https://africanjournalofbiomedicalresearch.com/index.php/AJBRr
Afr. J. Biomed. Res. Vol. 27 (September 2024); 09-12

Research Article

Cybercrime and Related Regulations: An Overview

Ahamd Khader Habboush[1], Zyad AlRabie[2], Ahmad Rasmi Ali Ayasrah[3], Mahmoud Ali Al Shugran[4], Binod Kumar Pattanayak[5*]

[1]Department of Computer Networks, Faculty of Computer Science and Information Technology, Jerash University, Jerash, Jordan*
[2]School of Business and Law, Jerash University, Jerash, Jordan
[3]Department of Cyber Security, Faculty of Computer Science and Information Technology, Jerash University, Jerash, Jordan
[4]Department of Computer Science, Faculty of Computer Science and Information Technology, Jerash University, Jerash, Jordan
[5]Department of Computer Science and Engineering, Institute of Technical Education and Research, Siksha 'O' Anusandhan Deemed to be University, Bhubaneswar, Odisha, India

ABSTRACT
Over the years, along with the popularity of global Internet as a widespread medium of communication, information security threats such as cybercrime has emerged as a global challenge for secure data communication. Prevention of such a global crime has become extremely difficult. However, numerous detection and protection strategies have been proposed. In addition, government agencies publish regulations to prevent such harmful activities to protect data security and privacy. In this paper, we discuss various cybercrime features along with their prevention strategies. We also discuss some regulations that can prevent malicious activities on the global Internet to ensure data security and privacy.

***Keywords*:** Iron oxide, Magnetic flocculation, nickel, oil refineries wastewa Component; Cybercrime, Cyber Criminals, Security, Regulations. ter.

Author for correspondence: Email:- ahmad_ram2001@jpu.edu.jo

Received: 12/06/2024, Accepted: 20/07/2024

DOI: https://doi.org/10.53555/AJBR.v27i2S.1561

INTRODUCTION

Emergence of Internet of Things (IoT) as a global communication medium has become extremely popular over the years. Unlikely the conventional Internet, IoT provides the facility of machine-to-machine (M2M) communication without any human intervention. A huge amount of data is being communicated over the Internet every day. However, security concerns of these data present a major challenge for the enterprises as well as individuals. Cybercrime elements are the main sources of such threats. Cybercrime can be defined as a crime committed on line using an electronic device whereas cybersecurity encompasses the methods to prevent such malicious activities on line [1]. Cybersecurity venture predicted that the cost resulting from cyber-crime online would touch USD 6 Trillion by the end of 2021. The consequences of cyber-crime attacks are data manipulation, hacking of information, breaking login credentials etc. The major areas that suffer from cyber-crime are the commercial enterprises and military services. The commercial enterprises can incur a huge financial loss whereas security breach in military service can very much bring harm to internal security of a nation. Straightforward prevention of cyber-crime is yet very difficult, but however, early detection and necessary protection from it is technologically possible. A wide spectrum of algorithms has

ben proposed by various researchers for this purpose. Mainly, machine learning and artificial intelligence-oriented tools are found to be significantly effective for protection from the cyber-crime attacks and provisioning of security for the data communicated on line. In addition, government agencies can publish stringent regulations for data communication which can result in early identification of the malicious elements on line and prevent them from accessing the on-line data.

Rest of the paper has been organized as follows. Section 2 covers the related work on cybercrime. Cybercrime as a phenomenon is covered in Section e. The nature of cybercrime is detailed in Section 4. Jordan Government's initiative to combat cybercrime has been covered in Section 5 and Section 6 concludes the paper.

Related Work

A wide range of articles have been published that cover the aspects of cyber-crime along with its prevention methods and related regulations. The impacts of cybercrime activities on businesses have been exclusively analysed by the authors in [2] where a focus has been made on the business laws and their implications are derived. A study on different types of cybercrime, the enterprises that would be affected by it, software tools used for early identification of cybercrime, detection of digital data sources, collecting evidences, preserving the integrity, searching for data that might result in a crime etc. are discussed in detail [3]. The crimes are investigated in conformance with the regulations and legislations. Development of information technology and subsequently development of cybercrime in Indonesia has been clearly described by the authors in [4] that relies on normative juridical using secondary data that consist of primary legal materials like the legislations related to cybercrime along with the examples of cybercrime in Indonesia. The contemporary advanced methods for fighting the cybercrime activities in the context of Kazakhstan has been detailed by the authors in [5] in accordance with the cybercrime regulations of Kazakhstan. An exclusive comparison between Criminal Law of Vietnam (CCV) with that of European Convention has been conducted by the authors in [6]. The findings of the investigation pointed out at the fact that although CCV included most of the crimes committed on line, it still lacked in the regulations against the crimes such as data interference, computer-based forgery, misuse of devices and child pornography. Financial cybercrime in the metaverse has been addressed by the authors in [7]. It has significantly affected the authorities, corporate sector as well as individuals. The authors recommend the procedures to fight such challenges. A refined and comprehensive taxonomy of cybercrime has been introduced by the authors in [8] that exclusively demonstrates its utility and widespread use. The authors also analyse the strategies used in Australia, Queensland and Abu Dhabi in order to fight cybercrime. A proper scrutiny and highlight of imminent needs for regulating cybercrime phenomena in accordance with the principles as applicable to international law has been addressed by the authors in [9]. The authors also address the subsequent consequences of cybercrime in order to establish a legal basis for its prevention and necessary punishments of cyber criminals. The necessity of law enforcement against cybercrime as claimed by the authors in [10], lies in appointment of qualified personnel who clearly understand cybercrime effects and their prevention as well as formation of stringent regulations to combat the occurrences of such acts. A comprehensive analysis of legal methods for protection of children from the consequences resulting from cybercrime in the context of Indonesia has been addressed by the authors in [11]. The authors claim that strengthening enforcement laws to protect children from cybercrime attacks is the need of the hour. A comprehensive review of literature in order to identify the challenges faced by fintech industry for combatting cybercrime along with the anticipatory solutions has been carried out by the authors in [12]. The security breaches in this case include information theft, intellectual property theft that may harm the reputation of an fintech industry. The authors here claim that a reliable cybersecurity framework to combat cybercrime would be very effective for the purpose. Comprehensive research on impacts of cybercrime activities in West Africa has been conducted by the author in [13] and the study reveals that at the micro level, a citizen faces financial loses and also loses the eligibility for international travel opportunities. I addition, at the mess level, e-businesses get victimized financially as well as reputational as a consequence of cybercrime. The authors in [14] discuss in detail the cyber law-making in the European Union EU). As claimed by the authors, EU brings out multiple mutual contradicting definitions of cybercrime between actors and the entities, also propose multiple approaches to cybersecurity. However, as per the authors, EU lacks competent agencies or institutions that can successfully implement cybersecurity. A review of law enforcement relating to cybercrime in Asia has been conducted by the authors in [15] thereby carrying out a comparison of cyber laws and regulations of various Asian countries keeping in view European Convention. A study on enacting regulations against cybercrime in Russian federation and development of Russian model for cyberspace has been conducted by the authors in [16]. Authors reveal that cybercrime in Russia not only affects Russia alone, but globally as well. Authors conclude that the hacking culture has emerged as the principal factor of emergence of cybercrime. A focus on different categories of cybercrime that are imposed on women, children and senior citizens has been made by the author in [17] thereby discussing various laws meant for protection of women, children and senior citizens from cybercrimes committed online. The strategy of eradication of cybercrime and criminalization of cybercrime as per Indonesian Law have been detailed in [18]. A study on investigation of factors that prohibit SMEs from recognizing and assessing losses incurred from cybercrime in South Africa [19]. For this purpose, the authors have surveyed 20 various business enterprises and conclude that the victimization emerging from cybercrimes results from unawareness of cyber-attacks lead the enterprises to be unable to recognize and assess the losses incurring from cybercrimes. A study on identification of related laws and regulations for governing the control and prevention cybercrimes relating to theft of related information related to acquisition of land and infrastructure in Indonesia [20]. In order to achieve this, the authors have conducted a survey by virtue of collection of information from various library resources, legal resources, case studies and informal discussions land officials in various regions of Indonesia. However, the authors make an observation that such crimes result from a nexus between the cyber criminals

and land officials. Globalization of cyber law to fight cybercrime worldwide has been addressed by the authors in [21]. The authors focus on a global fundament for creating cyber law to fight cybercrime thereby developing a collaboration between nations. Globalization of cyber law has also been discussed by the authors in [22]. The authors focus on protection of economic aspects from cybercrime. Artificial Intelligence (AI) and fifth generation (5G) network technology are being used by the South African banks for efficient financial operations. As claimed by the authors in [23], AI and 5G technology together are capable of combating cybercrime activities that may lead to financial losses, The Internet of Things (IoT) technology enables effective global communication between humans and machines with minimal human intervention. However, it faces significant challenges due to the vulnerability of small, wireless devices to cyberattacks. The proposed solution is to implement a comprehensive encryption system to protect these devices from such attacks[24].

Cybercrime as A Phenomenon

Salvador declaration 2012 states that "Development of Information, communications technology along with increased use of Internet will create a space for new possibilities for original criminals and new offenders to also contemporary switch from committing crimes in real world and virtual cyber world, cybercrime will be a growing, challenge for states, which shall be driven by underlying socio-economic factors as unique to any nation". With wide-spread use of Internet, huge amount of data is communicated over the Internet. With this, the risk on data privacy and integrity also increases significantly due to increasing cybercrime. The cyber criminals attack the government as well as private enterprises, banking sectors, children, senior citizens leading to financial losses, socio-economic hazards. This phenomenon can be tackled with a strong cyber law, preferably in global environment. The national governments must collaborate among themselves to come up with strong regulations along with stringent provisions of punishment for such activities.

Nature of Cybercrime

Cyber space is a virtual space where cybercrime occurs [24]. Taking into consideration general criminology, it can be concluded that cybercrime is a new, distinctive format of crime. Cybercrimes are categorized to two types such as (1) cyber space dependent; and (2) cyber space enabled. Cyber space dependent cybercrimes are committed with government agencies, financial institutions, corporate databases personal information etc. Whereas cyber enabled crimes are committed with women, children like pornography, cyber bullying, stalking, online frauds etc. Researches reveal that cybercrime perpetrators have different motives as compared to traditional offenders. A cybercrime perpetrator needs to learn operating with a computer and acquire knowledge of software as well as knowledge of Internet. Mostly, marginalised groups of people are targeted by the cyber criminals.

Initiative to Fight Cybercrime in Jordan's and other Arabic Country Perspective

Law No.17 related to cybercrime was ratified on 12th August 2023. The key points of this newly introduced law are detailed below.

1) **Gaining unauthorized access**: A person who commits the crime of unauthorized access to any information network/system would be punished with an imprisonment of one week to three months or a fine of 300 to 600 JOD (approximately USD 423 to 846) or both penalties being imposed;
2) Creating a false social media account: A person creating a false email account, web page or a social media account would be subject to a punishment of 1500 to 15000 JOD (approximately USD 2116 to 21157) or an imprisonment of minimum of three months or both penalties being enforced;
3) **Hacking information**: If a person hacks information from the website of a government agency, then the punishment for such an act is an imprisonment of five years with hard labour or a fine of 15000 to 45000 JOD (approximately USD 21157 to 63470) or both penalties being imposed;
4) **Using unauthorized means of online payment**: A person would be subject to an imprisonment of one to three years or a fine of 3000 to 6000 JOD (approximately USD 4231 to 8463) for using unauthorized electronics means of online payment such as false and invalid credit cards;
5) **Using an information network to publish pornographic materials**: A person who is involved in creating, publishing and promoting pornographic materials online, can new subject to imprisonment of less than six months or a fine of 3000 to 6000 JOD (approximately USD 4321 to 8463);
6) Disseminating false news and hate speech and insulting religious beliefs: A person using an information network or social media account disseminates false information thereby targeting national security can be subject to imprisonment of less than three months or a fine of 5000 to 20000 JOD (approximately USD 7052 to 28209) or both penalties being imposed.

Conclusion and Future work

Cybercrime has emerged as a major challenge to protect data security and privacy. In this paper, we have attempted to conduct an overview of cybercrime and related regulations comprehensively. The nature of cybercrime has been discussed in detail. We have also detailed the Government of India's initiative to fight cybercrime as a phenomenon. More and more studies need to be conducted on regulations of different nations to combat cybercrime and formulate a common regulation.

REFERENCES

Abubakari Y., The Reasons, Impacts and Limitations of Cybercrime Policies in Anglophone West Africa: A review, Social Space, Vol.21, No.1, pp.137-158, 2021.

Adinegoro R. and Santiago F., Management of Cybercrime Crimes in Indonesia Viewing from Criminal Law Political Perspective, Proceedings of Multidisciplinary International Conference (MIC), pp.1-9, 2022.

Ahamd Khader Habboush, Bassam Mohammad Elzaghmouri, Binod Kumar Pattanayak , Saumendra Pattnaik, Rami Ahmad Haboush, An End-to-End Security Scheme for Protection from

Cyber Attacks on Internet of Things (IoT) Environment, Journal Tikrit Journal of Engineering Sciences, Vol.30, No.4.

Alkaabi A., Mohay G., McCullagh A. and Chantler N., Dealing with problem of Cybercrime, Social Informatics and Telecommunications Engineering, LNICST, Vol.53, pp.1-18, 2011.

Anggono A., Tarjo and Riskiyadi M., Cybercrime and Cybersecurity at Fintech: A Systematic Literature Review, Jurnal Manajemen dan Oranisasi, Vol.12, No.3, pp.239-251, 2021.

Bawomo B. T., Reformation of Law Enforcement of Cyber Crime in Indonesia, Journal Pembaharaum Hukum, Vol.6, No. pp.332-349, 2019.

Bougaardt G. and Kyobe M., Investing the Factors Inhibiting SMEs from Recognizing and Measuring Losses from Cyber Crime in South Africa, Electronic Journal Information Systems Evaluation, Vol.14, No.2, pp.157-178, 2011.

Boussi G. O. and Gupta H., A Proposed Framework for Controlling Cyber-crime, Proceedings of the 2020 8th International Conference on Reliability, Infocom technologies and Optimization, 2020.

Broadhurst R. and Chang Y., Cybercrime in Asia: trends and Challenges, Asian Handbook of Criminology, pp.1-26, 2013.

Bucaj E., The Need for Regulation of Cyber Terrorism Phenomena in Line with Principles of International Criminal Law, Juridica, AUDJ, Vol.13, No.1, pp.141-162, 2017.

Chitimira H. and Ncube P., The Regulation and Use of Artificial Intelligence and 5G Technology to Combat Cybercrime and Financial Crime in South African Banks, Potcheftroom Electronic Law Journal, Vol.24, pp.1-33, 2021.

Dremliuga R., Dremliuga O. and Kuznetsov P., Combating the Threats of Cybercrimes in Russia, Communist and Post-communist Studies, Vol.53, No.3, pp.123-136, 2020.

Fahey E., Developing EU cybercrime and cybersecurity On legal challenges of EU institutionalisation of cyber law-making. In: Hoerber, T., Weber, G. & Cabras, I. (Eds.), The Routledge Handbook of European Integrations. (pp. 270-284). Abingdon, UK: Routledge. ISBN 9780367203078, 2022.

Hasbullah M. A, Identifying the Effects of Cybercrime on Business Laws: Implications for Businesses and Consumers, International Journal of Cyber Criminology, Vol.16, No.2, pp.119-130, 2022.

Iqbal M. and Jaya N. S. P., Development of Cyber Crime and Its Regulations in Indonesia, International Journal of Social Science and Human Research, Vol.4, No.2, pp.141-147, 2021.

Jeronimo A., The Globalization Effect of Law and Economic on Cybercrime, Journal Pembaharuan Hukum, Vol.6, No.3, 2019.

Katterbauer K., Syed H. and Cleenewerck L., Financial Cybercrime in the Islamic Finance Metaverse, Journal of Metaverse, Vol.2, No.2, pp.56-61, 2022.

Luong H. T. and Phan H. D., Cybercrime in Legislative Perspectives: A Comparative Analysis between the Budapest Convention and Vietnam Regulation, International Journal of Advanced Research in Computer Science, Vol.10, No.3, pp.1-3, 2019.

Mishra S., Cyber Crime in India with Special reference to Women, Children and Senior Citizens, Cyber Law Reporter, Vol.1, No.1, pp.45-63, 2022.

Murashbekov O. B., Methods for Cybercrime Fighting Improvement in Developed Countries, Journal of Internet Banking and Commerce, Vol.20, No.S1, pp.1-10, 2015.

Musofiana I., Sudarmaji A. and Maerani I. A., Aspects of Legal Protection of Children from Cybercrime, Journal Pembaharuan Hukum, Vol.7, No.3, pp.201-210, 2020.

Okutan A. and Cebi P. D. Y., A framework for Cybercrime Investigation, Procedia Computer Science, Vol.158, pp.287-294, 2019.

Siregar G. T. P. and Sinaga S., The Law Globalization in Cybercrime Prevention, International Journal of Law Reconstruction, Vol.5, No.2, pp.211-227, 2021.

Suhendi D. and Asmadi E., Cyber Laws Related to Prevention of Theft of Information Relayed to Acquisition of Land Infrastructure Resources in Indonesia, International Journal of Cyber Criminology, Vol.15, No.2, pp.135-143, 2021.