UDC 34
DOI: 10.15587/2523-4153.2022.253820

CYBER INSECURITY IN THE WAKE OF COVID-19: A REAPPRAISAL OF IMPACTS AND GLOBAL EXPERIENCE WITHIN THE CONTEXT OF ROUTINE ACTIVITY THEORY

Sogo Angel Olofinbiyi

How to cite:
Olofinbiyi, S. A. (2022). Cyber insecurity in the wake of COVID-19: a reappraisal of impacts and global experience within the context of routine activity theory. ScienceRise: Juridical Science, 1 (19), 37–45. doi: http://doi.org/10.15587/2523-4153.2022.253820

Shortly after the enthronement of COVID-19 on the global continent, cyberspace became a dominant arena for social, economic, religious, educational, recreational and political activities across the world. This paper draws insights from the existing literature to illustrate how COVID-19 has provided situational opportunities for cyber criminals to strike and exploit people of their valuable resources through creating fraudulent websites as well as spreading of malware and ransomware to vulnerable users. To this end, routine activity theory becomes very dominant and crucial in understanding the underlying basis for the increased cybercrimes that currently characterize the cyber space. The study demonstrates that the twin phenomenon of coronavirus and cyber insecurity has not only instilled fears into the hearts of cyber users but has also negatively impacted the global economy in various ways that cannot be quantified by any study. Since all measures put in place to contain the threats of the horrible virus, have, hitherto, remained counterproductive, the paper recommends essential cyber hygiene practices (such as, antivirus protection, malware and phishing awareness, weak spots identification, intelligent techniques, risk management approach, zero trust design, home network security and general cybersecurity awareness) as a coping strategy to salvage both the public health and security sectors from the twin occurrence of the Covid-19 pandemic and cyber insecurity, which has respectively inflicted and claimed millions of lives, and jeopardized significant portions of the global economy. Providing a continued cyber-safe remote-working environment for employees will be of ultimate measure

Keywords: *COVID-19, cyber attacker, cybercriminal, cyber insecurity, cyberspace, impacts and global experience, routine activity theory (RAT)*

1. Introduction

Cyber insecurity entails an unauthorized invasion of cyber privacy, trespassing, thefts, as well as denial of services attacks and malfunction, caused by any human factor in any system that is dependent on the internet using computer devices; and such trespassing may include hacking into a nation's or an individual's critical infrastructure [1]. Despite different measures, being put in place by various multinational organizations, targeted at ensuring that there is maximum security against cyber intruders, various cyber criminals still sneak in to inflict insecurity threats. Cyber insecurity has been in our life for centuries, but its trends began to escalate with the emergence of the Covid-19 pandemic. Cyber insecurity can actually be traced back to 1870 "when a male teenager was first hired as a switchboard operator and was able to disconnect and redirect calls using the line for personal usage". The advent of the computer age brought about the traditional hacker, who was first thought of as a harmless user with a curiosity about how computer can be manipulated to commit crime [2]. Over the years, hacking has taken on a grossly different dimension to criminality and is solely functional to the activity of cyber criminals. The existence of cyber insecurity has always presented itself with malware infections, Phishing, identity theft, zoom bombing, password sniffing, computer hacking, and web site damages [3]. This is a phenomenon that has staged the global sphere with more intense rigours into the wake of the coronavirus pandemic.

The paper contends that the best explanations for the underway global upsurge in cyber insecurity can adequately be enunciated by situational opportunity theories of crime; while the protective tide gauge to mitigate and counteract the waves of the rising tide in cyber insecurity, experienced during the nefarious reign of COVID-19, will always remain a function of continued cyber-safe remote-working environment. Crime commission is a function of opportunities, which depends on a twin factor of time and space. Opportunities to commit crime rely on everyday movements of activity and shift vastly by hour of the day, day of the week and month of the year, reflecting possible opportunities to carry it out. In these situations of opportunity shifts, offenders and their targets also shift according to their activities, such as trips to offices, schools, social/recreational settings. For instance, pickpockets consider the presence of crowds at the City Centre to operate and burglars target suburbs in the afternoon, during which inhabitants are at their places of work, religious Centres or institutions of learning. Given the above explanation as well positioned by Felson and Clarke [4], routine activity theory seems helpful in understanding the underlying factors for the unabated increase in the incidence of cybercrimes, considering the reality that the wake of COVID-19 has provided situational opportunities for the crime to trend. Not until this time, several research findings, media reports and international organizations have presented adequate information on the rapid spread of the ailment and the number of lives claimed and infected, as well as casualties, caused across the globe. However, the current study draws insights from the existing literature to illustrate how the pandemic has provided opportunity for cyber criminals to emerge and take control of the cyber space, traumatizing and harassing every global user of the internet facilities. Delving critically into the routine activity's construct, the explanations for exponential growth of cyber insecurity amid the coronavirus pandemic were offered.

The aim of the research was to illustrate how COVID-19 has provided situational opportunities for cyber criminals to strike and exploit the global citizens of their valuable resources, using routine activity as a theoretical construct to explain and interpret the underlying factors for the phenomenon.

2. Materials and Methods

Against the apparent gap in literature, the study engaged in desk research, analyzing data, obtained from media reports, journal articles, as well as conclusions, issued on cyber insecurity amid the COVID-19 pandemic by The World Health Organization, Interpol, South African Banks Risk Information Centre (SABRIC), International Telecommunications Union [ITU], The South African Institute of International Affairs, and academic institutions; and thus, setting for itself the goal of appraising the global experience on the exponential rise in cyber insecurity in the wake of the COVID-19 pandemic.

Through a systematic review of the empirical literature, using a meta-analytical methodological approach, the paper adopts the situational opportunities theory of crime, embedded within the context of routine activity construct to provide explanations for the key factors that engender the exponential increase in the incidence of cybercrimes amid the coronavirus pandemic across the global spectrum. Following a systematic review of the foregoing media reports, as well as other relevant empirical resources in the extant literature, the findings of the study were discussed within a criminological framework in relation to previous research inquiries.

3. Result

3. 1. Theoretical Reflections on the COVID-19 Pandemic

Routine Activity Theory (RAT) takes a central stage in the fields of criminology and sociology and it was originally developed by Lawrence Cohen and Marcus Felson, in 1979. The routine activity paradigm has its origin in the explanation of predatory crimes. The central idea of this theory is that for such crimes to occur in human society, there must be a confluence of three minimal variables in time and space: a likely offender, a suitable target, and the absence of a capable guardian against crime [4, 5]. The paradigm's central focus is on "likely offender", which more or less, influences the possibility of the other two variables. As well exemplified and expatiated upon in this study, the guardian may not necessarily be a police officer or security guard, rather it could be anybody, whose presence, expertise, training, or proximity would deter cybercrime from being committed against vulnerable targets. Thus, amid the outbreak of coronavirus, a cyber expert, an IT expert, or anybody, specialized in cyber security and internet fraud analysis or co-workers in related fields, would simply tend to serve as our guardian against falling prey to the malicious cybercriminals, particularly during this dark era of COVID-19 global disruptions.

Despite that guardianship is often spontaneous and unpremeditated, it is worthwhile to know, that it has a powerful impact against crime in every situation of human existence. On the contrary, in a situation when guardians are absent, a target is chiefly subject to the risk of criminal attack (Fig. 1).

Further explanation on the routine activity approach contends that the target is often preferred over the victim, who might absolutely be absent from the scene of the crime. For instance, the owner of a sum of money in a bank account is normally away when an internet scammer hacks into the account and takes the money away. In this regard, the money is the target and the owner is the victim. Nevertheless, it is the absence of the owner and other guardians (such as Card Verification Value (CVV Number), bank account number, ATM pin code,) that makes the scam easier. On the other hand, targets of crime could also be a person or an object, whose position in space or time puts it at more or less risk of criminal attack [6]. From another point of view, a target's risk of criminal attack is influenced by four main elements, summed up by Felson and Clarke (using the acronym VIVA: *Value, Inertia. Visibility and Access*

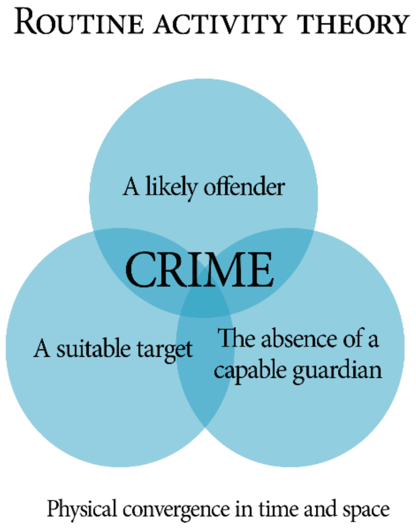
Routine activity theory
A likely offender
CRIME
A suitable target
The absence of a capable guardian
Physical convergence in time and space

Fig. 1. Adapted originally from the work of (Cohen & Felson, 1979)

The dissimilarity here is that all four of these parameters are considered from an offender's viewpoint. Criminals will only find interest in targets they *value*, for whatsoever reason (i.e. a criminal will always value a more precious material that may earn him/her a worthier benefit, specifically an object of monetary value, than the one with a lesser value). *Inertia* simply connotes the weight of the item (i.e a small electronic goods may be more prone to theft than a weighty item, unless the latter is wheeled to subdue their weight). By *visibility* we mean an exposure of theft targets to offenders. By this theorization, all global citizens that use the cyber space are theft targets to possible cyber criminals, as many are now exposed to online services in order to avoid being infected by the coronavirus. People's inevitable daily exposure to online activities as a means of ensuring continuation with their normal enterprises has predisposed the world population to a lot of malicious online websites, created by internet fraudsters to scam people of their resources. *Access* refers to the patterns and features of everyday life that make things easy for offenders to get access to suitable targets. With coronavirus moving across the world, patterns and modes of life are being subject to spontaneous changes, such that cause all activities to be cleaved to online adventures with no guarantee of capable guardian to protect targets from internet invaders who might have, by one means or the others, endeavoured to gain access to our private lives. Using this theoretical approach and a myriad of data reports, the COVID-19 pandemic laid the foundation for the escalation of the continuing predatory cybercrimes in the world. By the "rule of thumb", for predatory crime to occur, it is established, that a likely offender must find a suitable target in the absence of a capable guardian.

Another crucial dimension to this context is that many more organizations at this period have been left unguarded owing to COVID-19's worldwide lockdown, with many security/cyber experts (not excluding the law enforcement agents, high-profile government officials, law makers, judiciaries and executives) in disarray to perform their national obligations. In effect, the most conclusive explanation of cyber insecurity in the world today is a signal of the dispersion of activities away from in-office to online modification. As people spend most of their time on the internet, their risk of personal and property victimization rises with an exponential increase in COVID-19 progression.

3. 2. Covid-19 Trajectory: A Synopsis

Despite the global inoculation against the intractable virus, Covid-19 continues to spread around the world, with more than 230 million confirmed cases and over 4.7 million deaths across almost 200 countries of the world [7]. Neither the rich nor the poor have been spared since the advent of this trend. The death toll and the number of people being tested positive for the virus are rising on daily basis [8, 9]. In support of the WHO's report, as of September 27, 2021, there had been more than 232,265,106 confirmed cases of COVID-19 around the world and about 4,755,276 deaths, according to Johns Hopkins data at the time of this writing [10]. In retrospect, the U.S had its hardest and saddest time in history as the nation was ranked first as having the most reported confirmed cases, with more than 337,000 cases, followed by Spain (more than 131,000), Italy (more than 128,000), Germany (more than 100,000) and France (more than 93,000). According to the available data, more than 264,000 people had recovered from the virus [11].

In Africa, the numbers of those who are being tested positive are rising every day with over 7,075,119 confirmed cases of the virus and more than 177815 deaths at the moment of this writing. In 2020, according to the available data, the ailment was declared as a national disaster in countries like South Africa and Zimbabwe no sooner it became obvious that it would have devastating consequences for the poor and marginalized people, especially in high-density areas with insufficient water, sanitation and health care infrastructure [12].

As the COVID-19 pandemic roars across the global continent, we are all threatened and worried about the effects of this catastrophe on sustainable development. Reports show that in countries that the virus has already hit, a significant number of people, including innocent children, have lost loved ones. Even for those who have not yet been directly affected, COVID-19 is said to have been disrupting their lives in unimaginable ways [13]. The rate, at which the ailment is spreading, has not only engendered cyber insecurity outbreak, but also created great fears in the hearts of the world's populace – such that people now withdraw into their shelters like a snail in prolonged states of dormancy, awaiting the return of favourable conditions [14].

4. Discussion

4. 1. The Social Ills of COVID-19 on Cyberspace

Recently conducted studies have shown that the cyberspace has constantly been under threats since the emergence of the novel virus, as various kinds of cyber spies, thieves, saboteurs, and thrill seekers have found their ways into individual computer systems, thieving personal data and trade secrets, breaking off Web sites, disrupting organizational services, sabotaging data and systems, launching computer viruses and worms, infusing malwares and trojans into the computer devices, conducting fraudulent transactions, as well as scamming individuals and companies [15–17]. It was equally observed in the works Abukari, and Bankas [18], that these attacks were aided with exponentially powerful and easy-to-use software tools, which are freely available from millions of Web sites on the Internet.

In less than a couple of years of COVID-19's reign on the global continent, cybercrime has infiltrated a diverse range of global societies. As a corollary, financial information as well as other personal information, which have been held confidential for decades on the internet space, has been uncovered and divulged to cyber criminals. More importantly, Children of nowadays are not exempted from these social ills, therefore, they need constant supervision on the internet, because these criminals seek to hunt and abuse innocent children by distracting their e-learnings with pornographies.

4. 2. Malware and Domain Formation on Cyberspace

As the coronavirus pandemic becomes ubiquitous, it turned out to be the most searched word on the internet. This is evident upon everyone's desperation to know about the number of coronavirus positive cases and death tolls. In the same vein, an appreciable number of people and organizations are keen on devising the precautionary measures to be taken to prevent the social ills of coronavirus pandemic. There are a lot of coronavirus named domains on the internet today. A study, conducted by Sue Poremba [19], unfolds that the coronavirus pandemic has been negatively impacting the world for at least 5 to 6 months, and the malicious users, commonly referred to as 'cybercriminals', have not abandoned their bid to manipulate the pandemic for their own benefits. This is evident in the Google's report that, 18 million malware and phishing scams, related to Covid-19, were recorded every single day. Going by the conceptual clarification of routine activity theory, coronavirus has provided opportunity for cybercriminals to engage in creating identity domains in the name of coronavirus and injecting malware and harmful viruses into the website. As soon as the device is affected by this malware, all the user's credentials will fall into the hands of cybercriminals (ibid). The World Health Organization has observed suspicious emails, messaging attempts, made by cyber scammers who are taking advantage of COVID-19 [20], to access their device and data. According to WHO, the malicious code provides an intrusive software, including viruses, trojans, worms, backdoor, rootkit, botnets and spyware, which enable the cyber attackers to steal the data from their device and possibly take a control of the entire device [21]. The authors state further, giving the following example: "it once happened that attackers sent a blackmail to a victim and claimed to access the victim's information as well as his/her location via the internet, and threatened to infect the target and his/her family with Covid-19 unless a ransom was paid".

This is a common attack that the world's security experts have encountered 1008 times over a duration of two days, since the emergence of this ailment.

Given the modus operandi of cyber attackers as illustrated in literature, this paper identified social engineering (which is about manipulating the users and tricking them) as the most common tool of cybercriminals amid the COVID-19 pandemic. In the word of Engebretson, social engineering becomes one of the simplest techniques to worm out information from the target user through the process of exploiting human weakness [22]. On this note, Cybercriminals are devising their means to hack into the user's systems. Based on the conceptual analysis of routine activity theory, as lives have become more confined to online activities; and all employees are made to work on their systems rather than offices, cybercriminals gain absolute assessment of their suitable targets through constant online routine of the internet users; and break the cybersecurity of the users. Figuratively, the study adds that the more people spend more time online, the better the attackers assess their information and the more they are exposed to malware and attacks set up by the invaders. Hence, the Union Ministry of Home Affairs has warned about the cybercriminals who are spreading malware links about the coronavirus app, such as (Spymax, Coronalive 1.1). In support of this social reality, the **Check Point's Global Threat Index shows that cybercriminals are exploiting interest in the global epidemic to spread malicious activity through several spam campaigns, relating to the outbreak of the virus.** It was revealed, that if these apps were downloaded, cybercriminals would have access to steal all your data [23, 24]. The diagram, showing malicious domains creation (Fig. 2).

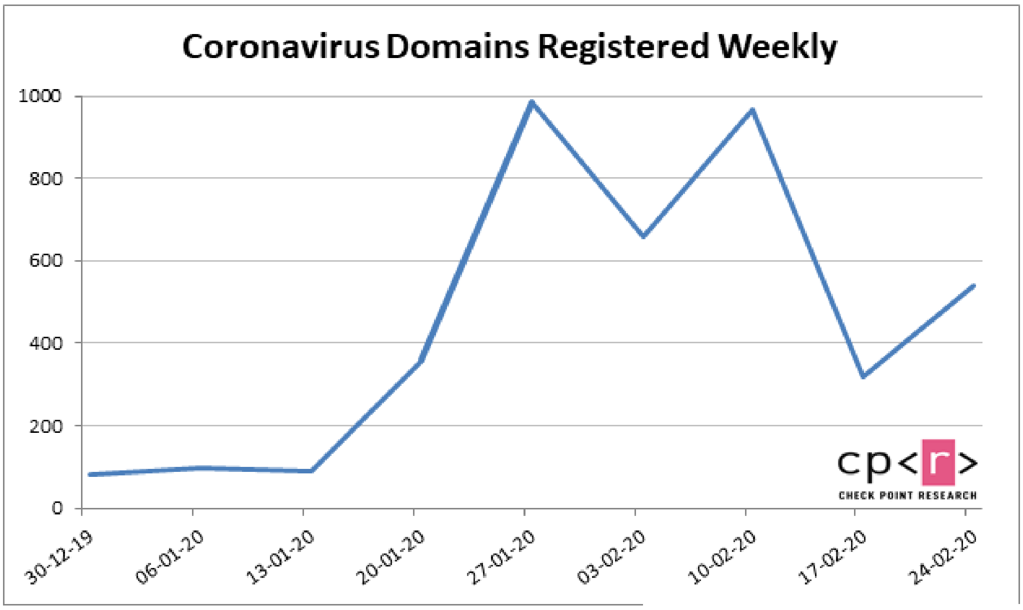

Fig. 2. Coronavirus Malicious Domains Formation. Source: **CheckPoint's GlobalThreatIndex**

4. 3. COVID-19 Social Ills and Global Experience

The incessant trend in COVID-19 upsurge has called for an increase in remote working across the world. Consequently, the devasting effects have been felt across various sectors of the global economy in the following significant ways.

Financial Sector

The spread of COVID-19 has sent a shockwave through the financial sectors of the world and poses substantial cyber risks to strategic sectors of the economy. The discontinuity of work and lockdowns in several countries has led to increased online activity as many people have had to resort to working from home [25]. Consequently, the financial sector of most global organizations has felt a huge blow since the virus has staged the global sphere. There has been evidence in the extant literature that the global systems have recurrently been attacked and millions of United States dollars have gone down the drain through persistent attacks by cybercriminals [26]. It was also established, that stock markets around the world and every segment of the global economy have been severely affected, while phishing, malware and ransomware (which are the techniques of social engineering, adopted by cybercriminals) have dealt a great blow to financial service industries across the world [27]. Given the various incidents of cyberattacks and threats around the world, the South African banks have taken pre-emptive measures to embark on a frequent drive to educate their clientele concerning fake emails and phishing [28]. As Chigada and Madzinga expressed further, "a wide range of phishing scams (i.e. bogus communications that purport to be from a well-known and trusted source, which request confidential information [typically login/password details or banking information]) are circulated by hackers on daily basis".

In a study, conducted by the Price Waterhouse Coopers, South Africa (PWC), cyberattacks and threats on financial institutions between February and April, 2020 were seen to increase by more than 238 % globally, at a time when the global economy was working tirelessly to fight the COVID-19 infections [29]. It was suggested, that the COVID-19 insurgency pioneered a perfect climate for cybercriminals to exploit their targets. Congruently, ransomware attacks experienced a nine-fold upsurge during the period, with phishing emails as the primary source of attacks, launched on the suitable target. From this standpoint, Chigada and Madzinga contend that cyberattacks and threats are remarkably growing, because cybercriminals are intelligent individuals who have gained better knowledge of the policies and procedures of financial institutions.

In support of Chigada's and Madzinga's viewpoints, Crisanto and Prenio submitted that cybercriminals will continue to exploit the weaknesses and vulnerabilities, opened up by the COVID-19 pandemic, thus increasing the incidence of cyber risks, money laundering and terrorist financing across the world [30]. The foregoing scholars unfold that, there was an upsurge in money laundering and terrorist financing, orchestrated through increased misuse of online financial services as well as virtual assets, harnessed to move and conceal illicit funds; and this perhaps shows some level of corruption, affiliated with government stimulus funds (e.g. the R500 billion COVID-19 stimulus package). Furthermore, there have been incidents of more than 1500 high-risk domains, containing both COVID-19 and financial themes, created by threat actors with the goal of stealing from the incautious public or firms.

Healthcare Sector

Research has shown that most healthcare organizations around the world depend on ICT applications, which offer patients and healthcare personnel e-healthcare services [31]. The advent of coronavirus has done nothing but exposure of e-healthcare services, soaring the war, currently being faced by healthcare institutions; and thereby resorting to overstretched resources and personnel that are responding to the novel coronavirus [32]. In the United States, the Centres for Disease Control and Prevention (CDCP) and other healthcare facilities have experienced attackers by Distributed Denial of Service (DDoS) through millions of connection requests. In the same vein, the World Health Organization (WHO) was also exposed to malicious attacks, launched at a critical time in the COVID-19 history, because of its resilient response to the collective safety and health needs of the global society [33, 34]. The authors stressed further that the attacks on WHO took some semblance of critical services, where the criminals had launched spear-phishing attacks, posting as the WHO and CDC. Besides fake news and spread of disinformation, which are regarded as the major threat contributors that characterized the COVID-19 era, the WHO added that more than 450 email addresses and passwords were leaked by hackers who accessed the WHO's server [35]. It was reported, that healthcare organizations that are at the forefront of dealing with the COVID-19 pandemic (chiefly hospitals, research organizations, laboratories and pharmaceutical companies) have been prime targets of cybercriminals [36]. In addition, there has also been an increased misinformation about COVID-19 via different platforms, creating panic and uncertainty for global citizens.

Cyberattacks on Video Conferencing Services

In the wake of COVID-19, the world's cyber security systems have been violated by habitual cyber invaders who leverage on remote working as an opportunity to disrupt video conferencing services. Drawing on insights from the exiting literature, it is established, that video conferencing has been the most acknowledged platform where people, governments, organizations and institutions meet to discuss issues that concern human and economic developments. Given the weaknesses, associated with the remote working system, there have been series of cyberattacks that were reported to have followed the adoption of video conferencing services as a means to continue with human struggle for survival and to reduce the spread of the killer disease among the global populace. Evidence in support of this assertion is captured in the narrative below: "Between February 2020 and May 2020 more than half a million people were affected by breaches, in which the personal data of video conferencing services users (e.g., name, passwords, email addresses) were stolen and sold on the dark web". To execute this attack, some hackers used a tool called 'Open Bullet' [37]

Furthermore, media reports unveiled that hackers also employ the use of 'credential stuffing techniques' to gain access to employees' credentials and steal their bio data, which are, in turn, sold to other cybersecurity syndicates. One of the aftermaths is a grave disruption to businesses and organizations that rely heavily on video conferencing platforms [38]. Credential stuffing is a form of cyberattack whereby hackers use previously-stolen combinations of username and password to gain access to other accounts [39]. This is virtually feasible, because it is always a common practice for people to use the same username/password combination across multiple accounts.

Moreover, there have been reported cases of hackers, disrupting South Africa's Parliament meeting by sharing obscene materials using the Zoom platform during the virtual held meeting [40]. Emphasizing on the increased threat of cyber insecurity around the world, the Interpol [41] reported that "cybercriminals are focusing their attention on government agencies and large firms to cause irreparable damage to information systems and their infrastructures". Subsequently, the exponential growth of cyberthreats and attacks has heightened the strain on law enforcement agencies around the world.

The Exponential Growth in Cyberinsecurity

The changing nature of cyberattacks and the increase in remote working call for a greater focus on cybersecurity, because of the global citizens' greater exposure to cyber risk. This is evident, for instance, from the fact that 47 % of individuals fall for a phishing scam while working at home [42]. Another crucial perspective to this debate is that, the average cost of a data breach, emanating from remote working, could be as much as $137,000. In furtherance of this submission, the City of London Police reported on

8th July, 2020, that since January 2020, the United Kingdom had lost more than GBP 11 million to COVID-19 scams. In a study, conducted in Switzerland, one in seven respondents to a survey had experienced a cyberattack during the pandemic period [43]. From the standpoint of routine activity theory (RAT) as first espoused by Cohen and Felson [44], the cyber attackers see the pandemic as an opportunity to step up their criminal activities by exploiting the vulnerability of employees, working from home, and capitalizing on people's strong interest in coronavirus-related news (e.g. malicious fake coronavirus related websites). From all indications, the upsurge in sophisticated cyberattacks calls for new 'cutting-edge detection mechanisms' (such as 'user and entity behavior analysis' or UEBA) to contain the threat [12]. This approach will help analyze the normal conduct of cyber users, and the knowledge obtained will also help detect instances where anomalous deviations from normal patterns occur during the course of using the cyberspace.

5. Conclusion

The continued cyber insecurity, which seems to have characterized the present-day cyberspace, was catalyzed by the unprecedented reign of coronavirus infection. The presence of coronavirus has not only instilled fears into the hearts of cyber users but has also negatively impacted the global economy in various ways that cannot be quantified by any study. The study presents the worst-hit of the Covid-19 pandemic on cyberspace, unfolding how criminals have taken undue advantage of the pandemic to step up their criminal ventures, through spreading malware and ransomware to vulnerable users, as well as launching of fraudulent websites for internet users and most renowned organizations and financial firms across the world. So far, so good, whether you are working from home, out of work, self-isolating or caring for others, it has become a known maxim, that these are lonely and dark times for all. With COVID-19 in vogue and cyberlives disrupted, the fight for global health security, economic buoyancy and emancipation from all shackles of oppression, inflicted on the world by COVID-19, should not cease until the world is recovered from this intractable pestilence.

Given the magnitude of daily challenges, presented by the pandemic, it should become imperative for the law enforcement agencies to become more proactive in terms of implementing and enforcing more preventive measures, policies and programmes that will gear towards public enlightenment on the social ills of the pandemic, as well as their protection against any attendant incidents of cyberattacks. By the same token, it is believed such programs will not only produce intelligent individuals with highly-inclined technological skills to restrict cyberattacks, but also, it will provide the law enforcement with skills, needed to act against any impending cybercrime when the need arises.

Against this backdrop, organizations and financial institutions around the world must pay more attention to adequately identifying and managing cyber risks that could negatively affect their functions, owing to the fact that cybercriminals thrive on organizations, which fail to implement effective cyber controls. For African countries with poor or limited cyber risk controls, cyber strategies and frameworks to intensively map and actively manage their IT system and infrastructure are crucial to mitigating the scourge.

Above all, this study adds that many organizations still do not provide a 'cyber-safe remote-working' environment for their staff, where business meetings will traditionally be held without being hijacked or disrupted by cyberattacks. To this end, employees, working from home, whether using their personal computer or a corporate-owned electronic device, should implement essential cyber hygiene practices, including but are not limited to antivirus protection, malware and phishing awareness, weak spots identification, intelligent techniques, risk management approach, zero trust design, home network security and general cybersecurity awareness [45].

References

1. Barau, A. S. (2016). Cyber insecurity as a manifestation of new form of global urban vulnerability. Imam Journal of Applied Sciences, 1 (1), 27–32.
2. Holt, T. J.; Huebner, B. M., Bynum, T. S. (2016). Cybercrime. The Handbook of Measurement Issues in Criminology and Criminal Justice. Wiley, 29–48. doi: http://doi.org/10.1002/9781118868799.ch2
3. Rossi, F. D., Hohemberger, R., Konzen, M. P., Temp, D. C. (2020). E-Banking Security: Threats, Challenges, Solutions, and Trends. Encyclopedia of Criminal Activities and the Deep Web. IGI Global, 893–904. doi: http://doi.org/10.4018/978-1-5225-9715-5.ch060
4. Felson, M., Clarke, R.V. (1998). Opportunity Makes the Thief: Practical theory for crime prevention. London, 44.
5. Boivin, R., de Melo, S. N. (2019). The Concentration of Crime at Place in Montreal and Toronto. Canadian Journal of Criminology and Criminal Justice, 61 (2), 46–65. doi: http://doi.org/10.3138/cjccj.2018-0007
6. Ten Boom, A., Pemberton, A., Groenhuijsen, M. S. (2019). The need for protection and punishment in victims of violent and nonviolent crime in the Netherlands: The effect of relational distance. Victims & Offenders, 14 (2), 222–238. doi: http://doi.org/10.1080/15564886.2019.1575300
7. WHO-Convened Global Study of Origins of SARS-CoV-2 (2021). China Part. Geneva: World Health Organization. Available at: https://www.who.int/publications/i/item/who-convened-global-study-of-origins-of-sars-cov-2-china-part

8. Hallal, P. C., Victora, C. G. (2021). Overcoming Brazil's monumental COVID-19 failure: an urgent call to action. Nature Medicine, 27 (6), 933–933. doi: http://doi.org/10.1038/s41591-021-01353-2
9. Introduction to COVID-19: methods for detection, prevention, response and control (2020). WHO. Available at: https://openwho.org/courses/introduction-to-ncov
10. Covid-19 data in motion (2021). Johns Hopkins University and Medicine. Available at: https://coronavirus.jhu.edu/
11. Salyer, K. (2020). COVID-19: What to know about the coronavirus pandemic. World Economy Forum. Available at: https://www.weforum.org/agenda/2020/04/covid-19-what-to-know-about-the-coronavirus-pandemic-on-6-april/
12. Coronavirus in Africa Tracker: How many covid-19 cases & where (2020). African Argument. Available at: https://africanarguments.org/2020/04/07/coronavirus-in-africa-tracker-how-many-cases-and-where-latest/
13. Modes of transmission of virus causing COVID-19: Implications for IPC precaution recommendations (2020). World Health Organization. Available at: https://www.who.int/news-room/commentaries/detail/modes-of-transmission-of-virus-causing-covid-19-implications-for-ipc-precaution-recommendations
14. Olofinbiyi, S. A., Singh, S. B. (2020). The role and place of COVID-19: An opportunistic avenue for exponential world's upsurge in cybercrime. International Journal of Criminology & Sociology, 9 (11), 221–230.
15. Muttoo, S. K., Badhani, S. (2021). An Analysis of Malware Detection and Control through Covid-19 Pandemic. 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom). IEEE, 637–641
16. Singh, S, Medatwal, C. A. (2021). Study on impact of Covid-19 Pandemic on cyberspace. International Journal of Management, 12 (3).
17. Gundur, R. V., Levi, M., Topalli, V., Ouellet, M., Stolyarova, M., Chang, L. Y.-C., Mejía, D. D. (2021). Evaluating Criminal Transactional Methods in Cyberspace as Understood in an International Context. CrimRxiv. doi: http://doi.org/10.21428/cb6ab371.5f335e6f
18. Abukari, A. M, Bankas, E. K. (2020). Some cyber security hygienic protocols for teleworkers in COVID-19 pandemic period and beyond. International Journal of Scientific & Engineering Research, 11 (4), 1401–1407.
19. Poremba, S. (2020). Businesses Underestimate COVID-19 Cybersecurity Risks. Available at: https://securityboulevard.com/2020/05/businesses-underestimate-covid-19-cybersecurity-risks/
20. Banerjee, D. (2020). How COVID-19 is overwhelming our mental health. Nature India. Available at: https://www.natureasia.com/en/nindia/article/10.1038/nindia.2020.46
21. Zhang, B. Y., Yan, X. A., Tang, D. Q. (2018). Survey on Malicious Code Intelligent Detection Techniques. Journal of Physics: Conference Series, 1087, 062026. doi: http://doi.org/10.1088/1742-6596/1087/6/062026
22. Breda, F., Barbosa, H., Morais, T. (2017). Social engineering and cyber security. Inem Conference: International Technology, Education and Development Conference. doi: http://doi.org/10.21125/inted.2017.1008
23. Pinto, D. (2020). Cyber criminals use coronavirus to loot gullible citizens. Available at: https://www.newindianexpress.com/cities/hyderabad/2020/mar/30/cybercriminals-use-coronavirus-to-loot-gullible-citizens-2123302.html
24. Update: Coronavirus-themed domains 50 % more likely to be malicious than other domains (2020). Check Point's Global Threat Index. Available at: https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/
25. Cybercrime and COVID-19: A concern for financial stability during the pandemic (2020). The South African Institute of International Affairs (SAIIA). Available at: https://saiia.org.za/research/cybercrime-and-covid-19-a-concern-for-financial-stability-during-the-pandemic/
26. Chigada, J., Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. SA Journal of Information Management, 23 (1). doi: http://doi.org/10.4102/sajim.v23i1.1277
27. Khan, N. A., Brohi, S. N, Zaman, N. (2020). Ten deadly cybersecurity threats amid COVID-19 pandemic. IEEE. Berlin. doi: http://doi.org/10.36227/techrxiv.12278792.v1
28. Identity theft, viewed (2020). South African Banks Risk Information Centre.
29. Impact of COVID-19: The World has changed and so have we (2020). Price Waterhouse Coopers. Available at: https://www.pwc.co.za/en/about-us/integrated-report-2020/impact-of-covid-19.html
30. Crisanto, J. C., Prenio, J. (2020). Financial crime in times of COVID-19 – AML and cyber resilience measures, bank for international settlements. Available at: https://www.bis.org/fsi/fsibriefs7.htm
31. Paek, H.-J., Hove, T. (2021). Information Communication Technologies (ICTs), Crisis Communication Principles and the COVID-19 Response in South Korea. Journal of Creative Communications, 16 (2), 213–221. doi: http://doi.org/10.1177/0973258620981170
32. Samsad, J., Forkan, A. (2021). Advancing Health Information System with System Thinking: Learning Challenges of E-Health in Bangladesh During COVID-19. International Conference on Health Information Science. Cham: Springer, 15–23. doi: https://doi.org/10.1007/978-3-030-90885-0_2
33. Balsom, W., Dixon, D. (2020). 'How COVID-19 shows the urgent need to address the cyber poverty gap'. World Economic Forum-Cybersecurity. Available at: https://www.weforum.org/agenda/2020/03/covid-19-pandemic-shows-the-urgency-for-addressing-the-cyber-poverty-gap/
34. Laskar, P., Yallapu, M. M., Chauhan, S. C. (2020). "Tomorrow Never Dies": Recent Advances in Diagnosis, Treatment, and Prevention Modalities against Coronavirus (COVID-19) amid Controversies. Diseases, 8 (3), 30. doi: http://doi.org/10.3390/diseases8030030
35. Beware of criminals pretending to be WHO (2020). World Health Organization. Available at: https://www.who.int/about/cyber-security
36. Chigada, J. M. (2020). A qualitative analysis of the feasibility of deploying biometric authentication systems to augment security protocols of bank card transactions. SA Journal of Information Management, 22 (1). doi: http://doi.org/10.4102/sajim.v22i1.1194
37. Regional cybersecurity forum for Europe and CIS (2020). International Telecommunications Union. Sofia Bulgaria. Available at: https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2020/CSF/SofiaBG.aspx
38. Impact of COVID-19 on Cybersecurity (2020). Deloitte. Available at: https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html
39. Nathan, M. (2020). Credential stuffing: new tools and stolen data drive continued attacks. Computer Fraud & Security, 2020 (12), 18–19. doi: http://doi.org/10.1016/s1361-3723(20)30130-5
40. Magome, M. (2020). South Africa sees sharp rise in virus, part of African wave. Associated Press. Available at: https://www.usnews.com/news/world/articles/2020-12-10/south-africa-sees-sharp-rise-in-virus-part-of-african-wave
41. COVID-19 cyberthreats, viewed (2020). Interpol. Available at: https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats

42. Why We Click: The Psychology Behind Phishing Scams and How to Avoid Being Hacked (2020). Tessian. Available at: https://www.tessian.com/blog/why-we-click-on-phishing-scams/
43. COVID-19 related scams – news and resources (2020). Action Fraud. Available at: https://www.actionfraud.police.uk/covid19
44. Cohen, L. E., Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. American Sociological Review, 44 (4), 588–608. doi: http://doi.org/10.2307/2094589
45. Aldawood, H., Geoff, S. (2020). Contemporary cyber security social engineering solutions, measures, policies, tools and applications: A critical appraisal, 2019-2020. International Journal of Security, 10 (1), 1–15.

Received date 24.02.2022
Accepted date 17.03.2022
Published date 31.03.2022

Sogo Angel Olofinbiyi, PhD, Department of Criminal Justice, School of Law, University of Venda, Private Bag X5050, Thohoyandou, Limpopo, South Africa, 0950
E-mail: olofinbiyis@gmail.com