M., Holt, T. J., & May, D. C. (2012). Predicting online harassment: Victimization among a juvenile population. *Youth & Society, 44*(4), 500–523.

Bryant, K. M., & Miller, J. M. (1997). Routine activity and labor market segmentation. An empirical test of a revised approach. *American Journal of Criminal Justice, 22*(1), 71–100.

Cimpanu, C. (2020). FBI says cybercrime reports quadrupled during COVID-19 pandemic, April 18, 2020, ZDNet.com, https://www.zdnet.com/article/fbi-says-cybercrime-reports-quadrupled-during-covid-19-pandemic/. Accessed 20 Apr 2020.

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

Costello, M., Barret-Fox, R., Bernatzky, C., Hawdon, J., & Mendes, K. (2018). Predictors of viewing online extremism among America's youth. *Youth & Society, 52*, 710–727. https://doi.org/10.1177/0044118X18768115.

Costello, M., Hawdon, J., & Ratliff, T. (2017). Confronting online extremism: The effect of self-help, collective efficacy, and guardianship on being a target for hate speech. *Social Science Computer Review, 35*(5), 587–605.

Costello, M., Hawdon, J., Ratliff, T., & Grantham, T. (2016). Who views online extremism? Individual attributes leading to exposure. *Computers in Human Behavior, 63*, 311–320.

Coyne, M. (2020). Crime rates across U.S. drop amid the coronavirus pandemic, Forbes (April 11, 2020), https://www.forbes.com/sites/marleycoyne/2020/04/11/crime-rates-across-us-drop-amid-the-coronavirus-pandemic/#3cb596c9311e. Accessed 3 May 2020.

Eck, J. E., & Clarke, R. V. (2003). Classifying common police problems: A routine activity theory approach. In M. J. Smith & D. B. Cornish (Eds.), *Crime prevention studies: Vol. 16. Theory and practice in situational crime prevention* (pp. 7–39). Monsey, NY: Criminal Justice Press.

England, R. (2020). FBI sees cybercrime reports increase fourfold during COVID-19 outbreak. *Engadget* (April 20, 2020), https://www.engadget.com/fbi-cybercrime-complaints-increase-fourfold-covid-19-091946793.html. Accessed 25 Apr 2020.

Evans, J. R., & Mathur, A. (2005). The value of online surveys. *Internet Research, 15*(2), 195–219.

FBI Charlotte. (2020). FBI Charlotte warns popular social media trends can lead to fraud, *FBI Charlotte* (April 20, 2020), https://www.fbi.gov/contact-us/field-offices/charlotte/news/press-releases/fbi-charlotte-warns-popular-social-media-trends-can-lead-to-fraud. Accessed 25 Apr 2020.

Felson, M., & Clarke, R. V. (1998). Opportunity makes a thief. Police research series paper 98, Policing and Reducing Crime Unit, Research Development and Statistics Directorate, London: British Home Office Research Publications, https://ugeb.pw/p_xek_seker.pdf. Accessed 3 May 2020.

Gartner. (2020). Gartner HR survey reveals 88% of organizations have encouraged or required employees to work from home due to coronavirus, Gartner (March 19, 2020) https://www.gartner.com/en/newsroom/press-releases/2020-03-19-gartner-hr-survey-reveals-88%2D%2Dof-organizations-have-e. Accessed 3 May 2020.

Hawdon, J., Bernatzky, C., & Costello, M. (2019). Cyber-routines, political attitudes, and exposure to violence-advocating online extremism. *Social Forces, 98*(1), 329–354.

Hawdon, J., Oksanen, A., & Räsänen, P. (2014). Victims of online hate groups: American youth's exposure to online hate speech. In J. Hawdon, J. Ryan, & M. Lucht (Eds.), *The causes and consequences of group violence: From bullies to terrorists* (pp. 165–182). Lanham, MD: Lexington Books.

Hawdon, J., Oksanen, A., & Räsänen, P. (2015). Online extremism and online hate: Exposure among adolescents and young adults in four nations. *Nordicom-Information, 37*(3–4), 29–37.

Hawdon, J., Oksanen, A., & Räsänen, P. (2017). Exposure to online hate in four nations: A cross-national consideration. *Deviant Behavior, 38*(3), 254–266.

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

Hollis, M. E., Felson, M., & Welsh, B. C. (2013). The capable guardian in routine activities theory: A theoretical and conceptual reappraisal. *Crime Prevention and Community Safety, 15*(1), 65–79.

Holt, T., & Bossler, A. M. (2008). Examining the applicability of lifestyle routine activities theory for cybercrime victimization. *Deviant Behavior, 30*(1), 1–25.

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

IC3. (2020). Cyber actors take advantage of COVID-19 pandemic to exploit increased use of virtual environments. FBI Internet Crime Complaint Center (April 1, 2020), https://www.ic3.gov/media/2020/200401.aspx. Accessed 25 Apr 2020.

Jacobs, S., & Barrett, D. (2020). New York City's crime rate plummets amid coronavirus shutdown. *The Washington Post* (March 26, 2020), https://www.washingtonpost.com/world/national-security/coronavirus-new-york-city-crime/2020/03/26/6a408e94-6f9a-11ea-a3ec-70d7479d83f0_story.html. Accessed 25 Apr 2020.

Lambert, L. (2020). Real unemployment rate soars past 20% and the US has now lost 26.5 million jobs. *Fortune, (April 23, 2020);* https://fortune.com/2020/04/23/us-unemployment-rate-numbers-claims-this-week-total-job-losses-april-23-2020-benefits-claims/. Accessed 25 Apr 2020.

Lederer, E. M. (2020). Crime rates plummet around the world as the coronavirus keeps people inside, *Time* (April 11, 2020), https://time.com/5819507/crime-drop-coronavirus/. Accessed 17 Apr 2020.

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior and Social Networking, 17*(8), 551–555.

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

MacInnis, B., Krosnick, J., Ho, A. S., & Cho, M. (2018). The accuracy of measurements with probability and nonprobability survey samples: Replication and extension. *Public Opinion Quarterly, 82*(4), 707–744.

Marcum, C. D. (2008). Identifying potential factors of adolescent online victimization for high school seniors. *International Journal of Cyber Criminology, 2*(2), 346–367.

Marcum, C. D. (2009). *Adolescent online victimization: A test of routine activities theory*. El Paso, TX: LFB Scholarly Publishing.

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behavior, 31*(5), 381–410.

McDonald, J. F., & Balkin, S. (2020). The COVID-19 and the decline in crime. *Social Science Research Network Electronic Journal*. https://doi.org/10.2139/ssrn.3567500.

Mervosh, S., Lu, D., & Swales, V. (2020). See which states and cities have told residents to stay at home, The New York Times (April 7, 2020), https://www.nytimes.com/interactive/2020/us/coronavirus-stay-at-home-order.html. Accessed 20 Apr 2020.

Miró, F. (2014). Routine activity theory. In J. M. Miller (Ed.) The encyclopedia of theoretical criminology, 1–7. Wiley Online Library, https://doi.org/10.1002/9781118517390.wbetc198. Accessed 3 May 2020.

Mohler, G., Bertozzi, A. L., Carter, J., Short, M. B., Sledge, D., Tita, G. E., Uchida, C. D., & Brantingham, J. (2020). Impact of social distancing during COVID-19 pandemic on crime in Indianapolis. *Journal of Criminal Justice*, In Press, *68*, 101692.

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

Navarro, I. N., & Jasinski, J. L. (2013). Why girls? Using routine activities theory to predict cyberbullying experiences between girls and boys. *Women & Criminal Justice, 23*(4), 286–303.

Pope, D. G., & Pope, J. C. (2012). Crime and property values: Evidence from the 1990s crime drop. *Regional Science and Urban Economics, 42*(1–2), 177–188.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47*(3), 267–296.

Räsänen, P., Hawdon, J., Holkeri, E., Näsi, M., Keipi, T., & Oksanen, A. (2016). Targets of online hate: Examining determinants of victimization among young Finnish Facebook users. *Violence and Victims, 31*(4), 708–726.

Reyns, B. (2013). Online routines and identity theft victimization further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency, 50*(2), 216–238.

Reyns, B. (2015). A routine activity perspective on online victimization: Results from the Canadian general social survey. *Journal of Financial Crime, 22*(4), 396–411.

Reyns, B., & Henson, B. (2015). 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*(10), 1119–1139.

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.

Reyns, B. W., Henson, B., & Fisher, B. S. (2016). 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*, 148–168. https://doi.org/10.1177/1043986215621378.

Rosenfeld, R., & Messner, S. F. (2012). The crime drop in comparative perspective: The impact of the economy and imprisonment on American and European burglary rates. In J. van Dijk, A. Tseloni, & G. Farrell (Eds.), *The international crime drop. crime prevention and security management* (pp. 200–228). London: Palgrave Macmillan.

Shayegh, S., & Malpede, M. (2020). Staying home saves lives, really! *Social Science Research Network Electronic Journal* https://doi.org/10.2139/ssrn.3567394.

Simmons, A., & Bobo, L. (2015). Can non-full-probability internet surveys yield useful data? A comparison with full-probability face-to-face surveys in the domain of race and social inequality attitudes. *Sociological Methodology, 45*(1), 357–387.

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.

Tillyer, M. S., & Eck, J. E. (2009). Routine activities. In J. M. Miller (Ed.), *21st century criminology: A reference handbook* (pp. 279–287). New York: Sage.

US CERT (2020). North-Korean cyber threat, US CERT (April 15, 2020), https://www.us-cert.gov/ncas/alerts/aa20-106a. Accessed 20 Apr 2020.

Vakhitova, Z., & Reynald, D. (2014). Cyberguardians: An empirical study of guardianship against cyber abuse. *International Journal of Cyber Criminology, 8*, 156–171.

Vakhitova, Z., Reynald, D., & Townsley, M. (2015). Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice, 32*(2), 169–188.

van Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology, 8*(2), 115–127.

Wansink, B. (2001). Editorial: The power of panels. *Journal of Database Marketing and Customer Strategy Management, 8*(3), 190–194.

Weinberg, J., Freese, J., & McElhattan, D. (2014). Comparing data characteristics and results of an online factorial survey between a population-based and a crowdsource-recruited sample. *Sociological Science*. https://doi.org/10.15195/issn.2330-6696.

Wolfer, J. (2020). The unemployment rate is probably around 13 percent. *The New York Times,* (April 3, 2020); https://www.nytimes.com/2020/04/03/upshot/coronavirus-jobless-rate-great-depression.html; Accessed 3 May 2020.

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

Yar, M. (2013). *Cybercrime and society*. London: Sage.

Yitzhak, Y. (2020). Social media interest is spiking worldwide—Except for Linkedin. *The Next Web*. (April 2, 2020); https://thenextweb.com/socialmedia/2020/04/02/social-media-interest-spiking-coronavirus-except-linkedin/. Accessed 17 Apr 2020.

Zimring, F. E. (2007). *The great American crime decline*. Oxford: Oxford University Press.

James Hawdon : is a professor of sociology and Director of the Center for Peace Studies and Violence Prevention at Virginia Tech. He researches how communities influence the causes and consequences of violence. Most recently, he has focused on how online communities influence political polarization, online hate, extremism, and cybercrime. He has been funded by the National Science Foundation, the National Institute of Justice, the National Consortium on Violence Prevention, and several other agencies. He has published or edited eight books and over 100 articles and technical reports.

Katalin Parti : is assistant professor of sociology at Virginia Tech. Dr. Parti's research focuses on cybercrime and online bullying. She evaluated cyberbullying programs of the Massachusetts Aggression Reduction Center as a Fulbright Fellow, and was awarded the European Safety and Prevention Award for channeling academic research results to schools. She has published in peer-reviewed journals such as the Pediatrics, the International Journal of Cybersecurity Intelligence & Cybercrime, the European Journal of Crime Criminal Law and Criminal Justice, and the Journal of Contemporary European Research.

Thomas Dearden : is assistant professor of sociology at Virginia Tech. Dr. Dearden specializes in research technology and crime, and corporate crime. He has conducted research for organizations across the globe, including the Polynesian Cultural Center in Hawaii, Food for Life Vrindavan in Uttar Pradesh, India, and Pay Tel in North Carolina. He has published his research in peer-reviewed journals including *The Journal of Financial Crime* and *The Journal of Investigative Psychology and Offender Profiling* and has presented at a dozen different conferences.