Commentary or Perspective: Opportunities to Leverage the Use of Global Public Health Innovative Research Technology in Combatting Cybercrime

Stan Mierzwa
Kean University

Lauren Spath-Caviglia
Kean University

Iassen Christov
Kean University

Recently while near my hometown baseball field, I was reminded of the Little League Pledge. Players traditionally recited the pledge prior to the start of a baseball or softball game; two lines particularly stood out to me, they were "I will play fair and strive to win. But, win or lose, I will always do my best." The first line mentioned got us thinking about the pandemic and rise in cybercrime. Why are there persons willing to partake in cybercrime, taking advantage of the situation the pandemic has created, and not playing fair? Can cybersecurity researchers utilize similar efforts or strategies used by the global public health to combat cybercrimes, during difficult causal situations? This paper will outline a subset of current research taking place concerning cybercrime and COVID-19 through a rapid literature review, bring to light strategies and technologies that can be used to complement the research, and bring a call to action for researchers and practitioners to give this topic greater attention, awareness, and more knowledge and focus.

Keywords: cybercrime, cybersecurity, self-report interviewing, computer-assisted-self-interviewing, Global Public Health Research

INTRODUCTION

With the pandemic having taken full action in the United States during March 2020, overall crime had taken a drop in various sectors and parts of the country. In a five-week change in crimes occurring at restaurants in Chicago by 74% reduction, while city-wide crime declined 35% (Pietrawska, et al., 2020). In another example, internationally, crime during a five-week period after government restrictions on activities began an 8.8% observation drop in reported crime (Gerell, et al., 2020). With a reduction in certain crimes, the news and trade press continued to express concerns about increasing cybercrimes. Cybersecurity professionals surveyed by the Enterprise Strategy Group (ESG) and the Information Systems Security Association International (ISSA) found that COVID-19 has led to an increase in cyber-attacks (Olstik, 2020).

At the beginning of the spread of COVID-19, RISKIQ, the attack surface management firm, quickly reported over 309,000 spam phishing emails (between April 11-13, 2020) with the subject lines of "COVID-19 updates" or "COVID-19 tracker in your city" and were designed to lure victims into clicking on an attachment (Khan, et al., 2015).

Another cybercriminal activity that was inspired by COVID-19 victimized persons who downloaded the Android app, named CovidLock. Users who installed the app would have experienced a ransomware event. The app was created to monitor heat map visuals and statistics on COVID-19. Installation of the app required users to allow the app certain permissions on the Android device. The false or malware app would lock user contacts, pictures, videos, and access to social media accounts on the unsuspected device (Whiteney, 2020).

With increased cybercrimes related to COVID-19, many of these events resulted from offenders partaking in the opportunity. As a result, this paper is a call to action for researchers to understand better such causal factors that lead to cybercrime and what can be done to curtail it the next time a significant event takes place globally. Are there opportunities to learn more about the behavioral aspects that led to individuals committing cybercrimes? What inspired and caused the impetus? At first, one may consider the thought of researching behavioral considerations of hackers to be naïve, perhaps it is. However, if a new approach or consideration for minimizing cybercrime just a bit evolves, by doing behavioral research, this would be one small positive step.

To determine behavioral actions related to cybercrimes, a method to obtain the most truthful answers to the committers' targeted questions is required. In order to obtain forward responses, there are opportunities to utilize innovative computerized interviewing technologies that may assist. These technologies could be utilized to ensure privacy is maintained, anonymous responses, and comfort and safety in knowing that the technology is trusted.

This paper will help outline potential tools and interviewing strategies that researchers can utilize to understand better the myriad of research questions that can be answered using proven technology tactics. Some of the technologies will be adopted from use in other research studies that require individual privacy and protection in answering questions related to public health and risky types of actions and behaviors. The research could be done with both the victims of crimes but equally and possibly even more importantly and to the extent possible, the perpetrators of the criminal activity.

METHODS

There exist many options for searching in the academic and trade press literature. In our rapid literature review, we present the results of a search for relevant articles pertaining to the COVID-19 pandemic situation and cybersecurity. Our focused areas of search include the online services ProQuest, EBSCO, and Google Scholar. ProQuest includes research material provided in over 40 databases in a large number of subjects. EBSCO is considered one of the leading providers of research databases and provides access to over an estimated 375 full-text databases. Google Scholar is considered one of the largest academic search engines in the world. Recent estimates suggest that Google Scholar covers 80-90% of coverage of all articles published in the English language.

Research Database Search Procedure Steps

Advanced searches were performed on all three selected online publication search engines. The searches included analyzing full-text, title, and abstract in each of the online databases. Google Scholar searches were performed using the online website and involved utilizing the "Sort by date" and clicking on the "Abstracts" button after an initial return of results to refine to only an abstract-related search. The multidisciplinary EBSCOhost Academic Search Premier service was searched with the same assigned criteria as used in the other services. A "Full text" search button feature as well as an "Abstracts" search feature function was utilized. As in the case of EBSCOhost, ProQuest database access was provided through the Kean University Library. Similarly to EBSCOhost, "Full text" and "Abstract" button functions were utilized to narrow down the assigned searches.

Rapid Literature Review

Increases in Cybercrime During COVID-19

From the early days of the COVID-19 pandemic as it hit the United States, there were reports of cyber threats and fraudulent activity. As the lockdowns began to occur, an increasing number of citizens were online more frequently and for longer periods, thus providing an opportunity for threat actors to attempt cybercriminal behavior. Between February and March, phishing cyberattacks increased from 36% to 64%, Distributed Denial of Service attacks jumped from 46% to 54% between Feb-March and March-April, Remote Desktop Protocol (RDP) attacks increased from 45% to 55% between Feb-March (Hakak et al., 2020). Cybercriminals will look for new vectors or weaknesses that exist or are known as easy and "low-hanging fruit" to exploit. Very quickly, at the onset of the COVID-19 pandemic, cybercriminals found simple methods to breach online Zoom virtual meetings.

Ironic Considerations With Increases in Cybercrime

An in-depth survey on the impact of the COVID-19 pandemic on cybersecurity highlighted certain results that appeared ironic, given the increases in cybercrime as resulting from this extreme event. Simultaneously as organizations reported in the survey that they witness a 63% jump in cyberattacks, 39% responded they are very prepared, and 34% just prepared in securing their devices and applications while staff is at home. When posed the question on spending expectations, 41% responded they do not expect any increases due to COVID-19, and even more curious, 26% said they expect less spending than budgeted. Although this survey was done very early on in the pandemic, this draws attention to whether increases in cybercrime will just continue (Olstik, 2020).

Protection of Data and Technology

A fundamental heavy-lift change has occurred concerning office workers operating remotely during and currently continuing with the emergence of COVID-19. Enterprises' online and remote-enabled systems and services must be resilient against cyberattacks (Deo, et al., 2020). In this article, the key points that are looked at are the pandemics' effects on global businesses and ways that an organization can better protect their data and technology. Cybercriminals are working diligently now more than ever to attempt to find weaknesses or vulnerabilities that they can expose to gain access to companies' private networks. Several pandemic results related to the protection of data and technology include that some organizations will need to move to a new operating model, including remote worker monitoring. Another important result is that new cyber risks that appeared during the pandemic will need to be further studied and understood (Deo, et al., 2020). With a remote working model becoming more of the norm for those positions that permit or can function, employee trust will be crucial. Interestingly, in a report from the data security company, Tessian, 91% of the IT leaders say they trust their employees to follow security best practices while out of the office. However, in the same study, 48% of employees admit they are less likely to because they may not be working on their usual devices (Carter, 2020).

Global Cybercriminal Statistics

Recently INTERPOL published a guide for criminal justice statistics on cybercrime activity. The report reinforced the notion that although many excellent practices are in place at a national level for collecting statistics on cybercrime, there exist very few such systems in place on the global level (INTERPOL, 2020). With this need, INTERPOL is directing to aggregate cybercrime data and statistics using its Cyber Analytical Platform (INTERPOL, 2020). Regarding this commentary paper's focus on pursuing greater knowledge on the cybercrime initiations reasons, it would be valuable to include data points related to the offender's reasons and initial drive for cybercrime activity.

DATA FINDINGS

Organizations are composed of information technology departments, which oversee the installation and maintenance of computer network systems within an organization. However, as organizations progressively depend on technology to run their day-to-day operations, the risk of cybercrimes is increasing. According to the Identity Theft Resource Center's 2019 End-of-Year Data Breach Report, on average, in 2019, an organization fell victim to ransomware every 14 seconds.

Currently, COVID-19 has impacted the world; these COVID-19 disruptions have affected organizations' information technology systems. The domino effect of COVID-19 has brought to the forefront two significant areas into questions for a majority of organizations': 1. cybersecurity preparedness and awareness and 2. the protection of data and technology. To answer these two questions, our team conducted a content analysis, which consisted of a full-text search of databases with the terminology of COVID-19, cybersecurity, or cybercrime. This resulted in the following findings:

FIGURE 1
PROQUEST LITERATURE REVIEW DATA RESULTS AS OF 10/19/2020

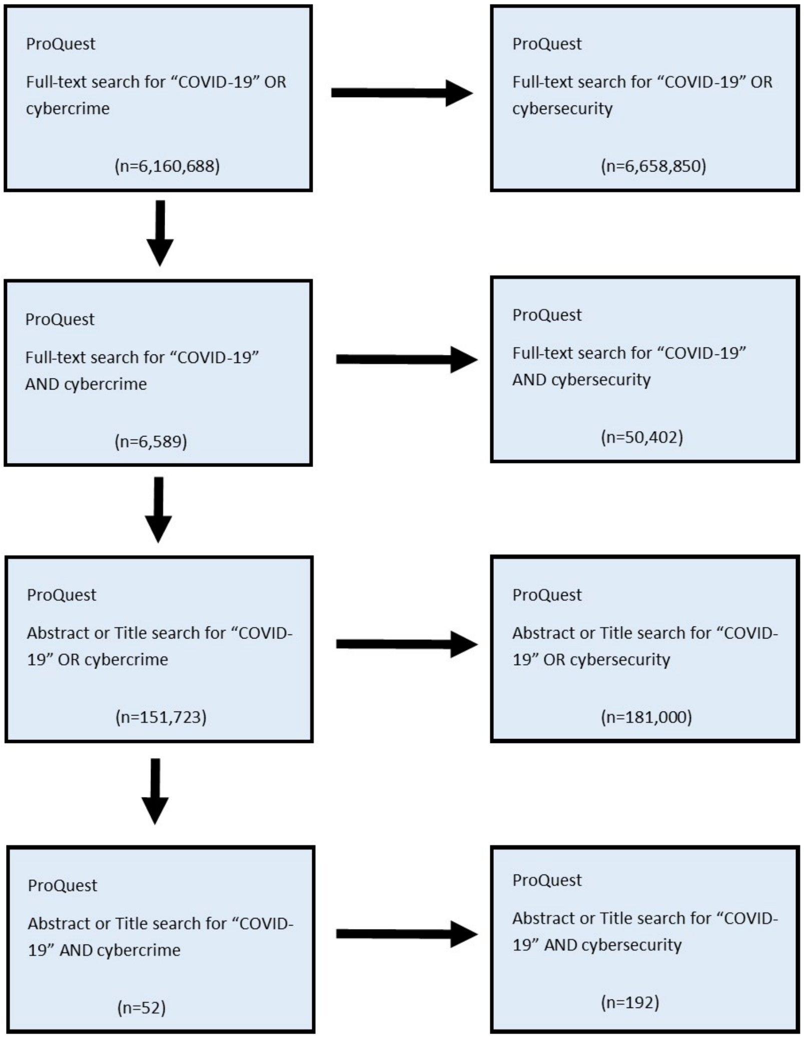

ProQuest
Full-text search for "COVID-19" OR cybercrime
(n=6,160,688)
ProQuest
Full-text search for "COVID-19" OR cybersecurity
(n=6,658,850)
ProQuest
Full-text search for "COVID-19" AND cybercrime
(n=6,589)
ProQuest
Full-text search for "COVID-19" AND cybersecurity
(n=50,402)
ProQuest
Abstract or Title search for "COVID-19" OR cybercrime
(n=151,723)
ProQuest
Abstract or Title search for "COVID-19" OR cybersecurity
(n=181,000)
ProQuest
Abstract or Title search for "COVID-19" AND cybercrime
(n=52)
ProQuest
Abstract or Title search for "COVID-19" AND cybersecurity
(n=192)

FIGURE 2
EBSCO HOST LITERATURE REVIEW DATA RESULTS AS OF 10/19/2020

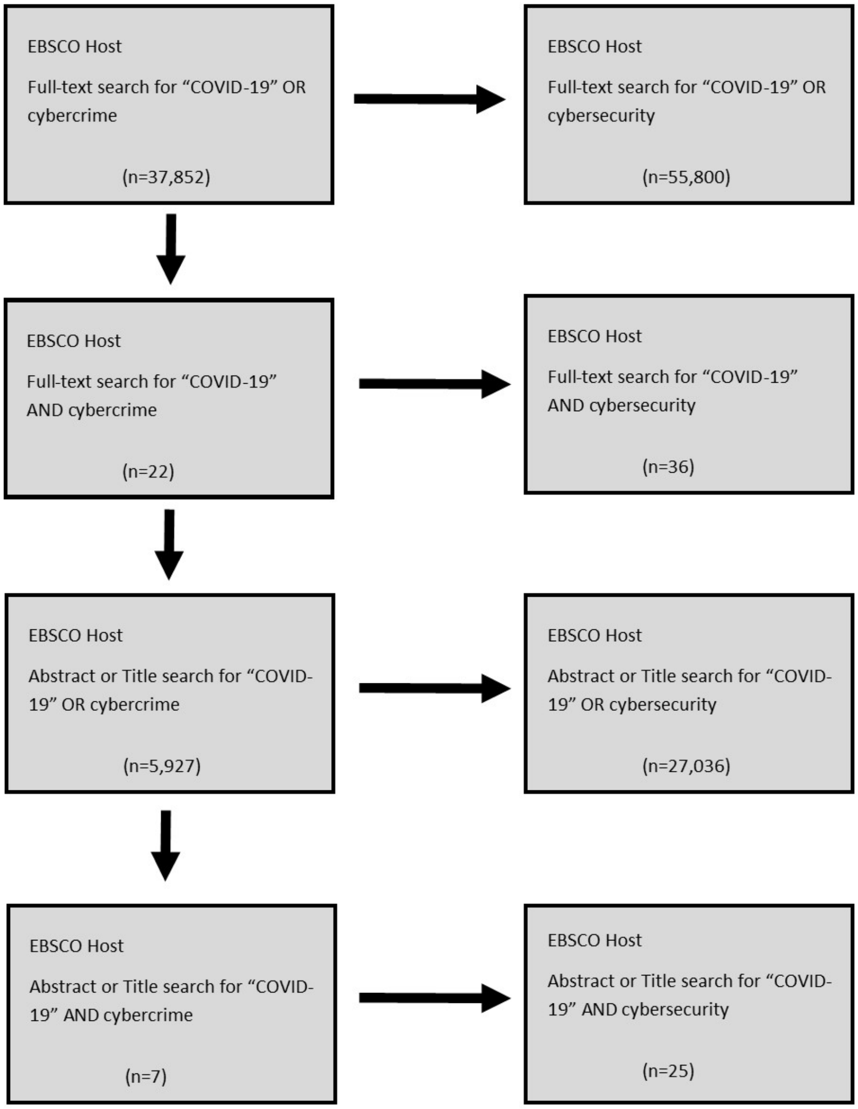
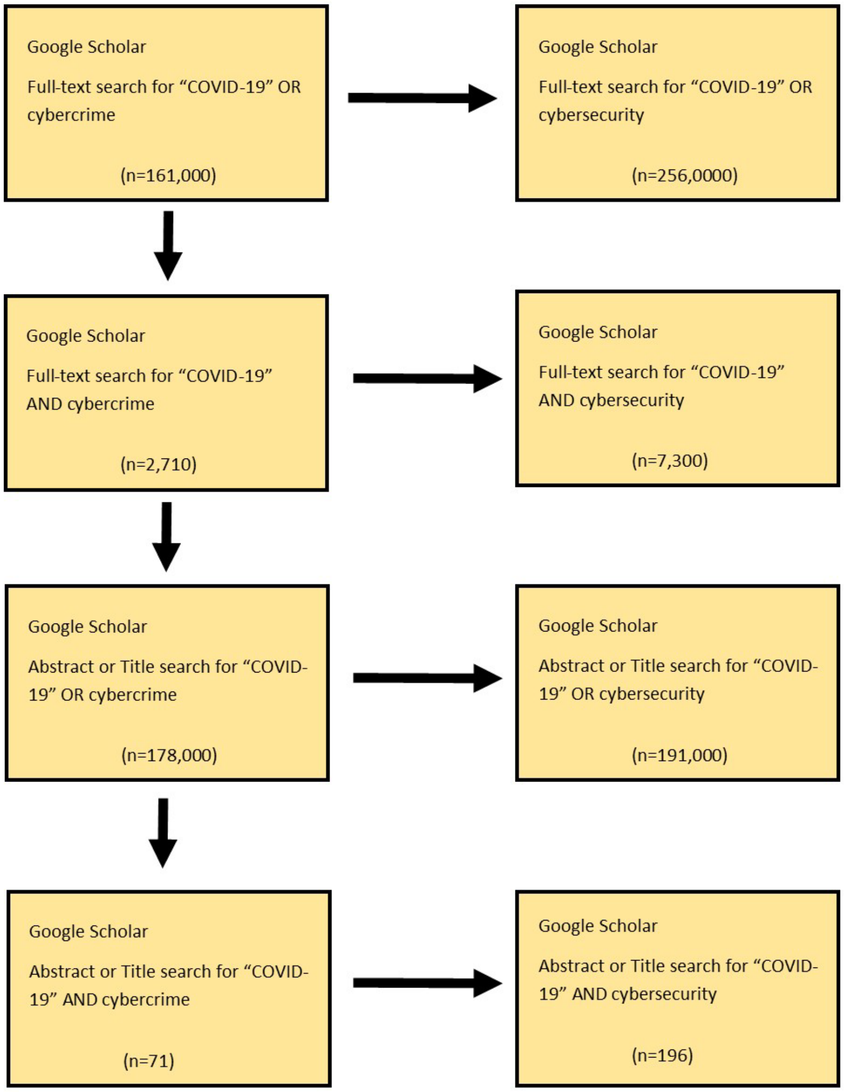

EBSCO Host
Full-text search for "COVID-19" OR cybercrime
(n=37,852)
EBSCO Host
Full-text search for "COVID-19" OR cybersecurity
(n=55,800)
EBSCO Host
Full-text search for "COVID-19" AND cybercrime
(n=22)
EBSCO Host
Full-text search for "COVID-19" AND cybersecurity
(n=36)
EBSCO Host
Abstract or Title search for "COVID-19" OR cybercrime
(n=5,927)
EBSCO Host
Abstract or Title search for "COVID-19" OR cybersecurity
(n=27,036)
EBSCO Host
Abstract or Title search for "COVID-19" AND cybercrime
(n=7)
EBSCO Host
Abstract or Title search for "COVID-19" AND cybersecurity
(n=25)

FIGURE 3
GOOGLE SCHOLAR LITERATURE REVIEW DATA RESULTS AS OF 10/19/2020


Google Scholar
Full-text search for "COVID-19" OR cybercrime
(n=161,000)
Google Scholar
Full-text search for "COVID-19" OR cybersecurity
(n=256,0000)
Google Scholar
Full-text search for "COVID-19" AND cybercrime
(n=2,710)
Google Scholar
Full-text search for "COVID-19" AND cybersecurity
(n=7,300)
Google Scholar
Abstract or Title search for "COVID-19" OR cybercrime
(n=178,000)
Google Scholar
Abstract or Title search for "COVID-19" OR cybersecurity
(n=191,000)
Google Scholar
Abstract or Title search for "COVID-19" AND cybercrime
(n=71)
Google Scholar
Abstract or Title search for "COVID-19" AND cybersecurity
(n=196)

Our content analysis has indicated that during COVID-19, organizations did take preventive measures to help safeguard their information systems as many employees transitioned to remote employment. Some preventive methods that organizations' have employed are as followed: enabled multifactor authentication and using virtual private networks. These preventive measures, unfortunately, highlighted the need for more enhanced preventive methods to combat these cybersecurity attacks. Advanced preventive measures that could assist with combating cybersecurity attacks are organizations will need to transition to new operating models, organizations will need to reset their security systems to ensure there are no outliers, and/or information technology security architectures should be reassessed.

Furthermore, our findings indicate consideration for a public campaign to bring attention to the need for preventive measures in protecting organizations' information technology systems from being exploited by cybercriminals during a worldwide pandemic. Although this paper does not address statistics in how many cases of cybercrimes occurred during COVID-19 as this pandemic is still current, it can be a topic worth exploring in the future.

BACKGROUND ON TECHNOLOGY SOLUTIONS FOR SELF-REPORT DATA COLLECTION

The use of self-report data collection is common in such fields as public health and areas where confidentiality is required to obtain the most honest answers. For example, global public health researchers will often use such methods as Computer-Assisted Self-Interviewing (CASI) or Audio Computer-Assisted Self-Interviewing (ACASI) technology solutions in the course of health-related research projects. Using these tools with a participant population that may not answer honestly and reliably in-person makes them valuable. Participants are generally provided a technology device, such as a tablet or smartphone, and reinforced that the act of the self-report survey will keep the information confidential and private. The use of the audio component in ACASI can be valuable when doing a self-report survey in a country where the participant may not be well versed in the survey language and provide a means for the survey respondent to listen to the sensitive questionnaire in their local language and dialect. This can be valuable, given cybercrime and fraudulent activity can occur transnationally with ease.

One typical method of probing survey participants is via the Face-to-Face (FTF) approach, which is still considered one of the most formidable ways to elicit survey responses. This can be difficult to engage with a population, particularly with those who have committed cybercrimes, and be less willing to face a human. Because of this, the authors are encouraging research using such tools that provide for greater self-report opportunities. The shape and technology methods that involve self-report quantitative surveying can also include many different strategies. Some of these include Computer-Assisted Telephone Interviews (CATI), Interactive Voice Response (IVR), Paper and Pencil(PAP), Video Audio Computer-Assisted Self Interviews (VACASI), and Short Message Service (SMS), to name a few (Mierzwa, et al., 2016).

In performing a cursory search in Google Scholar, using the search terms of “ACASI” AND “Cybercrime” yielded a search finding of eight articles, with no date limit. A similar search was done for “ACASI” AND “Cybersecurity”, which yielded only one article. This has led the authors to wonder if further research and use of these self-report data collection tools could or should be explored in examining why global cybercriminals are entangling themselves more frequently in cybercrime. For example, given the stay-at-home orders providing possibly more idle time, a self-report question could surround whether this was the first time for the offender and if so, how were they introduced to the idea and strategy taken with the cybercriminal activity? Additionally, with regard to less sophisticated breaches, such as with Zoom bombing, understanding the key contributors to why those who perpetrated these attacks did so.

DISCUSSION

Given the lack of research publications found related to doing ACASI survey research with cybercrime focus, concerns are apparent in whether cybercrime actors would be even willing to contribute to a self-report survey on their practices and reasons for initiating efforts during a significant event, such as COVID-19. Another concern revolves around how to recruit participants to engross in answering self-report survey questions to aid researchers. If researchers are successful in recruitment for a self-report survey surrounding cybercrime and COVID-19, a challenge exists in ensuring the participant’s responses and the survey activity will be kept with utmost confidentiality and anonymity. Confidence in the participants will be paramount to ensure they will not be immediately referred to law enforcement. The authors wonder if this is even possible.

In this commentary and prospective report, we have brought attention to the idea of doing further research, using self-report surveying technologies, to help elicit information about the cybercrime perpetrators. Studying the cybercrime actors is essential, but another approach to consider in future research can be to include the victims to better understand their plight with regard to why COVID-19 became an entry point for criminal activity. Using self-report surveying technology with the elderly population, or those who may have been more at-risk with compromised immune systems and experienced a cybercrime, for example.

Additional areas outside of cybercrime could also be approached with innovative self-report surveying technology such as but not limited to include:

1. Population not willing to participate in using COVID-19 contact tracing applications.
2. Groups or individuals who participated in the so-called "COVID-19" parties, where people were exposed to the virus in the attempt to be the first to get the illness.
3. Study the populations that did provide COVID-19 contact tracking information and elicit the extent of truthfulness provided.
4. Better understand why certain populations were less likely to follow pandemic prevention recommendations.

Other possible areas for cybersecurity and cybercrime research to be considered include whether adolescents, with more idle time available, partaken in deviant cyber threat activities due to COVID-19. If adolescents were more involved, were they recruited somehow, and in what manner were they educated in the cybercriminal actions? Integrating the use of novel electronic self-report surveying with the Internet Addiction Diagnostic Questionnaire Test with those that have been identified as cybercriminals could provide valuable knowledge of the psychology of cybercrime. Given the global or transnational nature of cybercrime, an interesting observation was documented in a 2016 study in Bangladesh of 400 undergraduate students; 25.3% were categorized as internet dependent, with 74.8% reporting as depressed (Arefin, et al., 2016). Involving more such surveys with the introduction of cybercriminal activity could aid to better understand why in the case of COVID-19, such an uptick in hacking attempts ensued.

LIMITATIONS

The authors have outlined relevant existing research publications and trade press articles about COVID-19 and including cybercrime and cybersecurity. The COVID-19 pandemic is still ongoing and only in full swing as of March 2020, just over eight months ago. This by default, may be considered too soon to be researching the topic; more time to allow researchers to publish materials about the said topic would work to the benefit of this research. In the literature review, specific keywords were searched, a larger scan, including a greater number of keywords would benefit the resulting findings.

The investigation performed in the scholarly databases were limited to three services. There exist many avenues for a researcher to evaluate available publications, and this research commentary limited its approach but could have expanded greatly.

CONCLUSION

Our rapid literature review has presented that few, if any, articles highlighted the reasons why cybercriminals take advantage of large-scaled "current event" issues, such as the COVID-19 pandemic. Much of the research literature currently available focuses on the presence of cybersecurity incidents, security breaches, privacy concerns, and methods to protect devices and systems from exploitation technically. Putting in place safeguards to prevent a cybercrime or cybersecurity incident is very often recommended as a matter of practice. Consider the National Cybersecurity Awareness Month that takes place in October each year and promoting protection is heavily emphasized. On the flip side, when cybercrimes or cyber incidents do occur, organizations and persons will resort to cleaning up the damage that ensued and as a matter of course, employ strategies to ensure the incident does not reoccur. Although this may seem rudimentary, in this paper we are recommending a "call to action" for cybersecurity, criminal justice and social science researchers to further explore reasons why criminals engage in crime activities when large-scaled events, such as COVID-19. In approaching a greater understanding and knowledge of the causes or impetus for cybercrime activities during COVID-19, new strategies can be developed to deter such criminal activities. Cybercriminals are using artificial intelligence (AI) and machine learning (ML) and all sorts of new technologies to wreak havoc, but in the same light, those charged with protecting and preventing cybercrime can also look to use AI and ML to help prevent criminal behavior, and using innovative self-report data collection can assist with more insights about the offenders.

REFERENCES

Ahmad, T. (2020). Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity. *Digital Learning*, *4.* Retrieved from https://kean.idm.oclc.org/login? url=https://www-proquest-com.kean.idm.oclc.org/docview/2385938465?accountid=11809

Arefin, A., Bashar, K., Asha, M., Bhuiyan, F., Tithi, M., & Haque, M. (2016). Internet Dependency and Its Association with Depression among the Students of North South University of Bangladesh. *EC Psychology and Psychiatry*, *1*(2), 44–48.

Business Wire. (2020). *The Impact of the COVID-19 Pandemic on Cybersecurity; Assessment of challenges posed by the pandemic ranging from spike in cyberattacks to lackluster support for cybersecurity prioritization*. Retrieved September 18, 2020, from http://resolver.ebscohost.com.kean.idm.oclc.org/openurl?sid=EBSCO%3aaph&genre=article&issn=10009140&ISBN=&volume=63&issue=23&date=20200604&spage=26&pages=26-27&title=Beijing+Review&atitle=COVID-19+and+Cybersecurity.&aulast=Ma+Bo&id=DOI%3a&site=ftf-live

Carter, R.A. (2020). Dealing with Data: Cybersecurity in the COVID-19 Era: Devoted to the Production and Sale of Rock and Clay Products. *Rock Products*, *221*(8), 52–57. https://kean.idm.oclc.org/login?url=https://www-proquest-com.kean.idm.oclc.org/docview/2435184601?accountid=11809

CISA-Alert (AA20-099A). (n.d.). *COVID-19 Exploited by Malicious Cyber Actors*. Retrieved April 29, 2020, from https://www.uscert.gov/ncas/alerts/aa20-099a

Deo, P., Raj, G., & Perumal, R. (2020). *How Covid-19 is Dramatically Changing Cybersecurity*. Retrieved September 15, 2020, from https://www.tcs.com/perspectives/articles/how-covid-19-is-dramatically-changing-cybersecurity

Forrester. (2019). *Prevalence of Legacy Tools Paralyze Enterprises' Ability to Innovate*. Forrester Opportunity Snapshot: A Custom Study Commissioned by ScienceLogic.

Gerell, M., Kardell, J., & Kindgren, J. (2020). *Minor COVID-19 association with crime in Sweden, a five week follow up*. Malmo University. Retrieved from https://osf.io/preprints/socarxiv/w7gka/

Greig, J. (2019). Just 12% of Companies have fully Transitioned to Modern IT Tools. *Digital Transformation – TechRepublic*.

Hakak, S., Khan, W.Z., Imran, M., Choo, K.K.R., & Shoaib, M. (2020). Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies. *IEEE Access*, *8*, 124134–124144. https://doi.org/10.1109/access.2020.3006172

INTERPOL. (2020). *Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence*. Global Action on Cybercrime Extended (GLACY+) Joint project of the European Union and the Council of Europe.

Khan, W.Z., Khan, M.K., Muhaya, F., Aalsalem, M.Y., & Chao, H-C. (2015). A comprehensive study of email spam botnet detection. *IEEE Commun. Surveys Tuts*., *17*(4), 2271–2295 (4th Quart).

Mierzwa, S., Souidi, S., & Savel, C. (2016). On Selecting an Appropriate Customizable Electronic Self-Report Survey Research Technology. *Procedia Engineering, Humanitarian Technology: Science, Systems and Global Impact*, pp. 66–71. Massachusetts.

Olstik, J. (2020). *ESG Report Report – The Impact of the Covid-19 Pandemic on Cybersecurity*. A Cooperative Research Project by ESG and ISSA.

Pietrawska, B., Aurand, S.K., & Palmer, W. (2020b). Covid-19 and crime: CAP's perspective on crime and loss in the age of Covid-19: Crime in Los Angeles and Chicago during Covid-19. *CAP Index*, (19), 3.

Stickle, B., & Felson, M. (2020). Crime Rates in a Pandemic: The Largest Criminological Experiment in History. *Am Journal Criminal Justice*, pp. 525–536. https://doi.org/10.1007/s12103-20-09546-0

Whiteney, L. (2020). *CovidLock Ransomware Exploits Coronavirus With Malicious Android App*. Retrieved from https://www.techrepublic.com/article/covidlock-ransomware-exploitscoronavirus-with-malicious-android-app/