PHOTON
Journal of Natural Sciences and Technology
p-ISSN: 2087-393X | e-ISSN: 2579-5953
http://ejurnal.umri.ac.id/index.php/photon

Narrative Review: The Role of the COVID-19 Pandemic in the Rise of Cybercrime Worldwide

Nirwana Seftiani Pinem*

Master of Forensic Science, Graduate School, Airlangga University, Indonesia

Received 16 April 2024 | Accepted 24 May 2024 | Published 31 May 2024
DOI: https://doi.org/10.37859/jp.v14i2.7698

Keywords:
Covid-19;
Cybercrime;
World

Abstract. The high incidence of cybercrime during the COVID-19 pandemic in Indonesia underscores the need for a study on the role of the COVID-19 pandemic in the global increase of cybercrime. This research aims to understand the role of the COVID-19 pandemic in the rise of cybercrime worldwide. The study uses a narrative review method, involving the search for articles with similar or related topics to gather relevant data. The keywords used were: cybercrime, COVID-19, World. Articles were sourced from trusted websites, including Google.com, Google Scholar, and Semantic Scholar, with a publication date range from 2019 to 2024. The results indicate that COVID-19 had a positive impact on communication services, PC delivery, social media usage, online shopping, and accelerated the use of cash alternatives. However, it also had negative effects, such as extreme global poverty, financial difficulties, loss of income, increased depression among American teenagers living with their parents, and international cybercrime targeting vaccine research and development organizations.

*Corresponding author.
E-mail address: nirwana.seftiani.pinem-2022@pasca.unair.ac.id

1. Introduction

Cybercrime is a broad term used to describe criminal activities where computers or computer networks are the tools, targets, or venues for such activities. It encompasses everything from electronic hacking to denial-of-service attacks. It also includes traditional crimes where computers or networks are used to facilitate illegal activities. Cybercrime can disrupt railway systems, mislead aircraft by sending incorrect signals, cause important military data to fall into foreign hands, and can make electronic media and all other systems collapse in an instant (Das and Nayak, 2013). The rapid growth of Internet usage in Asia, including a tenfold or more increase in China, India, and other countries since 2002, has been accompanied by a significant rise in cybercrime. The development of commercially scaled exploit tools and criminal networks focused on monetizing malware has exacerbated the risk of cybercrime. Law

enforcement responses in Asia are briefly reviewed in the context of the Council of Europe's 2001 Cybercrime Convention (Budapest).

According to Mr. Bhakti Eko Nugraho, a criminology lecturer at the Faculty of Social and Political Sciences, University of Indonesia (FISIP UI), one of the most concerning crimes that has seen a significant rise due to the increasing scale of its execution is cybercrime. The incidence of cybercrime surged notably during the COVID-19 pandemic. Cybercrime encompasses all illegal activities conducted by offenders using information technology systems and computer networks to directly attack the victim's information technology systems. More broadly, cybercrime can be defined as any illegal act supported by computer technology. During the COVID-19 pandemic, criminals exploited the situation by soliciting donations under the pretense of pandemic victims. Offenders tended to steal victim data and even breach bank accounts. Additionally, the shift in lifestyle during the pandemic led to a greater reliance on the internet among Indonesians.

According to data from the Indonesian National Police, from April 2020 to July 2021, there were 937 reported cases. Among these, three types of cases had the highest numbers: provocative content, hate content, and hate speech, with approximately 473 cases reported. This was followed by online fraud with 259 cases and pornography with 82 cases. The high incidence of cybercrime during the COVID-19 pandemic in Indonesia underscores the need for a study on the impact of the pandemic on the rise of cybercrime globally. Based on this, the aim of this research is to understand the role of the COVID-19 pandemic in the increase of cybercrime worldwide.

2. The Methods

The method used in writing this narrative review involves searching for articles with the same or similar topics to obtain data relevant to the subject under discussion. The keywords used were: cybercrime, Covid-19, World. Articles were searched on trusted websites, including Google.com, Google Scholar, and Semantic Scholar, with a publication date restriction from 2019 to 2024, and inclusion and exclusion criteria were applied. All selected articles were read in detail to determine whether they were suitable to be used as primary data sources. Subsequently, data analysis was conducted on the articles obtained, and arguments/discussions were developed based on each data source. Additionally, the strengths and weaknesses of the articles were considered to consolidate the data into a unified analysis.

3. Result and Discussion

The COVID-19 pandemic has become a global disaster, rapidly spreading and causing both health and economic crises across various parts of the world. According to a report from the World Health Organization (WHO), as of November 14, 2020, the number of confirmed COVID-19 cases worldwide had reached 53,164,803. In response to the pandemic, governments in various countries, including Indonesia, implemented lockdown measures aimed at slowing the spread of the virus within their nations.

3.1 United Kingdom

The history of personal data protection policies in the United Kingdom and other European countries is long-standing. Privacy rights were first addressed in the Universal Declaration of Human Rights following World War II. Recognizing the importance of privacy protection, Germany introduced the Data Protection Act in 1970. This move was followed by the UK and other European countries such as Switzerland, Austria, Sweden, and France. In 1980, European countries within the Organization for Economic Co-Operation and Development (OECD) issued the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. These guidelines established international normative

principles for privacy data management, including limitations on data collection, data quality, purpose specification, data disclosure restrictions, security measures, transparency, individual participation, and accountability. In 1981, the Council of Europe Convention was established, requiring European countries to adhere to principles that ensure fundamental individual rights regarding data privacy, regulated by national legislation.

The Snowden case in 2013 triggered a response from various parties, leading to the adoption of UN Resolution 68/167 on the Right to Privacy in the Digital Age. This resolution heightened awareness about the threats of covert surveillance and illegal data collection through cyberattacks. Meanwhile, the International Covenant on Civil and Political Rights specifies that personal data collection and storage by any entity must be clearly regulated by law to ensure that individuals' data does not fall into the wrong hands. The Data Protection Act evolved significantly, culminating in 2016 with the simplification of all related processes into a single regulation, the European Union-General Data Protection Regulation (EU-GDPR). Effective from May 2018, this regulation has been adopted by over 125 countries worldwide as a model for their data protection laws.

Under the EU-GDPR, individuals have the right to know what information is held about them by governments and organizations, including how their data is used, accessing personal data, correcting inaccuracies, halting or limiting data processing, retrieving and reusing data files, and objecting to data processing. The Act mandates fair data processing and transparency regarding the collection and use of personal data. It even requires organizations to obtain user consent before placing cookies or similar technologies on their devices. The Act outlines seven data protection principles: (1) fairness, lawfulness, and transparency, (2) purpose limitation, (3) data minimization, (4) accuracy, (5) storage limitation, (6) data security, and (7) accountability. Despite these advanced regulations, the UK still faces data security threats. During the COVID-19 pandemic, cyberattacks in the UK increased, targeting critical infrastructure and online fraud through phishing in the healthcare sector. The National Cyber Security Centre (NCSC) reported that cybercriminals often impersonate official health institutions, creating fake websites to solicit passwords and personal data or demand bitcoin donations for fake vaccines.

European countries, including the UK, have independent nonprofit organizations called Information Sharing and Analysis Centers (ISACs). These organizations provide centralized resources for gathering information on cyber threats, especially regarding critical infrastructure, and facilitate two-way information sharing between the private sector and government. During the COVID-19 pandemic, the number of phishing-related fraud reports in the UK rose significantly. By early May, over 160,000 suspicious emails were reported to the NCSC, and by the end of May 2020, losses of £4.6 million were recorded due to COVID-19-related fraud involving 11,206 victims. In response, the NCSC removed 471 fake e-commerce sites and HMRC took down 292 fake sites.

To address the surge in cyberattacks, the UK government enhanced public awareness about online fraud and phishing. On April 8, 2020, the NCSC collaborated with the US Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) to release guidelines on cybercrime and advanced cyber threats during the pandemic, through announcements and public awareness campaigns.

3.2 Malaysia

Malaysia began addressing data protection regulations in 1998, with the Personal Data Protection Act (PDPA) being enacted in 2010. A Department of Data Protection was established under the Ministry of Information, Communication, and Culture to oversee PDPA implementation. The PDPA includes seven principles a general processing consent, collection and notification, usage and disclosure,. security, retention and right to block processing, data integrity, access and correction rights. In addition to the PDPA, Malaysia has legal provisions in the Criminal Code for data privacy violations. In 2017,

the Malaysian government established the National Cyber Security Agency (NCSA) to secure and enhance the nation's cyber resilience, including protecting against data security threats.

NCSA's scope involves implementing cybersecurity policies and protecting national critical infrastructure. Reports from NCSA during the COVID-19 pandemic showed an increase in fraud and malware using COVID-19 themes to deceive victims into disclosing personal information and installing malware. Besides NCSA, Malaysia has the National Cyber Coordination and Command Centre (NC4), a task force that includes NCSA and members managing cybersecurity in various sectors such as government, banking, and defense. During the pandemic, attackers exploited public health issues and COVID-19. The Advanced Persistent Threat (APT) Group, suspected of state support, engaged in cyber espionage and cybercrime. This group targets advanced countries, executing attacks like data theft, operational disruption, or infrastructure destruction over extended periods. The Malaysian Prime Minister has directed NC4, NCSA, and NSC to coordinate public awareness campaigns on cybersecurity, including guidelines for safe remote work practices.

3.3 Indonesia

During the COVID-19 pandemic, Indonesia lacked specific regulations for online data security. Data privacy policies were only addressed in Article 26 of Law No. 11 of 2008 on Electronic Information and Transactions, and its 2016 revision, which mandates personal data use with consent and allows for legal action if rights are violated. The proposed Personal Data Protection Bill for 2020 borrows principles from European privacy laws. The absence of specific legislation means data privacy is protected through various separate laws such as Banking Law, Telecommunications Law, Consumer Protection Law, Population Administration Law, Human Rights Law, Administrative Population Law, Information and Electronic Transactions Law (ITE), Public Information Openness Law, and Health Law. Supporting regulations include Government Regulation No. 71 of 2019 on Electronic Systems and Transactions and Ministerial Regulation No. 20 of 2016 on Personal Data Protection.

Criminal offenses related to data protection can be found in Article 30(2) of the ITE Law, which penalizes unauthorized access to electronic systems with up to seven years of imprisonment and/or a fine of up to Rp. 700,000,000. Other offenses are covered under the Criminal Code, including theft and aggravated theft, as well as in Population Administration Law Articles 94, 95a, 96, and 96a. Current data privacy laws are fragmented and overlapping, necessitating a more streamlined regulation, as proposed in the Personal Data Protection Bill. To combat rising cyberattacks, the Indonesian government issued

Presidential Regulation No. 53 of 2017 on the National Cyber and Encryption Agency (BSSN).

BSSN, formed from the merger of the National Encryption Agency and the Directorate General of Informatics Applications (Aptika) of the Ministry of Communication and Information Technology, is tasked with effective and efficient cybersecurity management. In response to increased cyber attacks during the pandemic, BSSN, the Ministry of Communication and Information Technology, the police, Bank Indonesia, the Financial Services Authority, and other entities collaborated on public awareness and education campaigns. These efforts included webinars and public service ads to raise awareness about common cyber threats and preventive measures during remote work. BSSN also provides guidance and support to companies across sectors for implementing cybersecurity standards based on national and international benchmarks.

3.4 European Union

Most healthcare systems in the EU suffer from inadequate budgets, outdated technology, and insufficient patches and configurations. The COVID-19 pandemic has highlighted these vulnerabilities, making systems more susceptible to exploitation by attackers. EU countries are required to comply with the General Data Protection Regulation (GDPR) to protect personal data. However, widespread

adoption is still lacking, with organizations struggling to manage the situation with limited resources and expertise. According to Yiva Johansson, European Commissioner for Home Affairs, while the pandemic has slowed many aspects of normal life, it has accelerated online criminal activities. These include ; Cross-cutting crimes such as phishing, online fraud, and the spread of false information about COVID-19 cures, Ransomware attacks targeting healthcare industries, threatening to auction stolen data and demanding ransom payments. Child sexual abuse, including recording and posting abuse and encouraging others to do the same. Payment fraud involving SIM swapping to hijack accounts. Criminal abuse of the dark web, focusing on selling illegal COVID-19 related items.

3.5 United States

The impact of COVID-19 on cybercrime includes; Malware embedded in fake global COVID-19 maps, pretending to be live updates from Johns Hopkins University. Phishing scams, such as fake emails and WhatsApp messages posing as WHO updates, fake food assistance coupons, or government demands for online COVID-19 tests. Ransomware in fake “contact tracing” apps, demanding bitcoin payments or locking phones and leaking personal information. Blackmail threats involving fabricated "dirty secrets" that could expose victims to COVID-19 if they do not pay immediately. Fake e-commerce sites posing as pharmacies selling non-existent COVID-19 treatments or unproven drugs. Zoombombing, with the intrusion of pornography, hate speech, and threats into virtual meetings.

3.6 Germany

On September 10, 2020, over 30 servers at Düsseldorf University Hospital were hit by a ransomware attack, disabling the hospital's systems and resulting in emergency patients being turned away. This was the first reported death due to a cyberattack. Hospitals are prime targets for cyber attacks because of their critical role in providing health services. The attack demonstrates the serious impact of cybercrime on healthcare operations. The pandemic has also led to an increased need for communication, online shopping, and digital currency usage, while economic and psychological challenges are rising globally.

3.7 Government actions against cyberattacks during the COVID-19 pandemic

- Formation of a coalition against COVID-19 cyber threats for sharing intelligence on threats.
- CTI League's collaboration between cybersecurity communities and law enforcement to protect first responders.
- The FBI in the US forming a COVID-19 Task Force to enhance investigations and responses to related crimes.
- Europol launching the European Financial and Economic Crime Centre (EFECC).
- Multilateral organizations like INTERPOL and the UN intensifying efforts to educate about COVID-19 cybercrime.

4. Conclusion

Since the pandemic, there has been a dramatic shift to routine activities in the virtual world, including working, shopping, entertainment, and visiting doctors, as well as an increase in cybercrime. This has made the COVID-19 pandemic a significant factor in the rise of cybercrime across various countries. Although some offenders engaged in similar activities before the pandemic, they have continued to evolve by leveraging the pandemic context and exploiting potential victims. The results indicate that COVID-19 had a positive impact on communication services, PC delivery, social media usage, online shopping, and accelerated the use of cash alternatives. However, it also had negative effects, such as extreme global poverty, financial difficulties, loss of income, increased depression among American

teenagers living with their parents, and international cybercrime targeting vaccine research and development organizations.

References

Broadhurts, R., dan Chang, L, Y, C. 2006. Handbook of Asian Criminology. Springer. 49-63

Coventry Lynne, Branley Dawn. Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas. 2018 Jul;113:48–52. doi: 10.1016/j.maturitas.2018.04.008.S0378-5122(18)30165-8

Das, S., dan Nayak, T. 2013. Impact of Cyber Crime : Issues and Challenges. International Journal of Engineering Sciennces & Emerging Technologies. India. 6(2). 142-153.

Eropol. 2020. Catching The Virus Cybercrime, Disinformation and The COVID-19 Pandemic. 1-14.

Ferreira A. GDPR: what's in a year (and a half)?. Proceedings of the 22nd International Conference on Enterprise Information Systems - Volume 2: ICEIS; 22nd International Conference on Enterprise Information Systems; May 5-7, 2020; Online. 2020. pp. 209–216.

Ferreira, A. dan Cruz-correia, R. 2021. COVID-19 and Cybersecurity: Finally, an Opportunity to Disrupt?. University of Porto. Portugal. 2(2).

Meiyanti, Ruci dan Ismaniah, I. 2015. Perkembangan Digital Forensik Saat ini dan Mendatang. Jurnal Karya Ilmiah. 15(2).

Nugroho, A. C. 2020. Serangan Ransomware di RS Jerman diduga Sebabkan Pasien Meninggal. Diakses tanggal 1 Oktober 2023. https://teknologi.bisnis.com/ read/20200919/84/1293855/serangan-ransomware-di-rs-jerman-diduga-sebabkan-pasien-meninggal.

Wahyudi, D dan Jodi, S. 2019. Perlindungan Data Pribadi: Pentingnya Otoritas Pengawasan Independen. Jakarta: Elsam.