Journal of Theoretical and Applied Information Technology
15th June 2021. Vol.99. No 11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

COVID-19 AGE: CHALLENGES IN CYBERSECURITY AND POSSIBLE SOLUTION DOMAINS

ZAINA ALSAED[1], MAHMOUD JAZZAR[2]
Palestine Technical University – Kadoorie
Faculty of Graduate Studies
Jaffa Street, Tulkarm, Palestine
E-mail: [1]z.i.saed@students.ptuk.edu.ps, [2]mjazzar@ptuk.edu.ps

ABSTRACT

Threats to cybersecurity and cyberattacks respect no boundaries. Cybercriminals always try to exploit any crisis to facilitate their attacks, and of course, the COVID-19 pandemic is not an exception. From the very first beginning of the COVID-19 virus outbreak in March 2020, it has become very effective tool to commit cybercrimes as it has not only triggered huge upheavals in health, education, and the economy but has also led to broad implications on communication and information technology as well. In line with the increasing number and scope of cyberattacks, the growing concern caused by the pandemic has increased the possibility of successful cyberattacks. The significance of this paper is to highlight and review some types of cyberattacks associated with the COVID-19 presence. In addition, the paper recommends some guidelines and countermeasures for the micro-level of families, individuals and for business enterprise to implement potential means of risk management plans to actively mitigate and control the consequences of such malicious attacks.

Keywords: *COVID-19, Cybersecurity, Cybercrime, Cyberattacks, Risk Management*

1. INTRODUCTION

The middle of March 2020, after the breakout in the city of Wuhan, China, has witnessed the appearance of the COVID-19 virus, which is also named "2019-nCoV", "SARS-CoV-2" and "the Coronavirus". Organizations and governments around the world had to impose some restrictions and rules to reduce physical social contact to control the spread of the COVID-19 virus. These restrictions included social distancing policy, travel-bans and stay-at-home; work-from-home (WFH) orders [1]. However, life must go on, which implied that dependency on Internet services. data traffic has grown exponentially and unexpectedly, due to the high records of users' numbers, who have shifted to work remotely, use e-learning methods, in addition to online shopping, online bill payment, and much more services online [2]. Furthermore, introducing new programs to be used more than ever in cyberspace, e.g., video conference programs under time pressure, and predominantly, without adopting appropriate security environments [3].

Although the easy interconnection of Internet services has provided some kind of convenience for users, unfortunately, the rise in the usage of such services has led to a sharp increase in vulnerability to cybercrimes and heightened digital security risks during this pandemic which is directly linked to the use of the Internet. Therefore, while the globe is concerned with the universal risk posed by COVID-19, cybercriminals worldwide indeed are ready to exploit this pandemic by creating and transferring a different form of "viruses".

COVID-19 crisis is considered a challenging issue for cybersecurity. Such crisis has highlighted serious reminders of already existing unheeded problems that tend to define and improve cybersecurity means. This included some types of data damage and destruction, in addition to forms of cyber espionage, sabotage, fraud, embezzlement, theft of intellectual property, and harming business reputation [4].

This paper analyzes the system of cyber-attacks during the COVID-19 pandemic, discuss the the most important cyber-attacks that have been exposed worldwide during the pandemic. In addition, the relationship between threats, vulnerabilities and risks is linked through the cyber threats associated with the pandemic. The main objectives of this paper are to treatise statistics of

Journal of Theoretical and Applied Information Technology
15th June 2021. Vol.99. No 11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

cybercrime incidents during the sudden, unplanned COVID-19 crisis from different perspectives, and brief review of existing research about recorded cyberattacks with a critical analysis of such attacks. Moreover, the study discusses how sectors and companies have maintained privacy as well as the limitations. Further, categorizing the cyberattacks that were committed through the pandemic. Finally, suggesting tips and possible future solution domains to the problems stated.

2. RELATED WORK

As Parhami [5] expected, the daily rate of generated data in the 2020s will be 1 million levels up from daily generated data in the 2010s. This enormous amount of processed, transferred and stored data requires adequate methods of cybersecurity. This is primarily based on means of network, data, asset protection from any illegal access or modification [6]. Some essential terms associated with cybersecurity should be clear; in which to comprehend the data flow of information within cybersecurity. These interchangeably used terms are threats, assets, vulnerabilities, and risks. An asset could be a property, person, and information that should remain well protected. A vulnerability is a gap or a weak point in a software or a system that can be exploited by a threat. A threat is anything that exploits a vulnerability to damage an asset. A function of existing threats exploiting vulnerabilities to obtain, damage, or destroy assets cause a risk that must be well managed to affect the threats. The relationship between these terms is briefly demonstrated in Figure 1.

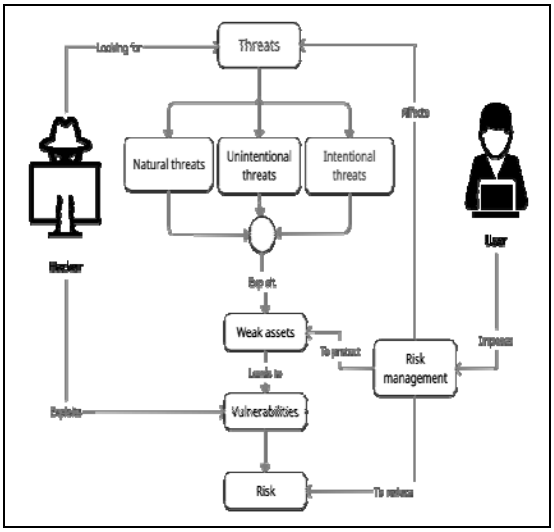

Figure 1: Threat, Vulnerability, and Risk Flowchart

Mitigation of cybersecurity impact was standardized by several organizations. Among these was The National Institute of Standards and Technology (NIST). One of its main objectives is to reduce and mitigate the influence of attacks by developing and implementing security guidelines, protocols, and frameworks. For instance, the most recent security framework designed for critical infrastructure suggested by NIST is version 1.1 [7]. It is based on the functions of Identification, Protection, Detection, Responding, and Recovering. Moreover, The International Organization for Standardization (ISO) has also provided a risk management framework under standard ISO-31000 [8]. Even though several frameworks for cybersecurity were suitable for small and large organizations, but their expediency has not been proved in the COVID-19 crisis yet.

The research area of COVID-19s' cybersecurity-associated impact is still very tight; because the greatest blackness of related work has only discussed the consequences of tracking applications that harm privacy concerns [9], [10]. Among these, a study has highlighted the apprehensions of installing similar applications. One of these applications was a mobile app called TraceTogether, which was released by the Singaporean government [11]; it is based on communication between adjacent Bluetooth devices when the app users are identified as a "Corona patient". They are asked to fill in information via the app, which could present a serious vulnerability and fertile ground to different privacy attacks [12].

Hitherto, the number of proposed privacy concerns and mitigation strategies is still not

sufficient. Framing the problem slightly differently, De Carli, et al stated that data collection in the health sector is vulnerable and risky due to the possibility of being compromised by opponents [13]. Accordingly, researchers have proposed a privacy-protection application named Wetrace. To increase security in data collection, this app employs Bluetooth low energy to transmit the message to the pointed destination.

Furthermore, some recent publications gave prominence to the implications of the expanding usage of technology. Which is marking more concerns and threats in terms of cybercrimes every day owing to this pandemic. In this context, the work of [14] has figured out the top ten-cybersecurity threats and severely affected sectors that were associated with the COVID-19 pandemic. Likewise, [4] focused on the cybersecurity issues that appeared from the challenging WFH instructions based on worldwide orders.

Attackers often spend long-time for discovering system vulnerability and for figuring out how to exploit and to gain access to information. However, penetrating the human mind does not require the same amount of time and effort, because humans are usually dominated by feelings and emotions that facilitate control over them. The pandemic makes these types of attacks such most dangerous methods used in hacking, as there are no protection programs or final solutions to limit and eliminate them. As such, attackers usually resort to using them when there are no specific vulnerabilities or methods to penetrate the target. Rather, it is all about training and educating people to reduce these attacks.

3. RESEARCH METHOD

The research approach is based on the randomization technique. Such technique involves randomly allocating experimental and tangible units across control and experimental groups that represent large groups. As such, the study characterise reflection and analysis of cyberattacks happen during the pandemic to impose the reason and the possible solution domains.

3.1 Most Vulnerable Sectors to Covid-19 Themed Attacks

3.1.1 Healthcare Sector

Across the boards, modern healthcare systems are established and built on an Information and Communication Technology application basis. In which it facilitates a large scale of medical services known as e-healthcare. It also offers a distinctive user experience to all of such systems' users, including healthcare staff and patients as well. Emphatically, Healthcare systems present the most targeted systems during the recent pandemic period, due to their direct link to the COVID-19 crisis. To clarify more, any lapse could lead to a critical situation ending in a loss of precious human lives. Moreover, any sort of malicious cyberattacks will probably outgrow the challenges currently encountered by the health sector. With wealth, resources, and workers, which are already expanded and are put under double pressure. They are also taking a vital place in response to the coronavirus. Whereas securing human lives is their major goal.

For instance, DDoS attacks was directed to The Department of Health and Human Services in the USA. It was committed by establishing a huge number of connection requests approximated to millions for a long time [15]. Fortunately, it was reported that this attack did not cut off the system utterly. Nevertheless, similar attacks could lead to unfavorable consequences and may cause disastrous conditions sometimes. As result, such attacks contribute to potential increase of botnets agents worldwide and amplification of such attacks.

3.1.2 Governmental Organizations and Media Outlets

The accuracy of information provided by the government and the media outlets amid the COVID-19 outbreak is a very challenging matter. Any delay or awry misleading information could result in creating fear and hype between the citizens. Hackers exploit this critical situation by spreading wrong information. They tend to do this by committing cyber-attacks on this sector. Leading to leverage anxiety and concerns that raise distrust between the public and the governments [16].

3.1.3 Business Enterprise and Financial Services

Aside from being an illness, that is a serious threat to human lives. COVID-19 has also shaken the global economy and international commerce and has put them at stake. Of course, that caused menacing businesses, distributing supply chains, and paralyzing daily lives. Resulting in a massive impact that will last for several years. Plenty of cyberattacks were directed to this sector, seizing the predictions of a financial recession during the outbreak of novel coronaviruses. Such of these were ransomware [17], malware, and phishing attacks [18]. With a sum of 18,235,

COVID-19-associated cyberattacks reports and about 13 million USD were lost due to cyber extortion. The US Federal Trade Commission assessed that a cost of millions USD was also ruined due to COVID-19-themed swindling transactions within a period of three months from Jan to Apr 2020 [19]. Furthermore, in regular situations, users in this sector were vulnerable to attacks of social engineering. In which the hacker masquerades to be a legit user to have access to the victim's personal information [14].

3.2 COVID-19-Themed Cyber Incidents and Attacks Taxonomy

More than ever, Hackers intend to take advantage of the expanded and tangled cyberattack surface. This was a highlighted result of the COVID-19 pandemic. In this context, according to Trends Micro's estimations [20], up to November 2020, the third quarter of this year, a total of 3,818,307 email threats and about 1 million hits on malicious URLs relating to COVID-19 were reported. With an increase of 47.4% from the second quarter to the third one of this year. Figure 3 outlines key cyber threats during the Coronavirus pandemic.

3.2.1 Regional Cybercrime Trends

While the coronavirus continues to transfer across the boards, cybercrime has spiked through the nations as well. With a variation of crime trends from a region to another. An overview to highlight the regional COVID-19-associated cyber threat trends landscape is provided below. Figure 2 illustrates the distribution of COVID-19-associated cyber threats among such regions.

Americas

After the official announcement of COVID-19 as a global pandemic. The government of the United States of America has been one of the major targets of cyberattacks. The recent massive data breach of the US government is proof of that. The remarkable US data breach or “the Sunburnt” hack, is described as one of the biggest data breaches not only in American history but also the global history. The victims of this cyber-espionage campaign are still under investigation by the Federal Bureau of Investigation. It was only detected at the end of 2020 after being dormant since March 2020. The US government has already acknowledged that the State Department, the Department of Homeland Security, and parts of the Pentagon had been compromised. With a record of 18,000 affected users so far. According to Reuters, hackers compromised emails sent by officials at the Department of Homeland Security. Experts say it could take several years to fully understand and estimate one of the worst hacking operations [21].

A marked dramatic increase in phishing attacks and fraud campaigns was also recorded in the United States of America. By taking advantage of the recent, prolonged crisis of COVID-19 breakout among people with a daily record of 20,000 to 30,000 attacks [22]. The adoption of teleworking in the USA by many organizations has become an efficient tool to gain control by cybercriminals. They progressively target employees by stealing high-risk and sensitive data. Furthermore, a sort of ransomware campaign has been launched. This was done by using LOCKBIT malware, which targets medium-sized enterprises in this area. Regarding sextortion by social media, child sexual exploitation models have intensified as well. Criminals intend to commit child sexual exploitation, in which the offenders contact their victims abusing social media's different platforms during the universal lockdown across the globe [23].

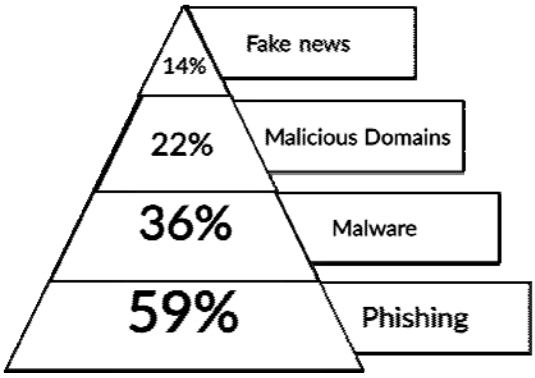

Figure 2: Distribution of the Key COVID-19 Inflicted Cyberthreats

Africa

Cyber threats in this region recorded a significant increase. Especially after the growth of using online or credit card payment methods over cash payment one. As a result, people have become more vulnerable to cyberattacks. Additionally, after starting the implementation of the work from home (WFH) policy by most institutions and companies there. Due to blending work and home environments, the exposure of these companies to cyber threats was heightened. Such as charity scams, sextortion, and phishing as well as a

deliberation of false information on social media [24].

Asia and South Pacific (ASP)

The most challenging issue here was the lack of cybersecurity awareness. Therefore, the most common cybercriminal trends reported in the ASP region were: the spread of wrong and misleading news related to COVID-19, fraud and phishing campaigns in addition to the online circulation of fake or illegal medical supplies, drugs, and weapons. An increasing number of cyber threats directed to teleconference tools was also recorded [23]. An internal European Union said that Russia's state-aligned media has held a huge misinformation campaign to degrade the influence of the COVID-19 and to spread fear and panic. This campaign is not targeted abroad only but also has reached national information too [25].

Middle East and North Africa (MENA)

MENA area outlined a developing utilization of social media to amplify and spread misinformation news regarding the COVID-19 pandemic. The role of social media was not limited to that only, but extended to include marketing of licensed and unlicensed products related to the Coronavirus. Moreover, phishing campaigns, registration of malicious domains, and online fraud related to COVID-19 were noticeable in this region [23].

3.3 Remarkable COVID-19 Themed Attacks

Figure 3 represents several cyberattacks that were associated with the presence of the COVID-19 pandemic. These affect the three primary security goals of:

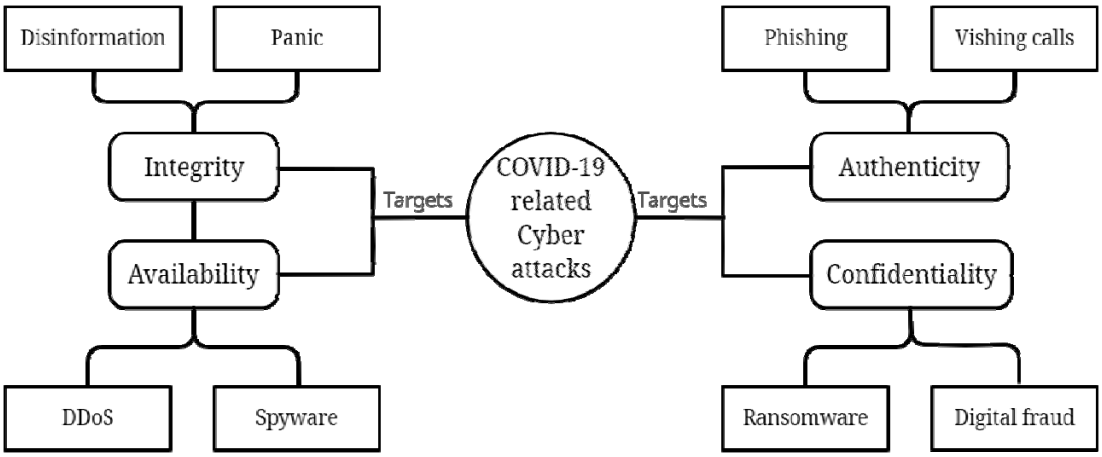

Figure 3: Key COVID-19 Themed Cyberthreats

Europe

About 66% of part nations from Europe announced a critical expansion in the malicious domains enrolled with COVID-19 related words. Such words as "Corona" and "COVID" are used to exploit the developing number of individuals looking for data about COVID-19 on the web [23]. Cybercriminals are also exploiting the pandemic to spread ransomware attacks against infrastructure that are already in critical charge of responding to COVID-19 challenges. Widespread phishing attacks are notable in Europe by law enforcement agencies, besides the frequent occurrence of cloning official government websites, to steal critical and confidential data for later use in future cyberattacks.

- *Confidentiality:* which guarantees that data is available only to allowed users. It is usually accomplished by encryption (which is the process that guarantees that information is covered to the external environment but open to associating users). To achieve economic advantages, criminals employ several kinds of methods, like ransomware. They do this to obtain an unapproved way to use tools, encrypt, and secure individual data on their devices. These events occur in significant business troubles to people and corporations [26].

- *Integrity:* The primary purpose of integrity is to protect information from any premeditated or unexpected variations by permitted/unpermitted users [26]. This

perspective guarantees that data is in its primary copy and keeps the information proportion of interior and outer applications. Through the COVID-19 outbreak, some crimes have concentrated on the integrity of such systems. So that illegal health experts profess to be approved specialists and use diverse methods (e.g., e-mail spam, phishing calls). This is mainly done to attract people towards gaining their criminal economic profits.

- *Availability:* assures that information and sources are immediately accessible to accredited users, especially through crises [26]. The COVID-19 crisis has observed numerous crimes that attack different areas (e.g., the healthcare sector, which was the most critical knockout). In addition to using malware attack approaches to interrupt the accessibility of crucial systems. The last outcome of endangering this security goal could end in rescheduling crucial medical operations, arrangements, and suspension in many therapies for patients.

- *Authenticity [27]:* is the newest extension to the CIA trio. Its basic aim is to confirm that the obtained information or message transfer is referring to that primary root. Such a goal is often obtained by authentication assurance through both static and dynamic schemes. Multiform malware was formulated throughout the COVID-19 outbreak to promote the embezzlement of data credentials owned by the user. Anxieties have also been boosted related to security and inspection, e.g., using COVID-19 tracing applications [28].

3.3.1 Disruptive Malware

This type of attack aims to make information unavailable or disturb the framework, worsening a generally desperate circumstance.

3.3.1.1 DDoS Attacks

Europol reported a consistent spike in DDoS assaults during the pandemic. These have noteworthy outcomes because the number of Internet clients is increased noticeably. This is due to social separating, telecommute conditions, and online instructive exercises (e.g., video instructional exercises) [29]. The US Health and Human Services Department also reported a relative incident of such attacks in March 2020.

3.3.1.2 Ransomware Attacks

CERBER, NetWalker, and Ryuk are the most common ransomware campaigns that were recently reported by INTERPOL private partners. These attacks skyrocketed during April 2020 by several hacking bands. These had been moderately lethargic a couple of months ago of that time. This infers that there are some cases in which some companies or organizations have been hit already, where the ransomware has not yet been activated. Cybercriminals are now even spreading ransomware-as-a-service on the deep web.

An Android application, named CovidLock, is an example of ransomware attacks during the recent pandemic. This app was launched to track information and statistics on COVID-19. To continue the process of installing and using the app, users should give specific permissions to their device. Once it is already installed, the user's personal information emails and social media accounts are inaccessible anymore. Unless the victim pays a specific amount of money called the ransom using bitcoins, there is a possibility to publish the users' information, exfiltration of sensitive data, and erasing the device data [30].

3.3.2 Malicious Domains

Hackers steal and exploit personal information by launching malicious websites, to use it for their intended aims. 3% of these are malicious, in addition to 5% of them that are suspicious. The COVID-19 relevant regions are approximately a half more than those recorded during the same time and more than the latest occasional events [31]. More than 4,000 domains registered with the words "coronavirus" and "COVID-19" have appeared on the internet since the beginning of 2020 according to the Checkpoint Risk Intelligence report [32]. While some of them are legitimate, but cybercriminals attempt to launch a large number of websites daily. In which malware spreading, phishing campaigns, and servers are compromised. Such domains are used as a honeypot for the victim and are employed to hold several frauds [6].

3.3.3 Phishing and Online Fraud

A social engineer can combine more than one aspect when carrying out an attack: human, computer, technical, social, and physical. Examples

of these attacks include direct attacks, impersonation, shoulder surfing, dumpster diving, being a third party, phishing attacks, baiting attacks, pretexting attacks, tailgating attacks, ransomare attacks**,** pop-up windows, scareware, phone/email scams attacks, quid pro quo and robocalls attacks.

From January 2020, the beginning of the novel Coronavirus outbreak, and according to Trend Micro's reports, about 900K messages linked to COVID-19 were detected. Exploiting the economic crisis and people's fear caused by COVID-19 existence. Cybercriminals have promoted their COVID-19-based social engineering methods by using COVID-19. RiskIQ [32] observed an incident in which over 300K spam e-mails over three days containing either "COVID" or "Corona" keywords. Such sort of emails comes under the pretext of COVID-19-related subjects that refers to information like "COVID-19 updates" and tags like "Dr" or "Prof".

The offenders pretend to take the role of the World Health Organization (WHO), to pull victims to fall into the trap by clicking on the attached files with the mentioned tags and extensions of ".rtf" [23].

3.3.4 Misinformation

The presence of the COVID-19 sudden pandemic has been a fertile environment for spreading fake and misleading news and claims. With the help of the widespread of social media networks across the globe. The world has all been sunk with infodemic attacks and distrust presumptions. That has resulted in global hype, fear, and panic during this health crisis [33].

Social Networking Platforms including Facebook, WhatsApp, and LinkedIn, were containing a huge amount of false or untrusted information. For instance, many articles on social media were spread as a tutorial on how to make homemade sanitizers. In addition to some claims that suggest ayurvedic medicine as an effective way against the infection of COVID-19, or drinking tea and some herbal combinations can prevent COVID-19 incubation and transmission, without any scientific proof or evidence to validate these allegations. This mainly leads to creating confusion between the audience and sometimes causing fatal consequences [34].

Furthermore, the threat of misleading information regarding the results of the American elections 2020 was announced by The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA). Cybercriminals could launch new websites, change the content of existing websites, besides sharing misleading posts on social networking platforms. This was done to prevail fake news to discredit the honesty of electoral tactics and procedures and to spread distrust in U.S. officials.

3.4 Potential Mitigation Solutions

3.4.1 General Guidelines

The most notable influence of COVID-19 is the turn of the cybersecurity scene from a corporate environment to a home one. The unexpected transformation has presented many new possibilities to cybercriminals. It resulted in rising a skyrocketed chance of vulnerability threatening. Throughout the COVID-19 crisis, a new stream of cyberattacks was witnessed. Working from home policies have also doubled the risk of cyber threats due to multiple reasons.

In the business context, the safety of hardware and software assets has to be well maintained by the IT relief staff and authorization to systems. Internet surfing should also be supervised under strict cybersecurity strategies. IT-associated assets should also be repaired and renewed periodically.

Likewise, working from home through employees' PCs with their inadequate networks extend the chances of cybercrimes. Thus, dealing with these vulnerable and unsafe transfer ways from home presents an entrance to hackers. User knowledge and awareness are significant to relieve and degrade the hazard of future cyberattacks. The most relevant security hints are: First, businesses that permit workers to utilize their PCs to WFH implement Bring Your Own Device (BYOD) strategies. These include security tips to help users to guard their tools.

Next, another approach is VPN adoption to interact among employees' private PCs and companies when applying WFH policies. Finally, the cybersecurity experience of workers has to be improved frequently by cybersecurity training schedules.

3.4.2 Rapid Risk Management Frameworks

One of the most effective ways to access, mitigate, and estimate the resulting risk of a threat is to use risk management frameworks. Such

frameworks are available, including SCADA systems [35], and cyber-physical systems [36], [37],[38],[39]. Therefore, the COVID-19 crisis justifies the need of creating a new, adequate, and agile framework that can be executed instantly. The required properties of this potential system are high scalability, accuracy, and time-efficiency. Which can be easily implemented and used by different types of users. Users who could be either technical-skilled or even non-technical-skilled computer users within changing conditions like remotely-based or office-based environments.

In addition to utilizing collaborative platforms, like INTERPOL's Collaborative Platform which was produced for information interchange and operative assortments. This stage affords a reliable resolution for member provinces to fasten in multi-jurisdictional shared task capabilities. It helps to fight offenses upon computer systems. This promotes fundamental connections between operational teams in the affiliate nations and with INTERPOL for the efficient distribution of cybercrime knowledge. It also works to produce suitable operational acknowledgment for the disturbance.

3.4.3 Fighting Infodemic Campaigns

When it comes to counter infodemic campaigns during an ongoing crisis like COVID-19, the matter becomes more challenging. Especially when determining the originality of the posted content on social media platforms. Accordingly, collaborative support of stakeholders is a serious need. Specially to control the phenomenon of infodemic campaigns. The involvement and cooperation between computer, social, and healthcare experts are also efficient. They represent a step towards the improvement of the process of identification and classification of fake online information.

Fulfillment of Prohibition Standards and Raising Awareness also help in fighting against infodemic campaigns. The progression of COVID-19 relevant infodemics is proposed to remain posing operational barriers for law enforcing bureaus, healthcare organizations as well as social experts across the world. To relieve these difficulties, blocking such campaigns through training and granting the users to be protected on the web is indispensable.

3.4.4 International Collaboration

A cooperative venture from diverse nations and governments through pandemics is very crucial, such as the continuous COVID-19 danger. To face and counter COVID-19-related cyber-attacks, work and plans of potential countermeasures are needed from the worldwide association. As well as launching an international task force to aid the distribution of contemporary cybersecurity skills. The importance of economic assistance cannot be undervalued in international cooperation projects, such as cyber hygiene education. Still, several priorities continue to appear and compete throughout pandemics' presence. Consequently, the support of funds of mitigation initiatives is also much needed to be listed among the means of countermeasures.

Collaboration and data transfer is expressly decisive to discuss these cyberthreats:

- Ransomware crimes upon the significant foundations, Signs of Compromise, Bitcoin bearings.
- Incidents linked to Credit Payment Deception and BEC.
- Malware publishing through non-official user tracing apps.
- Information concerning campaigns utilizing a massive scale of malicious domains.

3.4.5 Software Tools

Many software tools can support both corporations and the micro-level of individuals to defense against the cyber threats related to the novel COVID-19 virus crisis. These introduce software tools such as Intrusion Detection Systems (IDS), Security Information and Management Systems (SIEM), Big Data Analytics, and Intrusion Protection Systems (IPS). Such as monitoring and prevention systems for any cyberattack that could occur [41]. Petrenko et al. [42] emphasize that these methods and tools present a model of effective information security support systems as they detect and prevent unapproved use.

To react to the increase in economic aid support to their citizens, many national government companies in the US essentially required COBOL (Common Business Oriented Language) experts to refresh their software systems. This has proved the boundaries of resolution of legacy systems for different infrastructures and a shortage of software specialists who are responsible for controlling and supporting these applications. IT has now possessed an essential part in each project. It has also shifted the core of developments in marketing, education,

governance, courts, and more. On top of urgent requirement lists COBOL programmers should also be included to fight against COVID-19 [43].

3.4.6 Secure and Updated Systems

In this area, especially after blending work environments with the home environment by WFH policies, effort should be directed towards ensuring

the reliability and security of home systems. For instance, reinforcing operating systems is one of the most efficient mitigation plans that was approved by the Australian Signals Directorate's Australian Cyber Security Centre [40].

4. CONCLUSION

The COVID-19 era is an alarming call to all of us. The human being, IT, and our entire world and business after-COVID-19, will no longer remain as it used to be. In terms of cybersecurity, the recent COVID-19 crisis has opened prospects; revealed gaps and threats of existing IT systems, plans, and execution; and bestowed the IT shareholders, experts, and parties many potential challenges. Many companies and organizations are developing plans and strategies and spending huge amounts of money to overcome cyberattacks. Therefore, there are still many limitations and ineffective procedures in the ways to detect and reduce these continuous and increasing attacks. As result of the massive development in technology, technical expertise of the attackers, and tremendous technological development, there are unexpected vulnerabilities and increasing demand by humans for the use of technology.

The significance of this study is to highlight measured perspectives of the COVID-19 pandemic associated with cyber threats hazards and established respective countermeasures to mitigate the resulting risk of such cyberattacks. There is a set of hints, strategies to consider, investigate, examine, plan, and implement to face future similar pandemics.

ACKNOWLEDGMENT

The authors wish to thank Palestine Technical University-Kadoorie (PTUK) for supporting this research work as part of PTUK research fund.

REFERENCES:

[1] C. Sohrabi *et al.*, "Corrigendum to 'World Health Organization declares Global Emergency: A review of the 2019 Novel Coronavirus (COVID-19)' [Int. J. Surg. 76 (2020) 71–76] (International Journal of Surgery (2020) 76 (71–76), (S1743919120301977), (10.1016/j.ijsu.2020.02.034))," *Int. J. Surg.*, vol. 77, 2020.

[2] K. Mohsin, "Cybersecurity in Corona Virus (COVID-19) Age", *SSRN Electron. J.*, 2020,

[3] J. Wiggen, "The impact of COVID-19 on cyber crime and state-sponsored cyber activities", 2020. [Available]. Available: http://www.jstor.org/stable/resrep25300

[4] T. Ahmad, "Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity", *SSRN Electron. J.*, 2020.

[5] B. Parhami, "Data Longevity and Compatibility", in *Encyclopedia of Big Data Technologies*, Cham: Springer International Publishing, 2018.

[6] S. Hakak, W. Z. Khan, M. Imran, K. K. R. Choo, and M. Shoaib, "Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies", *IEEE Access*, vol. 8, 2020, pp. 124134–124144.

[7] Barrett Matthew, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1", Gaithersburg, MD, Apr. 2018.

[8] Iso, "ISO 31000 Risk management ISO 31000."

[9] W. Z. Khan, M. Y. Aalsalem, and M. K. Khan, "Communal Acts of IoT Consumers: A Potential Threat to Security and Privacy", *IEEE Trans. Consum. Electron.*, vol. 65, no. 1, Feb. 2019.

[10] W. Z. Khan, M. Y. Aalsalem, M. K. Khan, and Q. Arshad, "Data and Privacy: Getting Consumers to Trust Products Enabled by the Internet of Things", *IEEE Consum. Electron. Mag.*, vol. 8, no. 2, Mar. 2019.

[11] H. Cho, D. Ippolito, and Y. W. Yu, "Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs", Mar. 2020, [Available]. Available: http://arxiv.org/abs/2003.11511

[12] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy", *Found. Trends Theor. Comput. Sci.*, vol. 9, no. 3–4, 2013, pp. 211–407.

[13] A. De Carli *et al.*, "WeTrace -- A Privacy-preserving Mobile COVID-19 Tracing Approach and Application", Apr. 2020, [Available]. Available: http://arxiv.org/abs/2004.08812

[14] N. A. Khan and N. Zaman, "Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic", 2020.

[15] S. Stein and J. Jacobs, "Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak", [online]., 2020. https://www.bloomberg.com/news/articles/2020-03-16/u-s-healthagency- suffers-cyber-attack-during-covid-19-response. (accessed Dec. 06, 2020).

[16] A. Cook, "COVID-19: Companies and Verticals at Risk for Cyber- Attacks", [online]., 2020. https://www.digitalshadows.com/blog-and-research/covid-19-companies-and-verticals-at-risk-for-cyber-attacks/ (accessed Dec. 06, 2020).

[17] A. Al Hajj, "Cyber Security in the Age of COVID-19: An Analysis of Cyber-Crime and Attacks", *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 8, no. 8, Aug. 2020.

[18] Y. Dion and S. Brohi, "An Experimental Study to Evaluate the Performance of Machine Learning Algorithms in Ransomware Detection", *J. Eng. Sci. Technol.*, vol. 15, Dec. 2020, pp. 967–981.

[19] P. Witt, "COVID-19 scam reports, by the numbers", [online]., Apr. 15, 2020. https://www.consumer.ftc.gov/blog/2020/04/covid-19-scam-reports-numbers (accessed Dec. 12, 2020).

[20] "Developing Story: COVID-19 Used in Malicious Campaigns", [online]., Nov. 2020. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains (accessed Dec. 12, 2020).

[21] J. Tidy, "SolarWinds: Why the Sunburst hack is so serious", [online]., 2020. https://www.bbc.com/news/technology-55321643 (accessed Dec. 24, 2020).

[22] M. 365 D. T. I. Team, "Exploiting a crisis: How cybercriminals behaved during the outbreak", [online]., 2020. https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/ (accessed Dec. 24, 2020).

[23] "Alert (AA20-099A) COVID-19 Exploited by Malicious Cyber Actors", [online]., Apr. 08, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-099a (accessed Dec. 13, 2020).

[24] "COVID-19 Cybercrime Analysis Report-August 2020", 2020.

[25] I. Greenberg and K. Fomina, "Russia says it has hardly any coronavirus cases. Doctors say otherwise", [online]., 2020. https://www.codastory.com/waronscience/russia-coronavirus-mistrust/ (accessed Dec. 22, 2020).

[26] S. Hakak, A. Kamsin, O. Tayan, M. Y. I. Idris, and G. A. Gilkar, "Approaches for preserving content integrity of sensitive online Arabic content: A survey and research challenges", *Inf. Process. Manag.*, vol. 56, no. 2, 2019, pp. 367–380.

[27] W. Stallings, M. Bauer, and E. M. Hirsch, "Computer Security Prinicples and Practice", 2013, p. 13.

[28] T. Sharma and M. Bashir, "Use of apps in the COVID-19 response and the loss of privacy protection", *Nat. Med.*, vol. 26, no. 8, Aug. 2020, pp. 1165–1167.

[29] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy", Oct. 2019.

[30] L. Whitney, "CovidLock ransomware exploits coronavirus with malicious Android app," [online]., Mar. 17, 2020. https://www.techrepublic.com/article/covidlock-ransomware-exploits-coronavirus-with-malicious-android-app/ (accessed Dec. 13, 2020).

[31] "Update: Coronavirus-themed domains 50% more likely to be malicious than other domains", [online]., 2020. https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/ (accessed Dec. 22, 2020).

[32] TEAM RISKIQ, "Investigate | COVID-19 Cybercrime Weekly Update", [online]., Jun. 18, 2020. https://www.riskiq.com/blog/analyst/covid1

9-cybercrime-update/ (accessed Dec. 13, 2020).

[33] O. Beavers, "Pompeo says China, Russia, Iran are spreading disinformation about coronavirus", [online]., 2020. https://thehill.com/policy/national-security/488659-pompeo-says-china-russia-iran-are-spreading-disinformation-about (accessed Dec. 22, 2020).

[34] S. Menon, "Coronavirus: Herbal Remedies in India and Other Claims Fact-CheckedNo Title", [online]., 2020. https://www.bbc.com/%0Anews/world-asia-india-51910099

[35] Y. Cherdantseva *et al.*, "A review of cyber security risk assessment methods for SCADA systems", *Comput. Secur.*, vol. 56, Feb. 2016, pp. 1–27.

[36] H. Kure, S. Islam, and M. Razzaque, "An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System", *Appl. Sci.*, vol. 8, no. 6, May 2018, p. 898.

[37] F. Flammini, Ed., *Resilience of Cyber-Physical Systems*. Cham: Springer International Publishing, 2019.

[38] H. Mokalled, C. Pragliola, D. Debertol, E. Meda, and R. Zunino, "A Comprehensive Framework for the Security Risk Management of Cyber-Physical Systems", in *Resilience of Cyber-Physical Systems: From Risk Modelling to Threat Counteraction*, F. Flammini, Ed. Cham: Springer International Publishing, 2019, pp. 49–68.

[39] G. Falco, A. Noriega, and L. Susskind, "Cyber negotiation: a cyber risk management approach to defend urban critical infrastructure from cyberattacks", *J. Cyber Policy*, vol. 4, no. 1, Jan. 2019, pp. 90–116.

[40] I. Chomiak-Orsa, A. Rot, and B. Blaicke, "Artificial Intelligence in Cybersecurity: The Use of AI Along the Cyber Kill Chain", 2019, pp. 406–416.

[41] S. A. Petrenko, "Big Data Technologies for Cybersecurity", 2018.

[42] T. Weil and S. Murugesan, "IT Risk and Resilience-Cybersecurity Response to COVID-19", *IT Professional*, vol. 22, no. 3. IEEE Computer Society, pp. 4–10, May 01, 2020.

[43] AC SecurityCentre, "Strategies to Mitigate Cyber Security Incidents", 2017, [Available]. Available: https://www.cyber.gov.au/publications/%0Astrategies-to-mitigate-cyber-security-incidents