The Role and Place of Covid-19: An Opportunistic Avenue for Exponential World's Upsurge in Cyber Crime

Sogo Angel Olofinbiyi* and Shanta Balgobind Singh

Department of Criminology & Forensic Studies, College of Humanities, University of KwaZulu-Natal, Republic of South Africa

Abstract: An evidence-based analysis of COVID-19 suggests that the ailment is a bio-medically inclined natural mystic blowing through the world. To this end, this study focuses solely on the role the pandemic plays as an outbreak of cybercrime vector. The study presents a number of the world's most recent cyber insecurity cases that accompanied the onset of the pandemic and findings were discussed within the context of situational opportunity theory of crime. It provides a framework for emergency management approach to protect global citizens and institutions from cyberattacks, as well as, mitigating the outbreak of the crime being propagated by the presence of the novel virus. Global sensitization and awareness programmes across various communities on the potential dangers of cyber insecurity accompanying the COVID-19 pandemic should be helpful. Of most significance, the fight against the invisible warfare should continue with high spirits of relentlessness until absolute peace, relief, resilience and normalcy are able to take root in the global communities.

Keywords: Bio cybersecurity, Coronavirus pandemic, COVID-19, Cybercrime, Cybercriminals, Cyber insecurity, Cybersecurity awareness, Emergency management, Situational opportunistic crime.

INTRODUCTION

Cybercrime is nothing new and has been in vogue for many years as an instrumental response to achieving some specific form of socio-economic and political goals. As the world has evolved into the twenty-first century, so has the value of technologies in our lives grown on a daily basis; and so has the magnitude of crime committed against the mankind using the internet and computer devices escalated (Yar and Steinmetz, 2019). Cybercrime indisputably connotes a sort of crime that embraces internet or computer facilities as a medium to commit crime. Precipitating issues around this type of crime have become high-profile, particularly those surrounding hacking, phishing, cyber terrorism, malware, identity theft, child pornography, spam et cetera (Hill and Marion, 2016). Cybercrime 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 (Holt, 2016). Over the years, hacking has taken on a grossly different dimension to criminality and is solely functional to the activity of cyber criminals. Cyber criminals, whether good or bad, have created an ecological space to stay and have a role in our society as long as technologies advance (Mohammed *et al*., 2020).

Recently, as coronavirus evolved on the global spectrum, there seems to be an exponential upsurge in the activities of cyber criminals, as most of them have relentlessly been taking undue advantage of the emerging pandemic, using the available cyberspace to exploit people and organizations of their resources. This assertion forms the subject of this discourse. The Novel Coronavirus Disease, famously being referred to as COVID-19, was speculated to have originated from a Seafood Wholesale Market in Wuhan City, China (Shereen *et al*., 2020; WHO, 2020). Coronavirus cases have been ravaging the outermost and innermost part of the world for the past five months. Consequently, health systems of roughly all affected nations have collapsed and have become unfit to provide the basic right to health of their citizens (Amnesty International, 2020). No vaccine has hitherto been discovered to mitigate the effects of the virus for rapid recovery. Consequently, all governments of the world have only adopted a unified measure motivating the public for self-isolation, which we believe, is the only way forward for now. There is no point denying the fact that many countries have introduced and imposed lockdown rules and orders to compel people for social distancing (TRT, 2020). Unfortunately, in a bid to enforce the laws and maintain social control at various quarters, there have been several incidents of blatant and stark violations of human rights by the law enforcement agents. (Amnesty International, 2020). As the COVID-19 pandemic roars across the global continent, we are all threatened and

Address correspondence to this author at the Department of Criminology & Forensic Studies, College of Humanities, University of KwaZulu-Natal, Republic of South Africa; Tel: +27671017973; Fax: +27713870178; E-mail: sogoukzn@gmail.com

E-ISSN: 1929-4409/20

worried about the effects of this catastrophe on sustainable development. Reports show that in countries where the virus has already hit, a significant number of people, including innocent children, have already 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 (WHO, 2020).

On the global scale, COVID-19 has now been confirmed in more than 208 countries and territories around the world according to the World Health Organization (WHO, 2020). Neither the rich nor the poor have been spared. The death toll and the number of people being tested positive to the virus are rising on a daily basis (WHO, 2020). In support of the WHO's report, as of April 6, 2020, there had been more than 1.2 million confirmed cases of COVID-19 around the world and more than 69,000 deaths, according to Johns Hopkins data at the time of this writing. The U.S is currently having 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 (WEF, 2020).

In Africa, the numbers of those who are being tested positive are rising every day with over 10,000 confirmed cases of the virus and more than 480 deaths at the moment of this writing. According to the available data, more than 993 people had recovered from the virus. 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 on the poor and marginalized people, especially in high-density areas with insufficient water, sanitation and health care infrastructure (Msn News, 2020). 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.

As of today, more than half of the world's activities is on hold owing to COVID-19 pandemic. The coronavirus has presented itself as the most notorious and novel human disaster of the 21st century. Given the rigour and the speedy outbreak of the intractable pandemic, no literature on health-related human security can provide more than a snapshot of COVID-19 risks, threats and countermeasures, as well as its impacts on global health and economy. An important aspect of the cyber risks we face in the world today was recently engendered by the presence of the deadly virus. Its presence has created a life situation that seems to have aroused a global debate and controversy on human rights violation to freedom of movement, such that is commonly caused by the nationwide lockdown, forming part of the suggested global measures to reduce the speed of contagion across a diverse range of human societies (Givetash *et al*., 2020). So far, so good, whether you are working from home, out of work, self-isolating or caring for others, it must be universally accepted that these are lonely and dark times for all. Though every life situation appears as if it were on hold right now, the fight for global health security, economic buoyancy and emancipation from all shackles of oppression inflicted on the world by the notorious virus should not cease until the global sphere is recovered from this horrible pestilence.

THE GROWING THREATS AND MULTIDIMENSIONAL IMPACTS OF COVID-19 ON THE GLOBAL POPULACE

The war against COVID-19 has launched a thousand military metaphors in the British press and this invisible warfare has been described as the greatest challenge of enormous proportion to humanity since the "Second World War" (BBC, 2020). The nomenclature ascribed to the virus as an 'invisible enemy' cannot be contested, given the magnitude of the collaborative and technologically proven health weapons put in place by many of the countries of the world where the coronavirus has hit; yet the virus continues to blossom and emerge stronger, moving across the world like a wild fire and incapacitating our daily enterprises to the extent that all global citizens are ordered to retreat to their foxholes (BBC, 2020).

Many questions have been touring the world based on the metaphorical representation of COVID-19. One of the questions is: Is this indeed a war or mere ailment? If the question were to be answered, then how is Britain as well as the U.S (the World's Acclaimed Super Power of All Time) doing? Their frontline troops (health workers) are running out of personal protective equipment (PPE) (gloves, aprons, long sleeved gowns, surgical masks, eye goggles, face visors and respirator masks), ammunition (hospital beds) and heavy equipment (ventilators) (The Wall Street Journal,

2020). Supply lines are stretched thin and the worst case-scenario is that the countries' leaders– the Prime Minister, the President and members of the White House, Secretary of State for Health and the Chief Medical Officers of Hospitals – are all inactive and self-isolated in their bunkers where they cannot be functioning at 100% (The Conversation, 2020). On the whole, this study finds that the technologies indeed exist, but confusion reigns and the enemy continues to move among humans unseen. In the fog of war, the world is only relying on case counts to track its movements while it continues to open doors for criminal opportunities and reduce the world's population as it moves along unchecked (Jung *et al*., 2020)

Obviously, the COVID-19 pandemic has overlapped the fields of public health and cybersecurity in ways never lucidly observed in the history of time, generating and strengthening a solemn memory of the existing worldwide underlying problems, unresolved differences and disregarded warning signals that have continued to characterize the world's cyber security (CFR, 2020). The disruption of government and private-sector activities created by unplanned responses to COVID-19 has produced a wide space and leverage for cyber criminals to penetrate the public using different cyber terrorism approaches such as identity theft, malware, phishing, spam email messages and a host of other internet fraud techniques. Government lockdown orders and unprecedented social distancing by employees restricting business and institutional activities have adversely impacted the capacities of many global organizations to keep their computer systems and networks secure from infiltration, especially if being penetrated by sophisticated non-state actors (See CFR, 2020).

As COVID-19's dooms loom larger, the world resorts to sharing the available cyberspace with unknown cybercriminals. Today, COVID-19 has ordered everyone to become more dependent on the internet as desperate measures. It has launched an unexpected social distancing and disrupted economic activity, as well as reducing everyday life to nothing. As a corollary, our 100% dependence on the internet space has rendered us vulnerable to the malicious attempts of cyber invaders, who are fast exploiting the world's sudden and unplanned societal shift to online operations. Reports by the U.S law enforcement officials uphold this assertion, expressing that criminals are now using identity theft approach, selling fake COVID-19 cures online, posing as intergovernmental or governmental health organizations in phishing emails, and inserting malware into online resources tracking the pandemic (CFR,2020)

CORONAVIRUS AS AN OUTBREAK OF CYBER-CRIME VECTOR

Evident from various official reports, this paper has described COVID-19 as an outbreak of cybercrime vector. Currently, there have been limited statistical reports on cyber criminality related to the outbreak of COVID-19. Besides the criticism against the UK's response to the viral outbreak, a report by the National Fraud and Cybercrime Reporting Centre (NFCRC) in the United Kingdom recently uncovered that:

> *"21 reports of fraud linked to the virus, with victims' losses adding up to over £800,000. It was added that ten of the reports included the purchase of face masks from fraudulent online sellers; and one of the victims paid £15,000 for the apparently imaginary face masks, which were never delivered" (Action Fraud, 2020).*

More information from NFCRC disclosed that fraudsters had been using brand-names of World Health Organization (WHO) and the U.S Centres for Disease Control and Prevention (CDC), e-mailing potential victims and posing as if they were working with those organizations (Action Fraud, 2020). Evidence in support of this assertion is captured in the online report as follows:

> *"The fraudsters disguised to be WHO's covid-19 agents for the victims. They claimed they would be able to provide a list of infected people in the victim's area. The victims were then asked to click on links to malicious websites in order to obtain the lists and were at the time asked to make payments in Bitcoin".*

Based on background information from the United States Cybersecurity and Threat Intelligence unit, cybercriminals have been harnessing phishing and malware to target victims in Italy, the United States, Ukraine and particularly Iran, *inter alia* other nations (Recorded Future, 2020). Moreover, there was a cyber hack attack on the U.S Department of Health and Human Services during its response to the spread of COVID-19 on the 15th of March, 2020. The attack was primarily targeted at slowing down HHS computer

systems for actual exfiltration of data concerning any possible vaccine for the ailment (CDC, 2020). Finally, as the world strives to combat the demonic coronavirus outbreak, the global security experts are struggling to devise more means to uncover their malicious domains, so are cybercriminals becoming more dynamic at intensifying more efforts targeted at creating "zoom domains" as an important source of information gathering and scamming, since they are cognizant of "zoom" as the most commonly used, top-notch remote platform upon which organizations execute official transactions as well as exchange of business ideas during this sober sovereignty of the notorious virus. It is a truism that schools, tertiary institutions, private and public organizations, governmental and non-governmental organizations, banking systems, immigration organizations, to mention but a few, are not exempted as cheap preys to the relentless cyber adventurers. Our conclusion here, based on the available data, is that potential cyber criminals have been taking huge advantage of COVID-19's ever-increasing outbreak to create newly registered domains through which they attract the public interest. As of today, the number of newly registered domains related to coronavirus has grown up since the outbreak of COVID-19 has become more ubiquitous (see Figure **1**).

More information from the South African Banking Risk Information Centre (SABRIC) unravelled that cyber criminals have set on track using the novel coronavirus global panic as a delectable tool in their search for valuable banking information from citizens (Magubane, 2020). SABRIC disclosed that coronavirus scammers are using "social engineering" to exploit people with concerns for their health and safety. By definition, social engineering is the art of manipulating people with a view to convincing them to give up their confidential information. However, the types of information these criminals are seeking can vary, but when individuals are targeted, the criminals are usually trying to trick them into giving out their vital information such as, passwords or bank information. Alternatively, they may attempt to access your computer so as to secretly install malicious software that will give them access to your passwords and bank information, as well as having control over your computer.

In a statement by SABRIC's acting CEO, Susan Potgieter:

> *"scammers employed the use of spoofed emails to penetrate clients. Spoofed emails often look convincingly legitimate and, in the fog of panic, clients could easily click on a risky link where they would otherwise not think twice".*
>
> *"Although some spoofed emails can be difficult to identify, we urge bank clients to think twice before clicking on any link, even if an email looks legitimate. Any suspicious emails should not be opened and are best deleted."*

Moreover, there are a number of media reports that child pornography as well as sexual exploitation is another potential risk associated with the pandemic, as children across the world are on emergency holidays due to the spread of the virus. Consequently, some parents are granting permission to their children to join

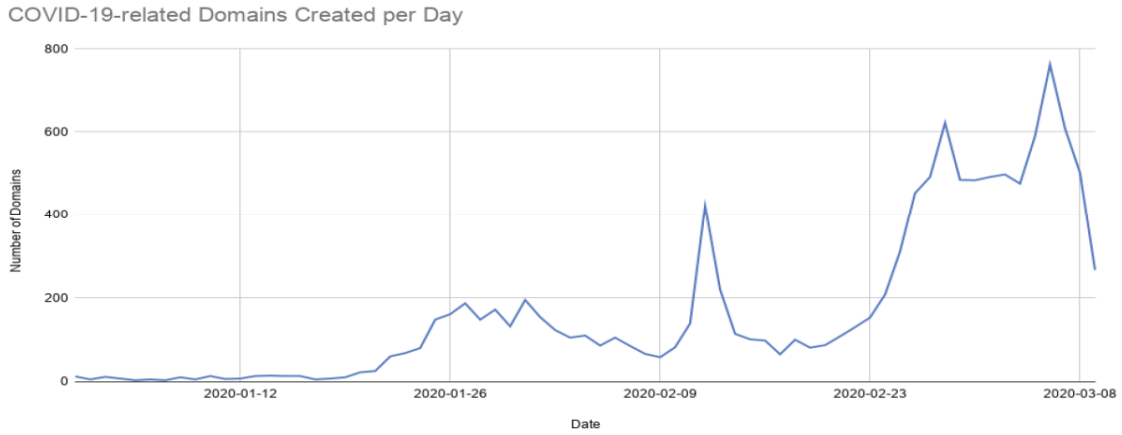

Figure 1: Graph showing the registrations of COVID-19-related domains per day in 2020. Recorded Future analysts created a query to find domain registrations of URLs containing "corona," "covid19," or "covid2019." See Addendum for a list of these domains.

Adapted from: Recorded Future®| www.recordedfuture.com | FR-2020-0312 | 14

zoom classrooms. There are reports that these children were coerced into participation in pornographic performances online via zoom video. Hence the Federal Bureau of Investigation (FBI) warns parents, guardians, caregivers, and schools to be extra-ordinarily vigilant against online sexual exploitation of children in their custody (Conner and Buckelew, 2020).

Evidence from the Boston Division of the FBI reported:

> *"video-teleconferencing hijacking, also called zoom-bombing, is emerging nationwide to exploit children sexually. There are also multiple reports of conferences being disrupted by pornographic, hate images and threatening language".*

However, as at the time this paper was written, there was relatively limited information source to substantiate these findings. It is, nevertheless, crucial to know that this study leveraged its findings upon these reports to describe the novel coronavirus disease (COVID-19) as a pandemic cyberattack vector.

TRIGGER FACTORS AND CYBERCRIME IN THE WAKE OF COVID-19

The best explanations for the recent world's upsurge in cyber insecurity can adequately be provided 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 emergency management principles. 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 Centre or institutions of learning. Given the above explanation as well positioned by Felson and Clarke (1998), routine activity theory seems helpful in understanding 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.

The routine activity paradigm has its origin from 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 (Boivin and de Melo, 2019.; Felson and Clarke (1998). 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. See Figure **2** for diagrammatic illustration.

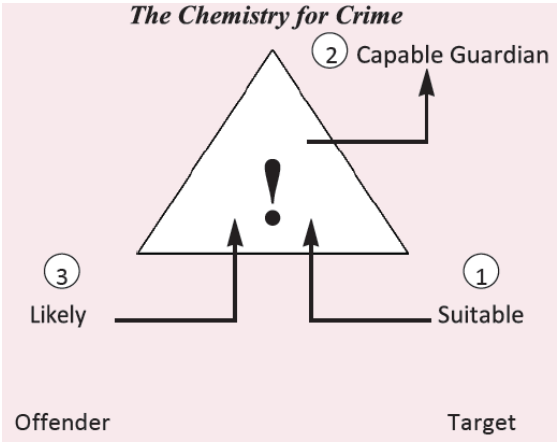

Figure 2: Routine Activity Theory and the Basic Crime Triangle.

Source: Felson, Marcus. 1998. *Crime and Everyday Life*, Second edition. Thousand Oaks, CA: Pine Forge Press.

Further explanation of routine activity approach contends that the target is often preferred over 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 (Ten Boom, Pemberton and Groenhuijsen, 2019). From another point of view, a target's risk of criminal attack is influenced by four main elements, summed up by Felson and Clarke (1998), using the acronym VIVA:

- Value
- Inertia
- Visibility
- Access

The distinction 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 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 internet 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 into 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 online data reports, COVID-19 pandemic laid the foundation for the escalation of the incessant 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 component of the explanation is that many more organizations at this period have been left unguarded owing to global COVID-19 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.

The study provides a framework for emergency management approach to protect global citizens and institutions from cyberattacks, as well as mitigating the outbreak of the crime propagated by the presence of the novel virus. Emergency management in the view of Amy and Philip (2001:2), is "a complex policy subsystem that involves an intergovernmental, multiphase effort to mitigate, prepare for, respond to, and recover from disasters". Of particular relevance, this perspective suggests a tetrapartite approach to mitigate a disastrous situation like this, if arisen either now or in the future. This approach, according to Federal Emergency Management Agency (FEMA, 1997), is known as Comprehensive Emergency Management (CEM) (see Figure **3**). The approach highlights four phases of modern disaster management.

i. Mitigation-This involves activities undertaken in the long term, prior to disaster strikes. They are designed to prevent emergencies and wane the damage that emanates from those that occur, including modifying the causes of hazards, lessening vulnerability to risk, and diffusing potential losses.

ii. Preparedness-This involves activities undertaken in the shorter term, prior to disaster strikes. They are designed to enhance the response and readiness of organizations and communities to disasters effectively.

iii. Response-This entails activities undertaken immediately following a disaster to provide emergency assistance to victims and remove further threats.

iv. Recovery- These are short- and long-term activities undertaken after a disaster. They are designed to return people and property in an affected community to at least their pre-disaster condition of well-being (FEMA, 1997).

Figure 3: An Interactive Schematic Sketch for Emergency Management.

Source: Boston University Emergency Management.

This approach will definitely be needed to manage and salvage both the public health and security sectors from the on-going biological warfare that has already inflicted millions of people and claimed thousands of lives of the world population.

CONCLUDING REMARKS

An evidence-based understanding of COVID-19 suggests that the ailment is a bio-medically inclined natural mystic blowing through the world. The consequence of which has paved the way for the outbreak of the world's most recent upsurge in cyber insecurity. As millions of lives have remained quarantined to their various abodes, global activities abruptly became disrupted with no hope of resumption in sight, all human daily routines have been moved online to compensate for the in-office activities, coronavirus pandemic continues to provide motivations and more opportunities to cyber adventurers who have been devising all routes to revive their dwindling financial situations. Given the enormity of deaths, health insecurity and socio-economic disasters recorded against the scourge, the paper submits that the world should face the reality and come together as one to fight this battle and rid the planet of this mystic. The international community should strive to launch a joint-task front against the coronavirus. In this regard, the World Health Organization, which is utmost positioned to pioneer a joint effort should stop asserting that member states are not forthcoming with data (TRT World News, 2020). The fight against the invisible warfare as first espoused by the American President, Donald Trump (BBC, 2020) should continue with high spirits of relentlessness until absolute peace, relief, resilience and normalcy are able to take root in the global communities.

SAFETY AND EMERGENCY MANAGEMENT MEASURES

To mitigate the spread and effects of COVID-19, global communities should not relent but continue to implement more stringent measures that enforce social distancing and remote working, *inter alia* health management mechanisms, as the trends continue. All organizations should ensure that they have appropriate measures in place to respond to a data breach should one occur. This will chiefly be relevant to all organizations whose employees are working remotely. All organizations should be encouraged to carry their IT teams and internet security experts along in this struggle. This is necessary to determine their rapid response capacities against any form of internet threat should the need arise. In as much as companies and organizations across the world have adopted the remote working system since the onset of COVID-19, there is urgent need for everyone to ensure that their computer systems are resistant to cyber threats. To achieve this, all employees' and individuals' cyber hygiene needs to be fortified with powerful anti-virus software that can be sensitive to external invasion.

Members of various communities should be reminded that government's extraordinary measures against COVID-19 do not automatically excuse parties from taking measures to protect personal and confidential information. All Companies and organizations are requested to include cyber risks as part of their Covid-19 response plan, as well as ensuring that remote-working employees are updated on what to do in cyber emergency (Rosalind and Naidoo, 2020). More importantly, there must be global sensitization and awareness programmes across various communities on the potential dangers of cyber insecurity that accompanied the COVID-19 pandemic.

The study implores the World Health Organizations and other health organizations of concern (particularly those on the frontline of research to discover a universally and scientifically approved vaccine for the virus) to intensify efforts in their fight against the global scourge. The truth now is that we are in the fog of this war and the global medical teams are 24 hours awake to provide a therapeutic vaccine for the ailment. In the same vein, since the coronavirus pandemic is a twin phenomenon of increased cyber insecurity, we urge cyber security experts and every cyber user to be more vigilant and awake to any potential invasion by internet intruders.

ADDENDUM

Registered Domains

The below URLs are the domain registrations that were created in similarity with the existing (authentic) COVID-19 related domains between January 1 2020 and April 6 2020

coronavirusoutbreakmap[.]com

www.coronavirusoutbreakmap[.]com

corona-virus[.]healthcare

coronavirusprotectionmasks[.]org

www[.]coronavirusprotectionmasks[.]org

coronavirus[.]1point3acres[.]com

coronavirus[.]dev

wuhancoronavirus[.]blogspot[.]com

coronavirusdata[.]org

www[.]coronavirusdata[.]org

coronamap[.]live

coronamap[.]site

coronatoken[.]org

bestcoronavirusprotect[.]tk

coronavirusnigeria[.]ng4n[.]com

corona[.]yagi[.]news

info-coronavirus[.]be

www[.]info-coronavirus[.]be

coronavirusnews[.]world

coronavirus[.]app

endcoronavirus[.]org

coronavirus-reports[.]com

coronavirus-map[.]com

www[.]endcoronavirus[.]org

coronavirusreport[.]buzz

www[.]coronavirusreport[.]buzz

coronavirusupdates[.]eu

coronavirus-monitor[.]ru

coronavirus123[.]com

coronavirusstatus[.]space

coronaviruszone[.]comRecorded Future® | www.recordedfuture.com | FR-2020-0312 | 15

coronavirusofficialnews[.]com

flashnewscoronavirus[.]blogspot[.]com

coronatracker[.]com

survivecoronavirus[.]org

corona[.]help

coronaboard-env[.]csgy3mxprm[.]eu-west-1[.]elasticbeanstalk[.]com

coronavirusinformationforus[.]blogspot[.]com

www[.]coronatracker[.]com

blogcoronacl[.]canalcero[.]digital

virus-corona[.]org

coronavirusupdates[.]online

coronavirus[.]zone

coronavirusthermometer[.]com

coronavirusawerness[.]blogspot[.]com

coronavirustoday[.]com

coronavirus[.]cc

corona-virus[.]tokyo

www[.]coronavirustoday[.]com

coronavirus-testing[.]com

stopcorona[.]org

coronavirusecuador[.]com

viruscorona[.]co[.]uk

coronastop28[.]com

coronavirusepidemia[.]blogspot[.]com

coronanow[.]kr

corona[.]kpwashingtonresearch[.]org

coronaviruses[.]com[.]au

mycoronavirus[.]world

coronavirus-in[.]space

coronawatch[.]eu

coronavirus[.]cms[.]am

www[.]coronawatch[.]eu

trackcorona[.]net

coronavirustechhandbook[.]com

coronavirus[.]tghn[.]org

coronawatch[.]now[.]sh

trackcorona[.]live

coronavirusupdate[.]tk

corona[.]kompa[.]ai

whereisthecoronavirus[.]comRecorded Future®| www.recordedfuture.com | FR-2020-0312 | 16

thecoronaviruslive[.]info

coronastats[.]net

coronalive[.]just-shared[.]top

coronavirus19news[.]com

coronavirus[.]page

coronavirusdefense[.]com

www[.]thecoronaviruslive[.]info

coronavirusaware[.]xyz

coronavirus[.]koudaitour[.]com

coronavirusabc[.]com

www[.]trackcorona[.]live

corona-nearby[.]com

coronabye[.]com

trackcoronavirus[.]com

preventcoronaviruses[.]blogspot[.]com

www[.]coronavirusabc[.]com

vaccine-coronavirus[.]com

coronavirus-realtime[.]com

whatcoronavirus[.]com

wuhan-virus-coronavirus-advice[.]blogspot[.]com

corona[.]sums[.]ac[.]ir

REFERENCES

Action Fraud. 6 March 2020. Coronavirus scam costs victims over £800k in one month. Available at: https://www.actionfraud.police.uk/alert/coronavirus-scam-costs-victims-over-800k-in-one-month National Fraud and Cybercrime Reporting Centre. U.K

African Argument. 7 April.2020. Coronavirus in Africa Tracker: How many covid-19 cases & where. Available at: https://africanarguments.org/2020/04/07/coronavirus-in-africa-tracker-how-many-cases-and-where-latest/

Amnesty International. 4 March 2020. Available at https://www.amnesty.org/en/latest/campaigns/2020/03/covid-19/

Amnesty International: Available at: https://www.amnesty.org/en/latest/news/2020/04/covid19-as-an-emergency-human-rights-issue/

Amy K. Donahue and Philip G. Joyce. 2001. A Framework for Analyzing Emergency Management with an Application to Federal Budgeting. Public Administration Review, Vol. 61, No. 6, pp. 728-740. https://doi.org/10.1111/0033-3352.00143

BBC. 11 March. 2020. Coronavirus: A visual guide to the pandemic. Available at https://www.bbc.com/news/world-51235105

BBC.19 March 2020. Coronavirus: Trump puts US on war footing to combat outbreak. Available at: https://www.bbc.com/news/world-us-canada-51955450

Boivin, R. and de Melo, S.N., 2019. The concentration of crime at place in Montreal and Toronto. *Canadian Journal of Criminology and Criminal Justice*, *61*(2), pp.46-65. https://doi.org/10.3138/cjccj.2018-0007

Boston University Emergency Management. 31 March. 2020. Available at: https://www.bu.edu/emd/emergency-management/emergency-management-principles/

CDC. 2020. Coronavirus. Available at shttps: //www.cdc.gov/coronavirus/2019-ncov/index.html Huang.

Conner strong and Buckelew. 2 April 2020. COVID19 presents potential for increased risk of child exploitation .Available at:https://www.connerstrong.com/blog/insights-detail/covid-19-presents-potential-for-increased-risk-of-child-exploitation/

Deprose, M. 28 March 2020: Southern Africa: Covid-19 as an emergency human rights issue. Msn News. Available at: https://www.msn.com/en-za/news/africa/southern-africa-covid-19-as-an-emergency-human-rights-issue/ar-BB11PDiy?li=BBqfWMJ&c=37331085359436976 90&mkt=en-us

Federal Emergency Management Agency (FEMA). 1997. Partnership for a Safer Future Strategic Plan FY1998 through FY2007, with Operational Objectives through FY2003. September 30.

Felson, M., and Clarke, R.V. 1998. *Opportunity Makes the Thief: Practical theory for crime prevention.*

Givetash, L. C., Nancy I., Mulligan, M., and Denne, L. 24 March 2020. Coronavirus: U.S. and Europe tighten lockdowns as restrictions lift in origin of pandemic. Available at: https://www.nbcnews.com/news/world/coronavirus-u-s-europe-tighten-lockdown-restrictions-lift-epicenter-n1167391

Hill, J.B. and Marion, N.E., 2016. *Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century: Computer Crimes, Laws, and Policing in the 21st Century*. ABC-CLIO.

Holt, T.J., 2016. Cybercrime. *The Handbook of Measurement Issues in Criminology and Criminal Justice*, pp.29-48. https://doi.org/10.1002/9781118868799.ch2

Jung, S.M., Akhmetzhanov, A.R., Hayashi, K., Linton, N.M., Yang, Y., Yuan, B., Kobayashi, T., Kinoshita, R. and Nishiura, H., 2020. Real-time estimation of the risk of death from novel coronavirus (COVID-19) infection: Inference using exported cases. *Journal of clinical medicine*, *9*(2), p.523. https://doi.org/10.3390/jcm9020523

Magubane, K. 17 March 2020. Banking body warns of coronavirus scams targeting panicked public. Fin 24.Avaialble from: https://www.fin24.com/Companies/Financial-Services/banking-body-warns-of-coronavirus-scams-targeting-panicked-public-20200317

Mohammed, A.M., Idris, B., Saridakis, G. and Benson, V., 2020. Information and communication technologies: a curse or blessing for SMEs?. In *Emerging Cyber Threats and Cognitive Vulnerabilities* (pp. 163-174). Academic Press. https://doi.org/10.1016/B978-0-12-816203-3.00008-3

Recorded Future. 12 March 2020. capitalizing on coronavirus panic, threat actors target victims worldwide. Available at: https://www.recordedfuture.com/coronavirus-panic-exploit/

Rosalind Lake and Priyanka Naidoo. 19 March 2020. Cyber risk during Covid-19 outbreak. Cyber Law News South Africa. Available at: https://www.bizcommunity.com/Article/196/639/201771.html

Shereen, M.A., Khan, S., Kazmi, A., Bashir, N. and Siddique, R., 2020. COVID-19 infection: origin, transmission, and characteristics of human coronaviruses. *Journal of Advanced Research*. https://doi.org/10.1016/j.jare.2020.03.005

Ten Boom, A., Pemberton, A. and 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), pp.222-238. https://doi.org/10.1080/15564886.2019.1575300

The Conversation. 1 April 2020. Coronavirus: If we are in a war against COVID-19, then we need to know where the enemy is. Available at: http://theconversation.com/coronavirus-if-we-are-in-a-war-against-covid-19-then-we-need-to-know-where-the-enemy-is-135274

The Wall Street Journal. 5 April 2020. Hospitals Facing Coronavirus Are Running Out of Masks, Other Key Equipment. Available at: https://www.wsj.com/articles/hospitals-facing-coronavirus-are-running-out-of-masks-other-key-equipment-11584525604

TRT World News. 17 March 2020. Available at: https://www.trtworld.com/life/the-international-community-fails-to-form-a-joint-front-against-coronavirus-34626

WHO. 2020. Introduction to nCoV. Retrieved 28 March 2020, from https://openwho.org/courses/introductionto-ncov

World Economy Forum. 6 April 2020. COVID-19: What to know about the coronavirus pandemic on 6 April. Available at: https://www.weforum.org/agenda/2020/04/covid-19-what-to-know-about-the-coronavirus-pandemic-on-6-april/

World Health Organization .2020. WHO Statement Regarding Cluster of Pneumonia Cases in Wuhan, China Geneva 2020. Available from: https://www.who.int/china/news/detail/09-01-2020-who-statement-regardingcluster-of-pneumoniacases-in-wuhan-china

Yar, M. and Steinmetz, K.F., 2019. *Cybercrime and society*. SAGE Publications Limited.

Received on 24-04-2020 Accepted on 22-06-2020 Published on 26-06-2020

DOI: https://doi.org/10.6000/1929-4409.2020.09.20