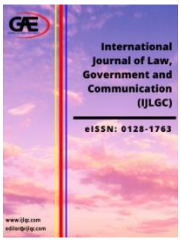
International Journal of
Law, Government and Communication
EISSN : 0128-1763
IJLGC

Volume 6 Issue 24 (June 2021) PP. 104-115
DOI 10.35631/IJLGC.624007



INTERNATIONAL JOURNAL OF LAW, GOVERNMENT AND COMMUNICATION (IJLGC)
www.ijlgc.com

GLOBAL ACADEMIC EXCELLENCE

NEW TRENDS IN CYBERCRIME IN THE MALDIVES - MOVING BEYOND LEGAL MEASURES IN THE NEW NORM

Fathimath Waheeda[1]

[1] Department of Law, The Maldives National University, Maldives
Email: fathimath.waheedha@mnu.edu.mv

Article Info:

Article history:
Received date: 15.04.2021
Revised date: 15.05.2021
Accepted date: 31.05.2021
Published date: 15.06.2021

To cite this document:

Waheeda, F. (2021). New Trends in Cybercrime in The Maldives-Moving Beyond Legal Measures in The New Norm. International Journal of Law, Government and Communication, 6 (24), 104-115.

DOI: 10.35631/IJLGC.624007.

Abstract:

INTRODUCTION
The health emergency crisis due the COVID-19 pandemic has created challenges globally. The same applies to the Maldives, as lockdown and social distancing measures was enforced, the use of virtual communication by public authorities, businesses and individuals likewise increased. The new normal of working from home, video conferencing and meetings, online learning and shopping have created a large group of vulnerable users, providing more opportunities for cybercriminals to exploit. In a time where resources are diverted to fight against the COVID-19 pandemic, the law enforcement, investigative and judicial procedures may be delayed or disrupted due to compulsory prevention measures. The changing face of cybercrime needs to be addressed through non-legal measures to reduce the detrimental effect.

OBJECTIVES
New cybercrimes have emerged during the pandemic, which has affected the vulnerable users in a difficult and unprecedented time. The objective of the study is to identify the nature of cybercrime, including the emerging crimes and to examine how these issues could be addressed through legal and non-legal measures.

METHODOLOGY
The methodology adopted is through the study of secondary data collected through research of recent articles, legal statutes and newspaper articles from March 2020 until present. The data collected was applied through study, observation and analysis.

SIGNIFICANCE
This study will identify the emerging crimes during the pandemic, and bring together different approaches, including non-law measures to highlight the best method to address this issue.

FINDINGS/RESULTS
Forms of cybercrimes identified as prevalent in the country, namely (1) misinformation; (2) phishing and (3) privacy issues. Misinformation and disinformation regarding the virus, cures and conspiracies plays a key role in undermining the public trust and the effectiveness of the public safety

Volume 6 Issue 24 (June 2021) PP. 104-115
DOI 10.35631/IJLGC.624007

measures. The ability to take action through legal measures were limited due inabilty to investigate, non-existence of applicable provisions, underreporting and late reporting amongst others. Non-legal measures such as awareness campaigns and cyber-education were utilised to empower vulnerable groups, especially children and seniors against emerging new forms of cybercrimes.

CONCLUSIONS

With the changing face of cybercrime and the prolonged uncertain future due to COVID-19, there should less reliance on the law and more proactive measures enacted at all levels to reduce the harmful effects.

Keywords:

Cybercrime, Misinformation, Phishing, COVID-19, Maldives

Introduction

The expansion of Information and Communications Technology ("ICT") has transformed the way people interact and live their life. For the Maldives, it provides immense benefits in terms of providing essential services within the country through an information network. The internet became a blessing for many people during the COVID-19 lockdown, as it allowed to communicate, share information and acquire goods during this period. Due to the stringent measures laid by the Health Protection Authority, face to face contact and gathering were restricted. Therefore the number of users, utilising online communication and services increased dramatically, which provided an immense opportunity for criminals to exploit and benefit by abusing vulnerable parties. In the period from January 2020 to September 2020, there was a 65 percent increase in cybercrime as reported in the Crime Statistics report 2020. (MPS, 2020). Even in the new normal, the government has restricted some activities and urged the public to utilize online services to control the spread of the virus. Even before the pandemic, it was a challenge for the government of the Maldives, to make the internet safer, to deter cybercrimes and to protect the national security information structure, in the absence of appropriate cybersecurity measures and adequate legislation.

Background: Current Framework

The Republic of Maldives is an archipelago which comprises of more than 1192 islands and is located in the Indian Ocean. In this many islands nation, only 200 islands are inhabited, with more than 80 islands developed as tourist resorts. The population is widely dispersed, with the capital Male accommodating more than 30 percent of the total population. According to an International Telecommunication Union ("ITU") 2018 Report, the Maldives has an internet usage at 63.2% of the population, which is higher than the Asia Pacific average at 44.3 percent. The mobile cellular subscriptions per hundred is at 206.3 as of June 2018, which is higher compared to the world average at 103.6 and Asia & Pacific average at 104.0. (ITU, 2018).

The government of Maldives is enthusiastic to develop a strong network to enable data exchange between government and related institutions and the E-government services, such as registration of births, driving license renewals, attestation of certificates, police reports, import/export declaration processes, registration of tourist resorts (Ibrahim, 2010). More recently, biometric passports, Edu portals, gov.mv and eCouncil System has been introduced (MCST, 2020). Even before the pandemic many government institutions had websites which provided essential information and downloads to facilitate and provide convenience to the users. Commercial ventures, such as E-commerce websites, online noticeboards, online food delivery services and online booking systems have developed rapidly in the last decade. Further the banking sectors, provides e-services including the Bank of Maldives, who introduced their internet Banking platform in 2007, and followed by their Mobile Banking Application more recently.

In the Maldives, developing the ICT infrastructure brought benefits in creating efficient and innovative methods of communication, commerce and trade. With the rising consumption of the internet and use of ICT, cybercrimes have increased in the country. As Dilipray mentioned in his report of 2014-2015, the country has faced cyber threats, as there are no cyber laws, nor a cybersecurity agency or a threat detection or mitigation system. This state remains true, even at present, which creates challenges to law enforcement due to the lack of an inclusive cybercrime legal framework and the obstacles to evidence collection (Zalif, 2020b). Since, 2009, cybercrime has caused hindrance to the public, and the criminal activities have varied from credit card fraud and phishing, unauthorised access, hacking and chat-abuse as well as blackmail through social media. Fake Short Message Service (SMS), phishing, fake lottery and promotions are widespread activities in the Maldives (Nadira, 2018). Similarly in 2020, the extent of fraudulent activities has increased as compared to 2019, which includes phishing phone calls, requesting money on promotions and through adding credit to phones, using counterfeit transfer slips after online shopping and demanding funds through impersonation (Liusha, 2020). Many E-platforms such as the internet banking and governments websites are often hacked due to the vulnerability and poor security (ITU, 2012).

The challenge here is for the government to make the internet usage safer without minimising the developmental opportunities. The Maldives has neither compiled a cyber-security policy, nor has it drafted or implemented any cyber-security or ICT laws to protect the users from the dangers of internet (Waheeda, 2018). During the outbreak of pandemic COVID-19, new emerging cybercrimes such as misinformation and disinformation and privacy related issues were highlighted. These kind of cyber activities, during an uncertain and unprecedented pandemic, play a key role in undermining the public trust and the effectiveness of the public safety measures. When effective legal measures are not present to curb the growth of misinformation, there are imminent dangers to failure to control the spread of false information. Public diplomacy and awareness raising is critical for prevention and must empower vulnerable groups, especially the children and seniors. At present where the resources are diverted to fight against the pandemic, ensuring effective solution through law enforcement and judicial procedures may not be the best options. The purpose of this essay is to identify the nature of cybercrime, including the emerging crimes and to examine how these issues could be addressed through legal and non-legal measures. The essay commences with a general introduction to the status of cybercrime in the Maldives, followed by the evolution of cybercrime in the pandemic. Further it provides an analysis of cybercrime and the emerging crimes on internet in the mentioned period. Lastly, the text concludes with the discussion of measures adopted to address the cybercriminal activities.

The Evolution of cybercrime in the COVID-19 Pandemic

The pandemic has rendered individuals and society more vulnerable in many respects, such as reliance heavily on the computer systems, smart phones and internet, to work, communicate and share information to mitigate the impact of social distancing. While cybercrime has existed before the COVID-19 health emergency, the extent of cybercrime has taken a different course as cybercrime has become a crime of opportunity. Due to the stringent measures and social-distancing measures imposed by the government, there has been a significant number of users utilising the online information systems for entertainment, education and business, providing an opportunity to exploit vulnerable users.

The Council of Europe (CoE) website (COE, 2020) has listed many vulnerabilities that have been exploited by criminals during this pandemic. The activities common to the Maldives includes phishing campaigns and malware distribution, ransomware, fraud schemes and misinformation and fake news. Phishing campaigns and malware distribution through non-genuine websites, documents providing information or advise on COVID-19 were used to infect computers and extract information. Similarly, ransomware targeted smart phones and other devises of individuals, using credible application to extort payments. Further misinformation and fake news spread through counterfeit accounts, created panic and instability and advanced distrust in the government and leading health institutions. In a moment of opportune fraud schemes misled consumers to purchase masks, sanitizers and fake medicines which claimed to prevent contraction of the disease. In the Maldives, due to the increased consumption, the price of these products rose, leading to government intervention in reducing taxes, to decrease the price increase (Shareef, 2020).

Cybercrime has existed and some forms had been prevalent, before COVID-19 emergency. In contrast cybercrimes such as misinformation and fake news and privacy related issues emerged during in the last year, resulting in serious consequences. Without adequate legal measures and law enforcement power, non-legal measures needs to be adopted to curb and control the criminal conduct.

Definition and Classification of Cybercrime

There is no universally accepted definition of cybercrimes, the word cyber is defined in Cambridge Online Dictionary as "involving, using or relating to computers, especially the internet" and in Oxford Online Dictionary as "relating to or characteristic of the culture of computers, information technology and virtual reality". Brenner (2004) classifies computer crime in three categories: (1) the use of a computer as a target of criminal activity; (2) the use of a computer as tool or instrument used to commit a criminal activity; and (3) the use of a computer as incidental to the crime.

Wall (2007) describes an approach defining three classes of cybercrime: Computer integrity crimes (Crimes against the machine), Computer assisted crimes (Crimes using the machine) and Computer content crimes (Crimes in the machine). In contrast, Wilson (2008) and Australian High-Tech Crime Centre (2003) classify cybercrimes into two categories: (1) Crime that is committed using computers and networks, and (2) traditional crime that is facilitated through the use of computer. Likewise, Urbas and Choo (2008) classify cybercrimes in two ways: where the computer is the target (eg, hacking, terrorism) and crimes where the computer is the tool (eg, fraud and identity crime). The second category is further categorised by differentiating between technology enabled, technology enhanced and technology supported.

Despite differences in approach, there is core consistency between the classifications. The computer is either the tool or the target. Further, there are many international instruments which deals with cybercrimes. The Commonwealth of Independent States Agreement on

Cooperation on Combatting Offences related to Computer Information 2001 (CIS Agreement) describes cybercrimes as a "criminal act of which the target is computer information'. The Shanghai Cooperation Organisation Agreement describes the offences as the "use of information resources and the impact on them in the informational sphere for illegal purposes".

The Council of Europe (CoE) Convention on cybercrimes in 2001 was the first international instrument seeking to address cybercrimes and harmonise the national laws. The CoE describes criminal acts committed "using electronic communication networks and information systems, or against such networks and systems' as cybercrimes. The CoE classifies computer crime or cybercrimes in four main categories as: (1) Offences against the confidentiality, integrity and availability of computer data and systems; (2) Computer-related offences; (3) Content-related offences, and (4)Offences related to infringements of copyright and related rights.

The CoE (2003) introduced an additional category "acts of racist and xenophobic nature" committed through computer systems. The categories have been used as guidelines developing national legislation related to cybercrimes by many countries. However, it should be noted that the CoE categorisation does not include some types of crimes that have emerged, through the use of ICT such as money laundering and identity theft. Because of the wide range of offences involved under the cybercrimes as stated in United Nations Office on Drugs and Crime (UNODC) study, it is best described as a collection of acts, rather than one single act. The UNODC considers 14 offences grouped under three broad categories (UNODC, 2013). These categories are shown in Table 1.

The terminology and grouping utilised in the above categorisation is based on the CoE Convention, with a slight difference where the computer-related offences and offences related to copyright infringement are merged into one category; the "computer-related acts for personal or financial gain or harm". The studies conducted by UNODC are based on this category where it shows many countries do not identify a large range of offences outside the 14 activities listed above.

In the Maldives, the commonly used term is "cybercrime" which addresses internet related crime. In the absence of cyber-specific legislation defining the term and the different criminal activities which it encompasses, the categories above- mentioned will be left open and to be decided based on case-by-case basis. At present, the law enforcement and the investigation are in the best position to identify activities in the forms of cybercrimes and hence prosecute them accordingly. The term is mostly used to define criminal activities using the internet and the context of computer devises and smart phones. The term cybercrime has been used in relation to cyber-criminal activities most common in the country such as hacking, Denial of service (DoS) attacks, online credit and debit card fraud and phishing (Hassan, 2017). In 2020, the crime statistics report identifies cybercrimes, including credit card fraud, hacking and identity theft (MPS, 2020).

Considering the broad variance of cybercrime, in the Maldives, at the stage where cybercriminal legislation is considered, the CoE categorisation provides essential insight into adopting new offences and guidance into enacting national legislation. Likewise, the UNODC provides the most common activities which is termed as cybercrimes.

Volume 6 Issue 24 (June 2021) PP. 104-115
DOI 10.35631/IJLGC.624007

Table 1 UNODC Categorisation

Acts against the confidentiality, integrity and availability of computer data or systems	Computer-related acts for personal or financial gain or harm	Computer content-related acts
❖ Illegal access to a computer system; ❖ Illegal access, interception or acquisition of computer data; ❖ Illegal interference with a computer system or computer data; ❖ Production, distribution or possession of computer misuse tools; and ❖ Breach of privacy or data protection measures	❖ Computer-related fraud or forgery; ❖ Computer-related identity offences; ❖ Computer-related copyright or trademark offences; ❖ Sending or controlling sending of Spam; ❖ Computer-related acts causing personal harm; and ❖ Computer-related solicitation or 'grooming' of children	❖ Computer-related acts involving hate speech; ❖ Computer-related production, distribution or possession of child pornography; and ❖ Computer-related acts in support of terrorism offences

Source: United Nations Office of Drugs and Crime (UNODC). (2013). Comprehensive Study on Cybercrime. New York: United Nations.

New and Emerging Cybercrimes During the Pandemic

In 2020, the pandemic created a "surge of malicious cybercrime" as cybercriminals has become more organised as they have pooled their resources to gain an advantage (Interpol, 2020). In order to counter the criminal activities, more collaboration between private and public, and international and domestic intelligence and expertise. The last year has accelerated the digital transformation of countries, and further showcased the cyberthreat landscape, as the volume of cybercrime increased globally (Interpol, 2020).

Some forms of cybercrimes have become more rampant during the outbreak of COVID-19, with the tendency of cybercriminals to exploit any possible opportunities. During this pandemic where most of the population are online for various reasons, certain forms of criminal activities have become more attractive as they are low risk with high yield. Ecommerce data interception and cyber scams has increased as online transactions have increased, cybercriminals have revised their fraud schemes and phishing schemes to lure victims. While many different cybercrimes have emerged the following discussion revolves around the following:

Misinformation

The COVID-19 pandemic has not just caused a health crisis, but also a social media crisis .The proliferation of misinformation on social media is faster than the spread of the virus and therefore can create detrimental consequences individually and within the community. An 'infodemic' of misinformation, as declared by the Director-General of the World Health Organisation (Department of Global Communications, 2020). 'Misinformation' has been defined by Wardle and Derakhshan (2020) as false information shared unconsciously, while disinformation is false information shared with an intent to cause harm. The term malinformation which is considered to be ‘authentic private information’ which is shared with the public to cause detriment by creating hate speech and harassment (Barua et al, 2020).

Due to the pandemic, the public had gone online, the internet has become the greatest source of health information worldwide due to smart phones and low-cost connectivity across the world. Research has shown that 70% of the adults use the internet to search healthcare information. Li et al. (2020) reports mentions that approximately 23-26% of videos in YouTube disseminated misleading videos about the COVID-19 pandemic. Furthermore, Facebook team has also reported that they posted warnings on around 90 million pieces of information creating misinformation about COVID-19 in regards to false cures and propaganda and conspiracy theories (BBC, 2020).

Misinformation about treatments and medicine may cause harm, as many are desperate to a find cure for the disease. BBC News reported that at least eight hundred people may have died because of misinformation related to the pandemic in the first three months of the year (Coleman, 2020). A further study reported that an estimate number of 5,800 people were admitted to the hospital as a consequence of fake information on social media (Islam, 2020). False information may also contribute to stress, fear and mental disorders. Further, amidst the fear of unprecedented health crisis, inaccurate information and exaggerated information may cause health anxiety and long-term stress which may be detrimental in the long term (Barua et al, 2020). In addition, researchers have also highlighted that misinformation in the form of conspiracy theories and religious fundamentalist view may cause and racism and public mistrust and unreasonable behaviour (Barua et al, 2020). Misinformation and inciting of hatred and distrust on the government and the leading health authorities, by criticising their measures and standards also causes discord and dissatisfaction amongst the community.

Misinformation and fake news result in unreasonable behaviour and exacerbate fears leading to behaviour such as toilet paper hoarding and stealing masks. Prices of essential goods and masks and sanitisers amongst others rise, due high levels of purchase due to exuberated fears (Shareef, 2020). In the light increased information, public health authorities using their websites issued precautionary advice and good hygiene practices (Zalif, 2020a). Since cybercrimes increased during the period of pandemic, and the prosecution of cases decreased due to investigation challenges. Non-legal measures need to be fully utilised to create awareness among the society, especially through education.

In the era of social media and the internet, sharing and using information is instantaneous, the individual should be able to manage the information encountered from different sources. The public needs to be equipped with literacy skills to manage this tsunami of information that they receive from daily sources (Mokhtari, 2020).

Phishing

The term “Identity crime” is used to describe offences that comprises of the theft of identity information (“identity theft”) which may lead to the creation of false identities and commission of identity fraud, which is the use of identity information to defraud individuals or businesses (Home Office, 2012). Due to the advancement of technology, new forms of criminal activity have emerged over the internet and social networks, such as blackmail, trolling and libel (Smith, 2013). Each of these crimes, whether traditional or virtual, display different modus operandi and combined with other characteristics, creates challenges for enforcement.

During this pandemic, identity theft issues and phishing attempts increased in the Maldives, reaching the highest in the lockdown period (MPS, 2020), with new methods used to exploit innocent victims. Prior the health emergency, this was the most prominent form of cybercrime in the Maldives (Waheeda, 2018). The methods utilised was different during this period, where the public was more desperate in many ways and therefore easier to manipulate. The following methods of phishing are prevalent in the Maldives and have increased during the lockdown and health security measures: (1) Phishing is the most common type in the cyberspace (Wall, 2013) which is characterised by attempts to fraudulently acquire personal information such as passwords by either impersonating a genuine person or a credible institution, using electronic communication such as emails; (2) Spear phishing have also been used to target specific groups of victims with personalised emails This sophisticated method exploits existing concerns targets groups with personalised mails (Leydon, 2012); (3) Wall (2007), also identifies pharming or spoofing which looks like genuine mails, which encourages individuals to open emails; (4) Pharming or Domain Name System (DNS) cache poisoning (or spoofing) contains seemingly important or relevant information in the sender and subject lines that tricks individuals to open the email (Wall, 2007); (5) Smishing involves sending of messages similar to that of phishing emails, requesting customers to confirm personal details, but these messages are received using SMS messages (Wall, 2013), and (6) Vishing which exploits voice over internet protocol (VOIP) is similar to phishing and smishing but through voice. Victims are deceived into calling back the given number or asked to log onto a web address given in the message (Wall, 2007).

Most of the above mentioned types were present in the Maldives, including phishing and smishing. At a time where the public is more vulnerable, the cybercriminal activities have serious consequences for the public. In addition to the financial detriment caused due to these activities, this also cause stress and anxiety to the individuals. This issue has existed within the country for a long period without an adequate redress. Banks and financial information have been at risk, because of these activities and banks has increasingly cautioned the customers with infomercials and warning and awareness sessions.

Privacy

During the pandemic, the social media and the internet has provided all kinds of information related to the current outbreak. The Health Protection Agency, as the lead organisation used the internet and social media as platforms to divulge information, such as cautions, precautionary measures and recommendations. This has been an essential tool to counteract the health crisis caused by the COVID-19 and used to provide the much required comfort to the public. However, even the HPA website was hacked leaving a video clip on the website (Munawar, 2020). A criminal investigation commenced to identify the perpetrators.

In a country without adequate legislation and data protection, the protection of the citizens and their human rights are difficult, but more critical. The right to privacy which is a fundamental human right, must be ensured, regardless of the situation. Confidential and private information must be kept private unless the subject gives permission to disclose. Revealing personal data about COVID-19 patients and other information must be penalised and ensured that such disclosure will not be repeated. Verbal abuses, and defamatory statements and misleading private information was excessively published on social media. Once published the internet makes it impossible to remove certain data, preventing the observance of the “right to be forgotten” principle of the individual. Personal data in regards to patients are sensitive and confidential data which may have severe consequences for the patient.

Special guidelines and Health codes should be adopted imminently to prevent the disclosure and privacy issues during this period. Public education and awareness has to be created for the issue. Stringent campaigns to inform the public of the error of disclosing information should be shared to resolve these issues as soon as possible.

Effective Measures to curb the cyber COVID-19 crimes

In the new normal conducting normal activities virtually has resulted in many changes to the daily life. During the pandemic, where there is stringent measures of lock down and the applicable social distancing measures, unexpected challenges to the institutions of the government. In a time where resources are still diverted to fight against COVID-19 pandemic, the law enforcement personnel's capacity to counter the new and increasing threats are reduced. Further the investigative and judicial procedures not halted but maybe delayed or disrupted due to changing proactive measures. Prior to pandemic, resolving cybercrime issues has been challenging, due to existing nature of the legal framework and inadequate legislation. Controlling cybercrime needs a multitasker approach due to the unique nature of the crime and due to its commission in cyberspace. More focus needs to be on self-regulation and education and awareness.

The inflexibility of statutes to adapt to the changing nature of cybercrimes makes it more ineffective, especially during a dire health emergency. In regards to cybercrime, the already existing challenges of underreporting and investigation needs to be highlighted and addressed. In the Maldives, cybercrimes have been difficult to prosecute, due to inadequate provisions, difficulty in investigation, and collection of evidence (Zalif, 2020b) creates difficulties if non-legal measures are not introduced. Further, for a country without a cyber law and cybersecurity laws, it becomes impossible to penalise the conduct during the public emergency.

The new emerging activities such as misinformation and phishing, disrupts the already fragile confidence in the system, preventing the effectiveness of the public safety measures. At a point where public diplomacy and trust may play a key factor, in preventing massive spread of the virus. The Health Protection Authority constantly cautioning the public not to panic and to refrain from spreading misinformation was an effective, as it was the main institution in charge (Ibrahim, 2020). Further, the Police Services released a statement that they would take action against persons spreading false rumours to create fear and panic amongst the public through the spread of misinformation (Avas, 2020). The WHO Maldives statement touched the importance of the fight against misinformation as a vital part of the battle against the pandemic globally, which stressed the individual and the media's role in combatting the epidemic through ensuring accurate information to be spread amongst the public. These public statements by the government and law enforcement agency, and International Agencies against the spread of rumours and misinformation had the most effect on the public, as it is voiced from different credible institutions.

To maintain solidarity and trust in the face of the epidemic was an important factor to reduce the risk further consequences to the community. Thus the role of the media, social media platforms, civil society and influencers to strengthen their actions in disseminating accurate information and curbing the spread of misinformation are mainstream to effective public health responses (UNICEF, 2020). The Maldives Broadcasting Commission decided to censure the Channel 13 news outlet for broadcasting a daily program with inaccurate and misleading information (Government of Maldives, 2020). The Maldivian media played an vital role in delivering news and updates in a timely manner from the Health Protection Agency.

The epidemic and infodemic has stressed the importance of information literacy, so that the general public is able to manage the tsunami of information received in daily life (Mokhrari, 2020). It is the government's role to create awareness and health literacy programs, so that individuals can protect themselves against unreliable information which may cause harm. Further they should design educational systems which embeds material at a readable and understandable level, so that the general public will be information literate. Although enforcing law against misinformation may not be possible in the country, it may not be ignored that many other countries have laws to address this issues. The main three types of legal regulation is: rules on content of media and platforms, sanctions against foreign state actors and regulations on anti-establishment speech (Nagasko, 2020).

Conclusion

In conclusion this text describes the emerging and increasing cybercrimes during the period of the pandemic and the need to resolve these issues adequately without relying on legal measures. Many cybercrimes have emerged during the public health emergency, both serious, trivial and disturbing crimes have been committed. At a moment where resources are allocated towards public measures, it may be difficult to resolve these issues. This discussion highlights three emerging cybercrimes such misinformation, phishing and privacy issues, that may need to be resolved to reduce detrimental consequences to the community, through non-legal measures. Advising and cautioning the public, educating and awareness are key to reducing a number of cybercrimes without legal and judicial intervention. With the changing face of cybercrimes and the prolonged uncertain future due to COVID-19 there should be more proactive measures, including legal measures enacted at all levels to reduce the harmful effects.

References

Australian High-Tech Crime Centre (2003), Fighting the Invisible. Platypus Magazine: Journal of Australian Federal Police, 80 2003 4-6

Avas (2020), Police warn against the spreading misinformation on COVID-19. https://avas.mv/en/81603

Baruaa, Z et.al (2020), Effects of misinformation on COVID-19 individual responses and recommendations for resilience of disastrous consequences of misinformation, Progress in Disaster Science, 100-119

BBC (n.d), Social media firms fail to act on Covid-19 fake news, https://www.bbc.com/news/technology-52903680

Brenner, S. W. (2004). U.S. Cybercrime Law: Defining offences. Information System Frontiers, 6(2), 115-132.

COE. (2001) Signed on 23 November 2001; effective on 1 July 2004.https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

COE. (2003) Additional Protocol Signed on 28 October 2003 ; effective on 1 March 2006. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

COE. (2020, March 27). Cybercrime and COVID-19 [Press Release]. https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19

Coleman, A. (2020, August 12) 'Hundreds dead' because of Covid-19 misinformation. *BBC*. https://www.bbc.com/news/world-53755067

Department of Global Communications (2020), COVID-19 Responses, *United Nations*. https://www.un.org/en/un-coronavirus-communications-team/un-tackling%E2%80%98 infode mic%E2%80%99-misinformation-and-cybercrime-covid-19

Dilipraj, E. (2014-2015). South Asian Cyber Security Environment: An Analytical Perspective. South Asian Defence Review. India: KW Publishers.

Government of Maldives (2020), Statement by the Government of the Republic of Maldives on the Decision by the Maldives Broadcasting Commission to censure local news outlet Channel 13. https://www.gov.mv/en/news-and-communications/statement-by-the-government-of-the-republic-of-maldives-on-the-decision-by-the-maldives-broadcasting-commission

Hassan, A. (2017). Cybercrime ge shikaara akah nuvumah heyluntherivama. [Take care not to become a victim of cybercrime]. *Police Life*

Home office (2012), False ID Guidance. http://www.homeoffice.gov.uk/publications/alcohol-drugs/alcohol/alcohol-upporting-guidance -/false-idguidance?view=Binary

Ibrahim, M & Ahmed, Ilyas (2010). Maldives. In S. Akhtar and P. Arinto (Ed), Digital Review of Asia Pacific 2009-2010 (p262-267) Delhi, India: Sage Publications.

Ibrahim, N. (2020) Two or more people tested positive for COVID-19 in the Maldives, *The Edition.* https://edition.mv/news/15383

Interpol (2021). ASEAN Cyberthreat Assessment: Key Cyberthreats Trends Outlook From The ASEAN Cybercrime Operations Desk, Interpol.

Islam, M.S. et.al COVID-19 Related Infodemic and Its impact on Public Health: A Global Social Media Analysis, The American Society of Tropical Medicine and Hygiene, 103 (4) 1621-1629

ITU. (2012). Readiness Assessment for Establishing a National CIRT (Afghanistan, Bangladesh, Bhutan, Maldives and Nepal), ITU/IMPACT

ITU (2018), Measuring the Information Society Report – Maldives.https://www.itu.int/en/ITU-D/LDCs/Documents/2017/Country%20Profiles/Country%20Profile_Maldives.pdf

Leyden, J. (2012, September 26). If you see 'URGENT tax rebate download' in an inbox, kill it with fire. http://www.theregister.co.uk/2012/09/26/spear_phishing_hooks/

Li, H.O., Bailey, A. M. J., Huynh, D. & Chan, J.W.T., YouTube as a source of information on COVID-19: a pandemic of misinformation?, BMJ Glob Health, 5 (5) (2020), Article e002604, 10.1136/bmjgh-2020-002604

Liusha, A. (2021, February 2). Makaraai Heealthun Massalathakun Salaamahvuma Heyluntheri vaan jehey [Have to be aware of fraud cases] *Police Life.* https://www.policelife.mv/page/151210

Mokhtari, H & Mirzaei, A (2020), The tsunami of misinformation on COVID-19 challenged the health information literacy of the general public and the readability of educational material: a commentary, Public Health, 187, 109-110

MCST. (2020). https://www.unescap.org/sites/default/files/H.E.%20Mr.%20Maleeh%20Jamal%2C%20Minister%2C%20Ministry%20of%20Communication%2C%20Science%20and%20Technology%20of%20Maldives.pdf

MPS, (2020). Crime Statistics-Quarter 1, 2020. https://www.police.gov.mv/s/crime_stats_quarter1_2020.pdf?v=1.1

Volume 6 Issue 24 (June 2021) PP. 104-115
DOI 10.35631/IJLGC.624007

MPS. (2020). Crime Statistics-Quarter 2, 2020. https://www.police.gov.mv/s/crime_stats_quarter2_2020.pdf?v=1.1

MPS, (2020). Crime Statistics-Quarter 21, 2020. https://www.police.gov.mv/s/crime_stats_quarter3_2020.pdf?v=1.1

Munawar, R (2020, May 4). Maldives commences investigations into HPA website hack. *The Edition.* https://edition.mv/news/16523

Nadira, F. (2018) Makara heelathun faisa hoadumuge massalathah raiiyithun mihaarah vure bodah heyluntherive samalukan dheynjehey. [The Public should be more aware and cautious of cases of acquiring money through fraud and deception]. http://www.policelife.mv/page/132679

Nagasko, T. (2020) Global Disinformation campaigns and legal challenges, International Cybersecurity Law Review 1 125 – 136

Shareef, A. (2020, March 19). COVID-19: President waives import levies on surgical masks, hand sanitizers. *The Edition.* https://edition.mv/news/15596

Smith, R. (2013). Identity theft and fraud. In Y. &. Jewkes (Ed.), Handbook of Internet Crime. Cullomption: Willian Publishing.

Wall, D.S. (2007). Cybercrime. Cambridge UK: Polity Press

Wall, D. S. (2013). Policing Identity Crimes. Policing and Society: An International Journal of Research and Policy, 23(4), 437-460.

Wilson, C. (2008). Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and policy issues for congress. https://fas.org/sgp/crs/terror/RL32114.pdf

Urbas, G. and Choo, K-K.R. (2008). Resources Materials on Technology-enabled Crime. Australian Institute of Criminology.

United Nations Office of Drugs and Crime (UNODC). (2013). Comprehensive Study on Cybercrime. New York: United Nations.

UNICEF, 2020, COVID-19 pandamic: countries urged to take stronger action to stop spread of harmful information. https://www.unicef.org/maldives/press-releases/covid-19-pandemic-countries-urged-take-stronger-action-stop-spread-harmful

Waheeda, F. (2018). Prosecuting Modern Identity theft: A Comparative Analysis. Contemporary and Emerging Issues in Syariah and Law, Uinversiti Sains Islam Malaysia (USIM) Press.

Wardle, C. & Derakhshan, H., Information disorder: toward an interdisciplinary framework for research and policy making. Council of Europe Report, 27 (2017). https://firstdraftnews.org/latest/coe-report/

Zalif, Z (2020a, March 9), Fight Against Misinformation is vital to combat COVID-19: WHO Maldives, *Raajje*. https://raajje.mv/72857

Zalif, Z (2020b, November 5). Enhancing response capacity of law enforcement agencies is pivotal to protect human rights: minister. *Raajje.* https://raajje.mv/89987