GSJ: Volume 11, Issue 3, March 2023, Online: ISSN 2320-9186
www.globalscientificjournal.com

INVESTIGATING THE IMPACT OF COVID-19 ON POST-PANDEMIC CYBERSECURITY AND CYBERCRIME

ABDUL RAUF

Department of Computer Science & Information Technology, Univerity of Engineering & Techology Peshawar, Pakistan
Email: rauf.tlha@gmail.com, mohammadnh93@gmail.com

ABSTRACT

The COVID-19 pandemic has had a significant effect on various aspects of life, including cybercrime. The pandemic has created an environment where cybercriminals can more easily carry out attacks, leading to an increase in both the frequency and variety of cyberattacks globally. This research aims to examine the impact of the pandemic on cybercrime worldwide by analyzing different types of cyberattacks. The focus will be on the evolution of these attacks from the initial outbreak of COVID-19 in China to current trends. Case studies will be used to illustrate how cybercriminals have taken advantage of significant events and government announcements to plan and execute their attacks. For example, the research may show how cybercriminals have exploited vaccine distribution announcements to launch phishing campaigns and how they have used fear of job loss to carry out ransomware attacks. The study's goals are to provide insight into how cybercriminals have exploited the pandemic and offer suggestions on how individuals and organizations can prevent and counter these attacks. Recommendations may include best practices for security measures such as multi-factor authentication, regular software updates, and employee cyber security training. The research may also offer tips for individuals to protect themselves from cybercrime, such as being cautious when clicking links or providing personal information online, especially during times of uncertainty and fear.

Keywords: Covid19 Pandemic, Cybercriminal Activities, Cybercrime legislation, Economic Consequences, Attack Timeline, Cyber Security, Intrusion Detection.

INTRODUCTION

Information is an asset to organizations and people have come to understand that information security risks can have a negative impact on their business, reputation, and relationships, resulting in financial losses in the commercial sector and potentially leading to legal issues. In 2019, a novel viral disease named Covid-19 was detected in humans and declared a global crisis by the World Health Organization (WHO) [1]. This pandemic led to mass quarantines in many countries around the world, starting from the city of Wuhan in China [2]. The pandemic has had a major impact on the lives of billions of people, causing financial downturns in many countries and changing the way people live their lives. Additionally, it has created secondary threats in the technology-driven society, leading to an increase in cyberattacks and cybercrime. Cybercrime is the biggest threat to the global economy, causing damage to business reputation, intellectual property, and resulting in data corruption and destruction.

The year 2020 to today is known as a billion dollars lost. It has been notified in 2020 that hackers have gained access to up to 4.6 million customers' personal data that include virtual card numbers as well. Russian Cyberattack in the same year on the government of the United State is one of the utmost disastrous data breaches (SolarWinds program including financial assets information, source code, and passwords) and invaded approximately 18,000 government and private networks[3]. In 2021 hacker did a ransomware attack on Florida-based software and demanded $70 million in bitcoin that have an adverse effect on business across five continents with the Russian hacking group tool Colonial Pipelines. In the year 2022 cybercriminals endanger the lives of people across the world the administers social security for Costa Rica was shut down and caused a state of emergency in the states. While another hacker breached Rockstars' internal slack channel and pilfered 90 videos of work-in-progress gameplay and hacked Uber (hacking email system, internal communication, code repositories, and cloud storage)[4], [5].

CLASSIFICATION OF CYBERCRIMINALS

The major reason for committing cybercrime is data breaching, monetary, personal motives, or any political and social crisis. It is classified under three heads deeding on the group that has been targeted for cyberattack. The following are mentioned as the classification categories:

1. Cybercrimes against individuals: These include ordinary individuals and the reason behind the cybercrimes are lack of information and cyber security. In a report generated by Norton about 44% of the individual consider themselves valuable targets for hackers. The cybercrimes that are mainly committed against individuals are: cyberbullying, cyberstalking, cyberdefamation, phishing, cyber fraud, cyber theft, and spyware.

2. Cybercrimes against organizations: It mainly targeted individuals to help the cybercriminals get a meager amount of ransom (depending upon the financial status of the organization). On the other

hand, extremely confidential data has been breached both public and private. It is generally launched on a larger scale and attacks a company's daily operations drastically. It includes attacks by viruses, salami attacks, web jacking, denial of service attacks, and data diddling.

3. Cybercrime against society: It also committed targeting the individuals in society and launched various cyberattacks against the community (particular section or entire country). It includes cyber pornography, cyber terrorism, and cyber espionage.

TIMELINE OF COVID-19 RELATED CYBERATTACKS

Cybercrime is technology-driven, which means directly related to technology and exploits it in its favor. Attackers took advantage of the unwary, panicked, scared people t to exploit them under various circumstances. In Covid19 pandemic, people were scared and depressed, and meanwhile, cybercriminals found it an opportunity to strike globally. Accordingly, a survey was conducted by IT professionals worldwide. It has been observed a drastic increase in cyberattacks in the area of data exfiltration and data leakage (unauthorized removal or transfer of data from a device). Half of the respondents were also affected by phishing emails [6]. A graphical representation is shown in Figure 1 with its percentage. The attacks include Data exfiltration and leakages, Phishing emails, account takeover, malware downloads, ransomware, and application-targeted attacks.

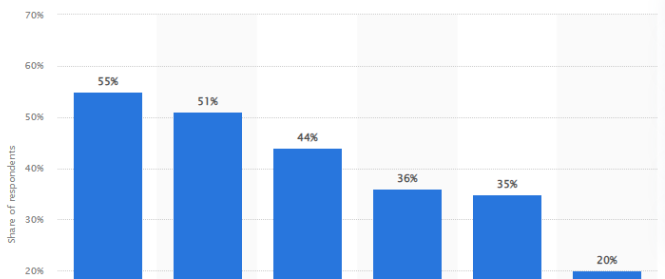


Figure 1: Comparative graph between Cyberattack and the respondents

In another survey [7] conducted by a Performance improvement partner to calculate the statistical data of the impact of cyberattacks globally during the pandemic situation shown in Figure 2, the United States declare that its first case of Covid-19 cyberattacks go up to 48% while in multiple states it is calculated as 64% and the world health organization reported that cyber-attack go up to 22% during the pandemic situation[7], [8].

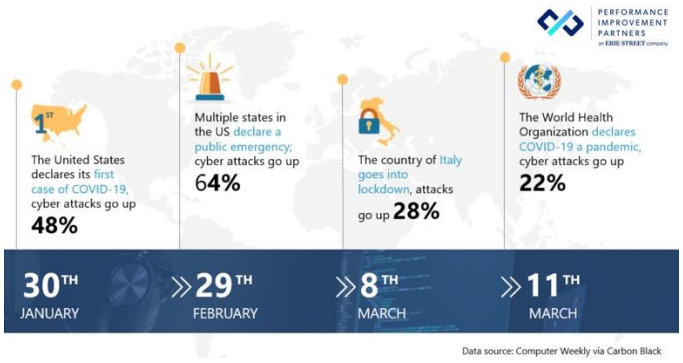


Figure 2: Cyberattacks globally during the pandemic situation declared by United States

SECURITY MEASURES OF ENCOUNTER

CYBERATTACKS

Multidimensional private and public collaborations are made between law enforcement agencies to tackle cybercrime effectively and the best way to go about it is by using Cross Domain solutions. It allows the organization to unify the system (hardware and software), and authenticates manual and automatic transfer of information access and different security classification levels. Following mentioned security measures are revealed to the user using a safe network and encounter cyberattacks:

1. **Use strong passwords:** One must maintain a different username and password combinations for every single account. Use strong passwords with a combination of letters, numbers, and characters to avoid brute force attack, etc.

2. **Protect data and online identity:** To protect data used encryption to the confidential and sensitive data and update regarding the fishing attacks to get rid of all the frauds. Moreover, identity protection must be ensured before making an online purchase, make sure the website is secure and authentic, and enable your privacy settings to avoid scams and fraud.

3. **Secure mobile device:** Avoid downloading malicious software to mobile devices and download applications from trusted sources. Update the operating systems, install anti-virus software, and use a lock screen to avoid access to your personal and financial information.

4. **Protect the computer with security software:** It includes firewall activation and antivirus programs to be installed on the computer, that monitor the data attempting to flow in and out over the internet and ensure safe communication, blocking bad traffic attacking the computer.

5. **Parental control and updating the computer with the latest patches:** Monitor the activities with parental control by keeping an eye on the browser history and the emails, enabling parental control in mobile apps and browsers from secured sites. In addition to it, to keep attackers away from computers patches must be applied and blocked the hacker to break into a system and take advantage of software flaws.

LITERATURE REVIEW

With the acceptance of digital technologies, many facets of society have moved online, ranging from shopping to social interactions then business, industry, etc. on the other hand the rate of crime increased statistically. The latest report established by Hiscox in 2019 [9] reported that cybercrime growing incidentally with a prediction to reach $6 trillion by 2021 according to the cybersecurity ventures[10]. As we know that cybercriminals can launch their attacks from any location across the globe due to their profitable nature and low-risk level that is why cybercrime is the adaptation of newbies.

Cybercrime is also known as a traditional crime, Cross and Shinder 2008 [11] describe cybercrime as a crime triangle, that specifies that cybercrime occurs due to three main factors. A victim, a motive, and an opportunity. The first factor known as a victim is the main target of the

attack while in paradox a motive is the aspect driving that drives criminals to commit attacks. The opportunity is a chance for the cyberattack to be committed, it can be an innate vulnerability in the system or any unprotected device. Other models for criminology are Routine Activity Theory and Fraud triangles use similar factors as in the previous model[12] to describe crimes [13]. Today's attacks have become more sophisticated and target specific (victims) entirely depending on the attacker's motivation mostly for financial gain, coercion, revenge, or reconnaissance. Dhanjani et al 2009 [14] define "opportunity attacks" as attacks that are major victims based on their vulnerability or use hooks to be attacked. The researcher elaborates on the meaning of hook as any mechanism used to mislead a victim into falling prey to an attack (take advantage of the distraction, time constraints, panic, or any other human factor). Nurse in 2019 and Wilson in 2011 [15] identifies these hooks and mentioned in their research study that victims are distracted by their interest and attention levels or when they are panicked. Correspondingly, time coerces puts victims under pressure that eventually leads to mistakes and increased likelihood to fall dupe to scams and attacks.

In the research study of Tysiac in 2018 [16], Opportunistic attackers seek to maximize their gain for that they wait for the best time to launch an attack based on the condition (natural disasters, ongoing political reforms, public events, and country crises are the perfect cases of the condition). A few examples are as mentioned: Natural disaster in 2005 named Hurricane Katrina caused massive destruction in the city of New Orleans and the surrounding areas in the USA, as mentioned in the report of FBL 2016 [17], After this natural disaster thousands of fraudulent websites appealing for philanthropical donations. In addition to that, the local citizen receives scam emails gaining access to personal information for possible payouts or government relief efforts. Similarly, scams and attacks have been witnessed in uncountable natural disasters since the earthquakes in Japan and Ecuador in 2016 reported by FTC [18], and bush fire in Australia in 2020 reported by Elsworthy. Likewise, on 25th June 2009, the tragic death of Michael Jackson dominated the news across the world, and scam emails were circulated online amongst the citizen after 8 hours of his demise with the details of the incident reported by Naked Security[19]. These spam emails contain links promising access to unpublished videos, pictures, or Jackson's merchandise that was linked to malicious websites and malware-infected attachments, more details are mentioned in the Hoffman research study in 2009 [20].

Research has revealed that large public events, such as the 2018 FIFA World Cup, attract a variety of cybercrime activities. A report by ESET noted instances of individuals being lured with false ticket giveaways and campaigns during the tournament. Another study conducted by Jannson in 2018 found that 164 million email addresses and passwords were compromised in a data breach at LinkedIn and subsequently offered for sale on the dark web. The data remained undisclosed for four years, which led to a plethora of opportunistic cyberattacks such as scams, blackmailing, phishing, and compromised accounts[21]. A study by Segura in 2017 highlighted that data breaches were utilized to send phishing links through private messages and InMail[22].

Global Threats during the Pandemic

In the year 2021[23], [24], adaptability and perseverance were the two main themes at the forefront. Organizations

adopted the emerging technology as a solution to overcome the challenges of the covid19 pandemic globally, showing resilience in the face of uncertainty. However, it led to software vulnerabilities that can be exploited by cyber adversaries. In 2021, the network of criminal enterprises focused to support Big Game Hunting (BGH) ransomware operations and this trend exemplifies by the eCrime ecosystem (threatened to shut down the operations) shifts observed in 2021. Despite efforts by law enforcement to seize ransom payments, a significant increase in ransomware-related data leaks (adversaries place on the victim data) were observed as compared to previous year. Additionally, targeted intrusion adversaries from countries such as Russia, China, Iran, and North Korea adapted to changing trends and events by employing new tactics, such as targeting IT and cloud service providers, weaponizing vulnerabilities, using ransomware for disruptive operations, and shifting to cryptocurrency-related entities.

CrowdStike intelligence premier two new adversaries: WOLF and OCELOT [25] for labeling the targeted intrusions originating from Turkey and Colombia, with its presence the offensive capabilities outside of government correlated with cyber operation enhanced (highlighted the variety of actor end goals). In the hacktivist landscape development of the grassroots operations and establishment of hacktivist groups (the Belarusian group cyber-Partisans since late 2020), expanded the diversification of the Iranian hacktivist (western political developments) ecosystem. This research report will encapsulate the entirety of analysis performed throughout 2021 that include the description of notable theme, trends, and cybersecurity. including descriptions of notable themes, trends and significant events in cybersecurity, this information empowers swift proactive countermeasures to defend valuable information, now and in the future.

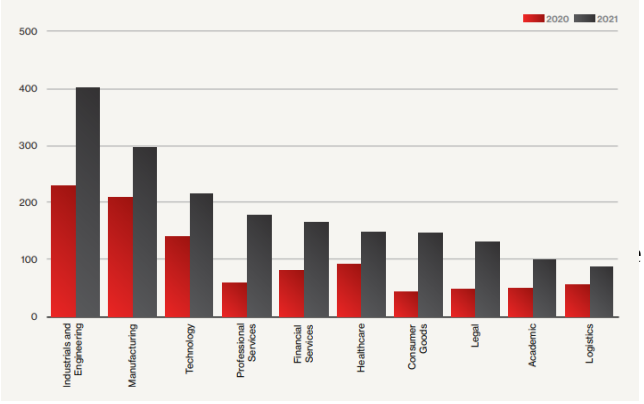
Our research report will also paint a picture to show the enterprise risk is coalescing some critical areas that are: cloud workloads, endpoints, identity and data. As we know that the threat actors continue to exploit application software vulnerabilities across endpoints and cloud environment. Moreover, ramping up the identities and stolen credentials bypassing the law enforcements. It has been observed in 2021 that up to 62% of the cyberattacks are malware free (e.g. hands on keyboard activities) and 32 % of the attacks are malware, the attackers increasingly attempting to accomplished their goals through an approach “living off the land” to evade detection by the antivirus products on their application software. Accordingly, to the Overwatch tracked report the increase number of intrusion campaigns were reported as compare to 2020[26][27]. The increase rate observed was near to 45% in such campaigns (categorize as unattributed). The Table 1 mentioned below analyze the types of threat activity in interactive intrusion campaigns for the period of 2020-2021.

Table 1: Threat Activity for the Period of 2020-2021 an Interactive Intrusion Campaigns

Type of Threat	Intrusions attribute	% in Year 2020	% in Year 2021
eCrime	Criminal intrusion activity committed for financial benefits.	52%	49%

Targeted	Targeted threat activity includes state-nexus destruction, cyber espionage and to generate currency to support administration.	13%	18%
Hacktivist	Hacktivist intrusion activities committed for visibility or to gain a momentum.	1%	1 %
Unattributed	To make a confident attribution against the insufficient data that is available.	34%	32%

Moreover, the impact of BGH in the year 2021 was palpable force felt across sectors worldwide with that the overall number of operating ransomware families increased as highlighted in the Figure 3 mentioned below how valuable victim data is to adversaries.



RESEARCH METHODOLOGY

Systematic Approach for Investigating the impact of pandemic

The systematic approach attempts to collect all practical incidents that fit against the research topic using obvious methods (standardized deviation) aimed at diminishing the bias and producing reliable findings for decision-making and awareness of the general public. It is a comprehensive and well-organized document [28], [29]. The cybercrime and cyberattack incidents erupting due to Covid19 pandemic pose serious threats step to the global economy of the worldwide population. Following mentioned are the steps used for conducting a systematic review of the research topic:

1. **Defining a problem statement:** Determining the problem statement with an explanation in research, identifying the effect of cybercriminals with the advancement and adaptation of technology. Moreover, we will investigate the effect of Covid19 on cyberattacks and cybercriminal activities with technology driven.

2. **Identify the scope of studies:** Identifying the research questionnaire addressing the thesis topic and narrowing down the scope of studies, using variety of online resources (journals, articles, conference proceedings, online relevant studies, books, advance search, and blogs).

3. **Searching, Collecting, and Refining Information:** In this step of the research study, we will look for the relevant research studies and evaluate, analyze, and synthesize it to identify the key findings that emerge. In this research, we will look for the precious cyber-

attacks and identify the reason behind each cybercriminal activity. Moreover, investigate the effect of it on the people, social and economic situation across the world.

4. **Processing, Comparing, and Presenting Information:** In this step critically evaluate and elaborate the information obtained through the previous step and compare it with the previous literature and then at last formulate a solution and present the information with the results and conclusion. Figure 4 mentioned below shows the steps required for the synthetic approach for investigating the impact of cybercriminal activities during the pandemic situation.

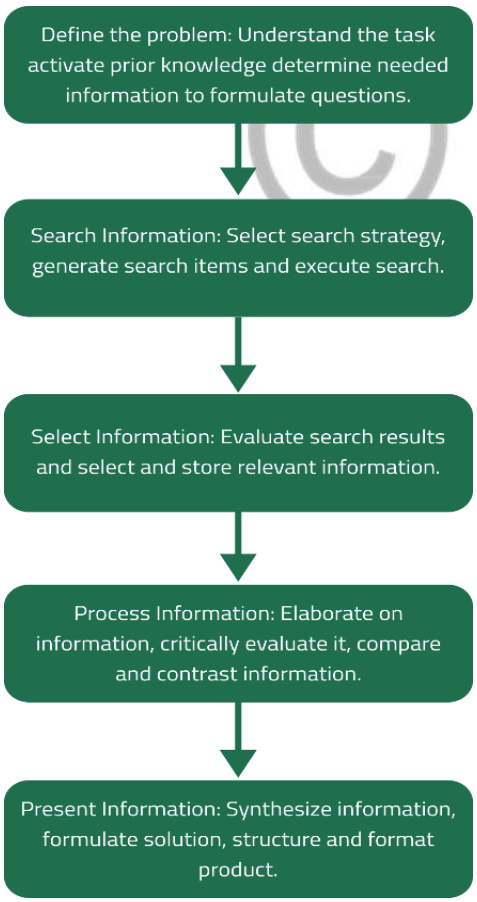


Figure 4: Steps of Systematic Approach for Investigating the Impact of Pandemic

RESULTS AND ANALYSIS

Result of Systematic Literature Review

We have discovered through our literature review and research methodology that a significant amount of research has been conducted in the areas of cybercrime, cyberattacks, and cyberthreats over the past few years and we examined that 161 research articles were found to be most closely related to our research study and objectives.

Research Paper Distribution

Total of 28623 research articles were in the first phase of information retrieval from six different databases and refined using the tollgate approach which includes five different phases to the refinement of research articles.
Figure 5 show the details of the refinement process using the tollgate approach.

Figure 5: Statistical Detail of the Refinement Process Using the Tollgate Approach

CONCLUSION

As technology advances and society adapts to it, the rate of cybercrime increases and impacts economic and societal circumstances, particularly during pandemics such as COVID-19. Our research over the past five years has

identified common patterns among many cybercrimes and cyber-attacks through systematic approach. It has been noted that the number of cyberattacks worldwide is on the rise each year and affecting individuals. The COVID-19 pandemic has had notable effects on cybercrime and cyberattacks, including an increase in phishing and social engineering tactics, a rise in ransomware attacks, an increase in attacks targeting remote workers, an uptick in supply chain attacks, and an increase in scams related to the pandemic. In summary, the COVID-19 pandemic has presented new opportunities for cybercriminals and has emphasized the requirement for advanced cybersecurity measures to combat cybercrime, particularly in a remote working scenario.

REFERENCES

[1] B. Pribadi, S. Rosdiana, and S. Arifin, "Digital forensics on facebook messenger application in an android smartphone based on NIST SP 800-101 R1 to reveal digital crime cases," Procedia Comput Sci, vol. 216, pp. 161–167, 2023, doi: 10.1016/j.procs.2022.12.123.

[2] K.-S. Choi, C. S. Lee, and E. R. Louderback, "Historical Evolutions of Cybercrime: From Computer Crime to Cybercrime," in The Palgrave Handbook of International Cybercrime and Cyberdeviance, Cham: Springer International Publishing, 2020, pp. 27–43. doi: 10.1007/978-3-319-78440-3_2.

[3] E. R. Leukfeldt, A. Lavorgna, and E. R. Kleemans, "Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime," Eur J Crim Pol Res, vol. 23, no. 3, pp. 287–300, Sep. 2017, doi: 10.1007/s10610-016-9332-z.

[4] M. Antonescu and R. Birău, "Financial and Non-financial Implications of Cybercrimes in Emerging Countries," Procedia Economics and Finance, vol. 32, pp. 618–621, 2015, doi: 10.1016/S2212-5671(15)01440-9.

[5] F. E. Eboibi, "A review of the legal and regulatory frameworks of Nigerian Cybercrimes Act 2015," Computer Law & Security Review, vol. 33, no. 5, pp. 700–717, Oct. 2017, doi: 10.1016/j.clsr.2017.03.020.

[6] L. Y. Connolly and D. S. Wall, "The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures," Comput Secur, vol. 87, p. 101568, Nov. 2019, doi: 10.1016/j.cose.2019.101568.

[7] K. M. Yilma, "Developments in cybercrime law and practice in Ethiopia," Computer Law & Security Review, vol. 30, no. 6, pp. 720–735, Dec. 2014, doi: 10.1016/j.clsr.2014.09.010.

[8] L. Tosoni, "Rethinking Privacy in the Council of Europe's Convention on Cybercrime," Computer Law & Security Review, vol. 34, no. 6, pp. 1197–1214, Dec. 2018, doi: 10.1016/j.clsr.2018.08.004. K. Elissa, "An Overview of Decision Theory," unpublished. (Unplublished manuscript)

[9] K. M. Yilma, "Ethiopia's new cybercrime legislation: Some reflections," Computer Law & Security Review, vol. 33, no. 2, pp. 250–255, Apr. 2017, doi: 10.1016/j.clsr.2016.11.016.

[10] M. Irfan, M. A. Ramdhani, W. Darmalaksana, A. Wahana, and R. G. Utomo, "Analyzes of cybercrime expansion in Indonesia and preventive actions," IOP Conf Ser Mater Sci Eng, vol. 434, p. 012257, Dec. 2018, doi: 10.1088/1757-899X/434/1/012257.

[11] G. Tsakalidis and K. Vergidis, "A Systematic Approach Toward Description and Classification of Cybercrime Incidents," IEEE Trans Syst Man Cybern Syst, vol. 49, no. 4, pp. 710–729, Apr. 2019, doi: 10.1109/TSMC.2017.2700495.

[12] G. Mui and J. Mailley, "A tale of two triangles: comparing the Fraud Triangle with criminology's Crime Triangle," Accounting Research Journal, vol. 28, no. 1, pp. 45–58, Jul. 2015, doi: 10.1108/ARJ-10-2014-0092.

[13] T. M. Maung and M. M. S. Thwin, "Proposed Effective Solution for Cybercrime Investigation in Myanmar," Int J Eng Sci (Ghaziabad), vol. 06, no. 01, pp. 01–07, Jan. 2017, doi: 10.9790/1813-0601030107.

[14] R. Leukfeldt, E. Kleemans, and W. Stol, "The Use of Online Crime Markets by Cybercriminal Networks: A View From Within," American Behavioral Scientist, vol. 61, no. 11, pp. 1387–1402, Oct. 2017, doi: 10.1177/0002764217734267.

[15] M. Bada and J. R. C. Nurse, "Profiling the Cybercriminal: A Systematic Review of Research," in 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Jun. 2021, pp. 1–8. doi: 10.1109/CyberSA52016.2021.9478246. C. J. Kaufman, Rocky Mountain Research Laboratories, Boulder, Colo., personal communication, 1992. (Personal communication)

[16] S. Kemp, D. Buil-Gil, A. Moneva, F. Miró-Llinares, and N. Díaz-Castaño, "Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19," J Contemp Crim Justice, vol. 37, no. 4, pp. 480–501, Nov. 2021, doi: 10.1177/10439862211027986.

[17] S. W. Brenner, "10. The Council of Europe's Convention on Cybercrime," in Cybercrime, New York University Press, 2020, pp. 207–220. doi: 10.18574/nyu/9780814739334.003.0012.

[18] P. Anesa, "Lovextortion: Persuasion strategies in romance cybercrime," Discourse, Context & Media, vol. 35, p. 100398, Jun. 2020, doi: 10.1016/j.dcm.2020.100398.

[19] S. Ibrahim, "Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals," Int J Law Crime Justice, vol. 47, pp. 44–57, Dec. 2016, doi: 10.1016/j.ijlcj.2016.07.002.

[20] F. Iqbal, B. C. M. Fung, M. Debbabi, R. Batool, and A. Marrington, "Wordnet-Based Criminal Networks Mining for Cybercrime Investigation," IEEE Access, vol. 7, pp. 22740–22755, 2019, doi: 10.1109/ACCESS.2019.2891694.

[21] A. M. Bossler and T. Berenblum, "Introduction: new directions in cybercrime research," J Crime Justice, vol. 42, no. 5, pp. 495–

499, Oct. 2019, doi: 10.1080/0735648X.2019.1692426.

[22] X. Li and Y. Qin, "Research on Criminal Jurisdiction of Computer cybercrime," Procedia Comput Sci, vol. 131, pp. 793–799, 2018, doi: 10.1016/j.procs.2018.04.263. S.P. Bingulac, "On the Compatibility of Adaptive Controllers," *Proc. Fourth Ann. Allerton Conf. Circuits and Systems Theory*, pp. 8-16, 1994. (Conference proceedings)

[23] C. Cheng, L. Chan, and C. Chau, "Individual differences in susceptibility to cybercrime victimization and its psychological aftermath," Comput Human Behav, vol. 108, p. 106311, Jul. 2020, doi: 10.1016/j.chb.2020.106311.

[24] V. L. Schul'tz, V. v. Kul'ba, A. B. Shelkov, and L. v. Bogatyryova, "Scenario Analysis of Improving the Effectiveness of Cybercrime Investigation Management Problems," IFAC-PapersOnLine, vol. 54, no. 13, pp. 155–160, 2021, doi: 10.1016/j.ifacol.2021.10.437.

[25] U. Jerome Orji, "An inquiry into the legal status of the ECOWAS cybercrime directive and the implications of its obligations for member states," Computer Law & Security Review, vol. 35, no. 6, p. 105330, Nov. 2019, doi: 10.1016/j.clsr.2019.06.001.

[26] T. J. Holt and B. Dupont, "Summarizing the special issue on the human factor in cybercrime," Comput Human Behav, vol. 138, p. 107411, Jan. 2023, doi: 10.1016/j.chb.2022.107411.

[27] Dr. C. le Nguyen and Dr. W. Golman, "Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action,'" Computer Law & Security Review, vol. 40, p. 105521, Apr. 2021, doi: 10.1016/j.clsr.2020.105521. J. Williams, "Narrow-Band Analyzer," PhD dissertation, Dept. of Electrical Eng., Harvard Univ., Cambridge, Mass., 1993. (Thesis or dissertation)

[28] J. S. Hiller and R. S. Russell, "The challenge and imperative of private sector cybersecurity: An international comparison," Computer Law & Security Review, vol. 29, no. 3, pp. 236–245, Jun. 2013, doi: 10.1016/j.clsr.2013.03.003.

[29] V. C. Strasburger, "School Daze," Pediatr Clin North Am, vol. 59, no. 3, pp. 705–715, Jun. 2012, doi: 10.1016/j.pcl.2012.03.026. E.E. Reber, R.L. Michell, and C.J. Carter, "Oxygen Absorption in the Earth's Atmosphere," Technical Report TR-0200 (420-46)-3, Aerospace Corp., Los Angeles, Calif., Nov. 1988. (Technical report with report number)