Global Journal of Politics and Law Research
Vol.12, No.1, pp.78-88, 2024
ISSN: ISSN 2053-6321(Print),
ISSN: ISSN 2053-6593(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Confronting Cybercrimes Under the Provisions of Public International Law

Heba Jawdat Almuhaisen

doi: https://doi.org/10.37745/gjplr.2013/vol12n17888 Published February,13 2024

Citation: Almuhaisen H.J. (2024) Confronting Cybercrimes Under the Provisions of Public International Law, *Global Journal of Politics and Law Research*, Vol.12, No.1, pp.78-88

ABSTRACT: *This study emphasizes the urgent necessity for constant updates and improvements to the international legal instruments so that they can cope up with the sophisticated and dynamic nature of the cyber threats. A major emphasis is given to the importance of the international cooperation and the harmonizing of the law enforcement practices across the world by under- standing the fact that the cybercrime has the transnational character and would be ineffective if competed by a nation in isolation. This study mentioned the ethical issues and the privacy concern when cyber law enforcement is being mentioned. It emphasizes on the need for bal- ancing the security measures and the protection of rights of individuals and their privacy as a huge concern and the approach for the authorities on the gathering data of individual to the organization recommended to be balanced. It recommended on the legal framework which are transparent, clear and proportionate with the surveillances and the data gathering, the framework can also imply with the oversight to prevent any abusive and malicious use of the approval and data gathering. Looking forward, the future for the international law that com- bats the crime such as the cybercrime in the cyberspace is yet and will continuously evolve, as the threat evolving, the legal response and the mechanism of the cooperation will need to remain in place. The paper also restated that the adaptability and the ethical consideration and the cooperation by the international community are the spectrum of the way to ensure the legal strategies to protect the cyberspace and the rule of law and human rights in digital age.*

KEYWORDS: cybercrimes, provisions, public, international, law

INTRODUCTION

An issue that denizens of Earth universally recognize and cannot avoid the existence of is in- formation security [1]. I would venture to say that the most rapidly expanding way to commit Continental, Quasi-International, and International crimes is in the arena of cybercrime [2]. How- ever, the tools for investigating and prosecuting these cyber-related offenses are predominantly national, leading to significant challenges [3].

Cybercrimes present numerous obstacles for conventional criminal law and the broader criminal justice framework [4]. The term 'cybercrime' encompasses a broad spectrum of illegal activities [5]. These include crimes against the confidentiality, integrity, and availability of data and computer systems, computer-centric offenses, and content-based crimes such as child exploitation material and acts of racism and xenophobia, as well as copyright infringement [6]. Another key issue is the complexity and novelty of Information and Communication

Technology (ICT) to those in the traditional criminal justice system [7]. Addressing crimes that involve these technologies requires personnel who are highly skilled in investigation, prosecution, and judicial processes [8]. The technological and computer literacy required for this is often unfamiliar to those in law enforcement and legal professions [9].

A third significant challenge in addressing cybercrimes is related to issues of sovereignty, as these crimes occur in a virtual space [10]. The unique and global nature of cybercrimes leads to inconsistencies between different criminal justice systems, which poses a major obstacle in effec- tively combating these crimes [11]. The surge in global connectivity has coincided with significant economic and demographic shifts in many countries, leading to increased income inequality, con- strained private sector expenditure, and diminished financial liquidity. Concurrently, the perpetra- tion of cybercrimes has become less reliant on sophisticated skills or methods [12]. Particularly in developing countries, there's a growing trend among young men, often starting in their late teens,engaging in computer-based financial fraud. It's estimated that over 80% of cybercrimes stem from some form of organized activity, frequently with an international aspect [13]. This involves a cycle of malware creation, computer infection, botnet management, harvesting personal and financial data, selling this data, and ultimately profiting from stolen financial information.

In contrast to traditional crimes, laws targeting cybercrimes require more sophisticated inves- tigative measures, rules concerning jurisdiction and electronic evidence, underscoring the need for international collaboration [14]. A cybercrime offense often acquires a transnational dimension when an element or significant effect of the offense occurs in a different territory, or if part of the crime's execution involves another territory [15].

The World Internet Conference (WIC) stands as one of the most influential and anticipated yearly events in the realm of cyberspace, given its scale and the pertinence of topics discussed. Its fourth edition in Wuzhen, themed "Developing Digital Economy for Openness and Shared Benefits — Building a Community of Common Future in Cyberspace," offers a prime opportunity to deliberate on enhancing international cooperation to combat cybercrimes effectively. Ensuring cyber security is crucial for realizing the full potential of a global digital economy that is equitable and transparent in resource sharing.

Cybercrime crimes

The integration of information technology, media, and communication is bringing about significant changes in both society and technology [16]. These developments, especially in the realm of com- puters, are profoundly shaping how the world interacts. Computers, now accessible to everyone from children to the elderly, offer considerable benefits in terms of efficiency and time-saving in various tasks.With these technological advancements, a new legal framework, known as cyber law, has emerged. Cyber law, a term combining 'cyber' and 'law,' primarily addresses the increasing issue of cybercrime [17]. Cybercrime poses a serious threat to societies and local communities, significantly influenced by the rapid advancement of the internet [18]. This progression has dual impacts: while it facilitates communication and is essential for many aspects of modern life, including work, it also introduces substantial risks, particularly concerning privacy and security [19].

The internet's capability to breach personal and institutional privacy by exposing personal identities can lead to more severe problems [20]. As a result, cybercrime is a growing concern both nationally and internationally, challenging to manage due to its transnational nature [21]. This issue is not confined to any single country and can affect economic, social, and cultural sectors globally. The erosion of physical boundaries in the digital world alters many aspects of daily life, where the rapid changes brought by the internet can also foster negative outcomes, notably cybercrime. Hackers, often the perpetrators of these crimes, exploit computer and internet technologies, some- times distributing harmful links that can lead to further cybercrimes [22].

This evolving landscape presents researchers with a unique opportunity to explore the complexities of cybercrime, investigating its origins, impacts, and potential solutions in an increasingly connected world [23].
Cybercrime encompasses various modes of operation, each with its distinct characteristics and implications:

- **Illegal Contents:** This mode involves hackers uploading or inserting data that is false or misleading, commonly known as a hoax [24]. For instance, they might post news articles that reference real events but contain entirely fabricated information. The content of these articles does not align with the actual facts of the events they purport to describe.
- **Data Forgery:** This form of cybercrime involves the falsification of data. Hackers often use this technique to upload misleading or harmful information to dangerous websites, frequently employing other people's data without their consent. This practice not only misrepresents information but also poses serious risks to individuals whose data is misused.
- **Cyber Espionage:** This involves spying activities conducted over the internet. Hackers gain unauthorized access to other devices or computer networks to extract sensitive information. This type of crime is prevalent in scenarios like business competition, where crucial data is stored on a particular group's computers.
- **Infringements of Privacy:** This crime targets the private and confidential data of individuals. Hackers illegally obtain and trade personal information to unscrupulous parties, causing harm to the victims whose privacy has been breached. The secretive nature of this crime makes it particularly invasive and damaging.

The challenge in combating these cybercrimes lies in the ever-evolving nature of computer tech- nology, internet networks, gadgets, and other telecommunication tools [25]. As these technologies advance rapidly, so do the methods and sophistication of cybercriminals, making it increasingly difficult to address these issues both nationally and internationally.

Cybercriminals, commonly referred to as hackers, typically utilize various devices and tools available on the internet and computers to conduct their activities. They often develop and execute programs to infiltrate other people's computer systems [26]. The primary targets and objectives of hackers generally include:

1. **Credit Card Database:** Hackers aim to access databases containing credit card information for fraudulent purposes.

2. **Bank Account Database:** They target databases holding bank account details to illicitly transfer or steal funds.
3. **Customer Information Database:** Accessing databases with customer information can lead to identity theft and other forms of fraud.
4. **Transactions with Falsified Credit Cards:** Hackers engage in transactions using stolen or counterfeit credit card details.
5. **System Disruption:** Often, hackers disrupt systems due to competitive reasons between companies, or for other motives. For example, a newly inaugurated company might be targeted by hackers employed by its competitors to disrupt its operations or steal sensitive data.

Hackers are sometimes insiders, like long-time employees, who are hired by companies to engage in cybercrimes against competitors. These actions have a detrimental impact on the affected individuals and businesses. According to a report by CNBC Indonesia, the annual income for hackers can reach significant amounts, making hacking an attractive field for some. This has led to a growing interest in hacking, often starting from activities like online gaming or through specialized courses.

The IT sector is increasingly sought after, with high-paying roles like data scientists, web developers, information security analysts, and software development engineers. However, there's a risk that IT professionals may misuse their skills for illicit activities, contributing to the types of cybercrimes discussed.

Cybercrime is highly detrimental and poses significant threats to internet users, affecting their privacy and security. Each country's government should deal with this problem properly with the use of fines for cybercriminals and making strong regulation. It's a lot more complex to get enforcement. Since, all the crime doesn't happen in the same country. Criminals might be from different country, hence same law count enforcement are not there in every country. So international understanding and goodwill is needed to combat this type of crime. The police legal system for every country would be different, international coordination and diplomatic agreement are must to intensify measure to combat cybercriminal similar activities.

Challenges in International Law

Many international legal frameworks have outlined solutions for cybercrime and the jurisdiction that applies to it are contemplated in a number of the key international legal framework elements. For instance:

- **The Budapest Convention on Cybercrime (2001):** Was adopted by the Council of Europe on November 23, 2001, and primarily deals with the issue of jurisdiction in cybercrime matters. It is widely recognized for its comprehensive approach to these issues.
-
- **Additional Protocol to the Budapest Convention (2003):** Adopted in Strasbourg on January 28, 2003 (ETS No. 189, Article 4.1), this protocol extends the convention's scope to include criminal acts of a racist and xenophobic nature committed via computer systems.
- **Arab Convention on Combating Information Technology Offences (2001):** Signed in Cairo on December 21, 2001 (Article 30.1(a)), this convention focuses on jurisdictional aspects related to information technology offenses in the Arab region.

A common element across these conventions is the adoption of the territorial principle as the primary rule for establishing jurisdiction. Our study particularly focuses on the Budapest Convention on Cybercrime due to its significance and the involvement of Hungary. As of September 2020, 65 countries, including Hungary, had ratified the convention.

The jurisdictional provisions of the Budapest Convention are outlined in Article 22 of Section 3. This article allows states to exercise jurisdiction over offenses committed within their territory, on vessels bearing their flag, on aircraft registered under their laws, or by their nationals. Signatory states may express reservations or stipulations regarding the convention's regulations.

The convention also addresses jurisdictional conflicts. In cases where multiple parties claim jurisdiction over an offense under the convention, the involved parties are encouraged to consult and determine the most appropriate jurisdiction for prosecution.

Extradition is a crucial aspect linked to jurisdiction and is governed by the convention. [27] In the realm of international law regarding cybercrime, the provisions for extradition are critical [28]. According to the Budapest Cybercrime Convention, extradition requests can be denied if they don't align with the national law of the requested country or the relevant extradition treaties. Specifically, if extradition for an offense under the convention is refused solely due to the nationality of the person sought, or because the requested state believes it has jurisdiction over the offense, the requested state is obligated to prosecute the case domestically upon the requesting state's demand and report the results back.

Similarly, the United Nations Convention against Transnational Organized Crime, particularly Article 15, Point 5, mandates that when multiple States Parties are investigating the same conduct, their competent authorities should consult each other to coordinate their actions.

The Budapest Cybercrime Convention plays a vital role in establishing a cooperative frame- work for states dealing with cybercrime [29]. However, from our perspective, there's a need for updating the convention's regulations. While it addresses many issues, it doesn't fully resolve sev- eral problems that arise outside the territorial principle. Consultation between states is essential, but it doesn't always provide clear answers or guidelines for specific issues. To date, international law hasn't established a hierarchy among jurisdictional principles. As cybercrimes become more common, the slow and often ineffective consultation processes may not be adequate in combating these crimes. There is lurking concern that these bargains are often unfruitful, possibly making it more difficult to address the myriad facets of cybercrime in an efficacious manner.

Technological Evolution and Legal Responses

The dynamics of technology and its rapid change often challenge existing legal frameworks, espe- cially in relation to cybercrime [30]. In many cases, the development of the law lags behind the development of technology and this means that little time is given to consider matters such as cy- bercrime since it may have just sprung up. In this case, the traditional laws, which were developed for an era when technology was less connected and much simpler, may

cause the traditional legal approaches to be irrelevant in dealing with crimes that exist in the digital world. As a result, there may be a great enforcement and prosecutorial gap, limiting the scope that one can exercise the law in relation to the crimes.

International law plays a key role in the dynamic world, as it must satisfy an exigent task to rise in the face of continuous technological changes and continue to be relevant, as the regulation, principles, and standard which are held important within the legal field needs to be realigned to the digital environment in which we currently find ourselves. As such we now require to predict what current technology there is and what future technologies there will be in place to identify any potential issue, and act on it in legal terms, thus using what may be called a proactive approach rather than reactive.

One of the most impactful breakthroughs in the field is the integration of digital forensics in law enforcement. An essential portion of solving cybercrimes, digital forensics employs ground
breaking technology to uncover, identify, and bring about justice to electronic fraudsters. The work in digital forensics has been used to trace and tag cyber attackers to tracking down digital footprints of online abductors.

In the case of cybercrimes, it has been recognized by the legal international community that global cooperation is needed to help solve these crimes because many times they occur outside the borders of one specific country. Examples of this include global data sharing agreements, international cybercrime task forces, and cooperative legal frameworks that have been created to assist in the prevention and prosecution of cybercriminals. This has occurred because the legal systems between country's that would have never collaborated before have been given a common goal to protect individual citizens from global cyber threats.

Other exceptional cases of effective integration between technology and law enforcement have also arisen from countries on a national level. For example, some nations have setup a specific cybercrime units within the law enforcement itself, with leading, well equipped technology to tackle complex cyber investigations coupled with experience police personnel. Also, some countries have formulated cybercrime legislations to criminalize certain perpetrated acts like identity theft, data loss, and online swindling in order to abridge the formality of prosecution in such offences.

Summarizing, it's terribly important that as the digital world and online technology continues to morph, legal frameworks do as well. As the technological world and the legal world start to merge, it will be necessary that the legal world to keep up with the constant changes of the rapidly evolving technology. By doing so, it will keep the world a lot safer and a lot more legal on the internet by keeping up with law infringements.

Proposals for Strengthening International Law

In an effort to strengthen the international law response to the growing number of cyber attacks, it is necessary to adopt a multi-pronged approach involving the amending of existing laws, the intro- duction of new provisions and a further commitment to international cooperation. One important point to make is the need to regularly review and

make relevant adjustments to international legal instruments in order to keep up with the fast-changing technological advancements. An effective response to cyber crime will require the co-operation of a wide range of agency types at a global level. Laws may need to be introduced or tightened to enable agencies and individuals to be able to deal with offences committed by rape of the internet which will mean changing some definitions perhaps to recognise these new types of offences. Rules on jurisdiction are likely to need to be amended to ensure a more effective approach to cross-border crimes occurs. Guidance on data protection and privacy in the cyber age need to be clearer but this must be a moving feast to take account of new technologies that will rear their head in the coming years [31].

Another crucial point is international collaboration. There's a need to strengthen partner-ships across nations that will enable member countries to share better information, expertise, and resources; and together pool ideas, knowledge, and resources in the fight against cybercriminals [12]. ways to improve that are: establish common protocols for digital forensic investigation across borders, improve the process of extradition, and harmonize the legislation on cybercrimes. Joint cybercrime task forces (JCTFs) and international conventions are ways to boost international col- laboration [31].

National governments and international bodies play a huge role because national governments should adopt and implement international agreements to assist in the fight against cybercrime and ensure that domestic laws are compatible with the obligations flowing from such agreements. Should also invest in building the necessary technological infrastructure and in capacity-building amongst criminal justice actors in relation to cybercrime investigation, due process, and prosecu- tion.

The international organisations could take a lead and be the initiator to harmonize the multi-lateral co-operations by organizing the platforms for discussion, negotiation and conciliation amongst state parties, taking a common stand to combat cybercrime. Furthermore, international organiza- tions could also offer technical assistance, training, equipment and information to any party with the weak penal infrastructure or without well-sophisticated digital devices or tools.

Additionally, there is an increasing requirement for public-private partnership endeavors to match the ever-growing complex cyber field. By working with technology companies and specialists in cyber security, governments can use their knowledge and experience to form more effective laws and strategies, prepare against and respond to threats faster and hence bounce back better from any fallout.

To emphasize, enhancing international law aimed at cutting down on cybercrime necessitates a multi-pronged approach that factors in amendments to laws, cooperation among countries, buy-in from national governments and international organizations, in addition, to useful private sector partners. All these will mean a more effective and the most up-to-date battle plan for the dynamic nature of cybercrime.

Ethical and Privacy Considerations

When it comes to cyber crime you find a lot of mixed emotions in the whole scene, when you look at things in view of the law enforcement I find people think we should have more leway and be able to search or do what we need to do to search and stop these untraceable crimes, but on the other hand what about your personnal rights a ordinary person has the right not to have someone watching there every move, and collect data from there computer or anything else electronical with out a cause [32]. The topic raises important questions in ethics, namely, how can a balance be struck between the need for privacy and the successful enforcement of the criminal law, particularly in the context of international cyber law enforcement where there is a diverse range of legal and cultural norms? The nature of the internet as a global phenomenon and the jurisdictional problems this causes further messy the waters in terms of ensuring privacy if respected across different legal systems [33].

A key ethical issue is the extent to which governments and law enforcement agencies should be allowed to monitor digital communications and access personal data [34]. While there is clearly a need to develop technologies to detect and prevent cyber crime this must be balanced against the need to ensure the privacy rights of individuals. There needs to be a clear and transparent legal framework governing such activities with penalties for abuse of privacy. The principle of proportionality is also important here. It is paramount that surveillance is undertaken only where there is clear evidence that threats are significant and real and that other industry responses are not suitable. It is also vital that there is considerable independent oversight to ensure any detection technology is used properly and so the right balance can be struck between the right to privacy and the need for collective security.

International collaboration in the the cyber law execution can acquire ethical questions when agencies have to share data with one another. The ethical questions mainly come into the answer when it comes to cross border sharing of data as there may be a difference in standards according to each and every countries privacy policies and data protection policies. It is something which agencies will have to take care of to get their cases solved or at-least makes it less worse than what exactly it might have been [33].

An excellent illustration of such ethical dilemmas are case studies in cybercrime investigations. Law enforcement's use of malware to infiltrate criminal networks brings up points of lawfulness and ethics for legal hacking. [35] Cases involving the extraction of data from encrypted devices call for debates on individual and corporate rights to secure digital information v. law enforcement necessity for key evidence.

Furthermore, what adds up to the collective security-local protection paradox is mass surveil- lance that may take place through facial recognition or data mining algorithms on public spaces, or networks, often without a person's explicit consent. While these technologies can serve as powerful weapons to combat criminals, it has the potential to create a pervasive surveillance culture, which may eventually be detrimental to the trust between the public and law enforcement.

Thus, when dealing with cybercrimes and international law enforcement privacy and ethics go hand in hand; and to be integrated both factors require a delicate balance. Apart from

having a grip on the technology behind surveillance, a theoretical understanding of the legal and ethical framework that envelops privacy and rights is required. But it is of great importance to bear in mind that transparency, proportionality and accountability serves as strong basis for maintaining public trust and assuring that their fundamental privacy rights are preserved.

CONCLUSION

Throughout the course of this paper, we have seen that the challenges that are involve in the realm of the fight against cybercrime under international law are too large to be surmounted with an adequate degree of precision. To fight effectively against cyber criminals, it is important have to the legal methods to fight them. A strong finding is that the legal methods have to adjust the international legal methods has to be adjusted in a way to meet the rapidly technology of the current generation.The importance of changing and refining the international legal instruments, to foster stronger international cooperation and develop of harmonized law enforcement practices across jurisdictions is underlined. Further development of such areas is seen as the way forward for international law in order to tackle the cybercrimes in the future. The future of international law in dealing with cybercrimes is still in the state of flux and with the changing circumstances and challenges of cyber threats, frameworks of law will continue to develop, evolve and be developed to take on these emerging and current challenges in the digital dimension.

The role of international cooperation is emphasized as key in this. Due to the transnational nature of cybercrime no single nation is able to effectively combat it alone. Collective efforts to combat the threats fall under various banners including but not limited to intel sharing, joint investigations and harmonized legal approaches. Ethical considerations when it comes to cyber law enforcement are also posing important questions- what will be our outlook as a society on how much personal protection/privacy/rights that will be eroded/eradicating.
Thus, combatting cybercrime proves to be counterintuitive; cybercrime is in the business of being cutting edge, therefore, by the time laws and guidelines are enacted and set the crest of cybercrime industries are on to the next thing providing 24x7x365 efficient, anonymous illegal activities; much like a clever chameleon who adapts to its surroundings to blend. Whether you've become a victim of search engine poisoning or your personal information has been stolen and is currently being sold on the deep web; you have been hit by cybercrime. Working together globally to identify and address these and many other types is crucial, developing proper legislation and tracking trends can be the only way.

References

[1] Yusuf Perwej, Syed Qamar Abbas, Jai Pratap Dixit, Nikhat Akhtar, and Anurag Kumar Jaiswal. A systematic literature review on the cyber security. *International Journal of scientific research and management*, 9(12):669–710, 2021.
[2] Tim Hall, Ben Sanders, Mamadou Bah, Owen King, and Edward Wigley. Economic geographies of the illegal: the multiscalar production of cybercrime. *Trends in Organized Crime*, 24:282–307, 2021.
[3] Jacob Mofokeng Mmabatho Aphane. South african police service capacity to respond to

cybercrime: Challenges and potentials. *Journal of Southwest Jiaotong University*, 56(4), 2021.

[4] Jildau Borwell, Jurjen Jansen, and Wouter Stol. Comparing the victimization impact of cybercrime and traditional crime: Literature review and future research directions. *Journal of Digital Social Research*, 3(3):85–110, 2021.

[5] Kirsty Phillips, Julia C Davidson, Ruby R Farr, Christine Burkhardt, Stefano Caneppele, and Mary P Aiken. Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic sciences*, 2(2):379–398, 2022.

[6] Tiia Somer. Taxonomies of cybercrime: An overview and proposal to be used in mapping cyber criminal journeys. In *ECCWS 2019 18th European Conference on Cyber Warfare and Security*, volume 475. Academic Conferences and publishing limited, 2019.

[7] Catherine Friend, Lorraine Bowman Grieve, Jennifer Kavanagh, and Marek Palace. Fighting cybercrime: A review of the irish experience. *International Journal of Cyber Criminology*, 14(2):383–399, 2020.

[8] Michael Martin Losavio, Pavel Pastukov, Svetlana Polyakova, Xuan Zhang, Kam Pui Chow, Andras Koltay, Joshua James, and Miguel Etchart Ortiz. The juridical spheres for digital forensics and electronic evidence in the insecure electronic world. *Wiley Interdisciplinary Reviews: Forensic Science*, 1(5):e1337, 2019.

[9] Rebecca S Trammell. What do practicing lawyers need to know about technology? *Wiley Interdisciplinary Reviews: Forensic Science*, 2(4):e1374, 2020.

[10] Majid Yar, T Hall, and V Scalia. Transnational governance and cybercrime control: dilemmas, developments and emerging research agendas. *A research agenda for global crime. Edward Elgar, Cheltenham*, pages 91–106, 2019.

[11] Augustine N Egere. Grassroots police officers' cyber-terminology knowledge and its impact on cybercrime investigations in northeast nigeria. *European Journal of Theoretical and Applied Sciences*, 1(5):370–380, 2023.

[12] Gargi Sarkar and Sandeep K Shukla. Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology*, page 100034, 2023.

[13] Stearns Broadhead. The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. *Computer Law & Security Review*, 34(6):1180–1196, 2018.

[14] Dr Craig S Wright. Geographical aspects of cybercrime: A literature review. *Available at SSRN 4521486*, 2023.

[15] RV Gundur, Michael Levi, Volkan Topalli, Marie Ouellet, Maria Stolyarova, Lennon Yao- Chung Chang, and Diego Domínguez Mejía. Evaluating criminal transactional methods in cyberspace as understood in an international context. 2021.

[16] Meghna M Nair, Amit Kumar Tyagi, and N Sreenath. The future with industry 4.0 at the core of society 5.0: Open issues, future opportunities and challenges. In *2021 international conference on computer communication and informatics (ICCCI)*, pages 1–7. IEEE, 2021.

[17] Jitender Kumar Malik and Sanjaya Choudhury. A brief review on cyber crime-growth and evolution. *Pramana Research Journal*, 9(3):242, 2019.

[18] Bosede Olanike Awoyemi, Olufunmilola Adekiitan Omotayo, and Jane John Mpapalika. Glob- alization and cybercrimes: A review of forms and effects of cybercrime in nigeria. *Internal Journal of Interdisciplinary Research and Modern Education. PP 18*, 25, 2021.

[19] Ashwin Karale. The challenges of iot addressing security, ethics, privacy, and laws.

Internet of Things, 15:100420, 2021.

[20] Hussam N Fakhouri, Sadi Alawadi, Feras M Awaysheh, Faten Hamad, Sawsan Alzubi, and Mohammad Naser AlAdwan. An overview of using of artificial intelligence in enhancing secu- rity and privacy in mobile social networks. In *2023 Eighth International Conference on Fog and Mobile Edge Computing (FMEC)*, pages 42–51. IEEE, 2023.

[21] Ryan Buhrig. Capacity, capability, and collaboration: a qualitative analysis of international cybercrime investigations from the perspective of canadian investigators. *International Cybersecurity Law Review*, pages 1–15, 2023.

[22] Anita Lavorgna. Unpacking the political-criminal nexus in state-cybercrimes: a macro-level typology. *Trends in Organized Crime*, pages 1–20, 2023.

[23] Jack Nicholls, Aditya Kuppa, and Nhien-An Le-Khac. Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. *Ieee Access*, 9:163965–163986, 2021.

[24] Chen-Yu Li, Chien-Cheng Huang, Feipei Lai, San-Liang Lee, and Jingshown Wu. A comprehensive overview of government hacking worldwide. *IEEE Access*, 6:55053–55073, 2018.

[25] KRIS OBIAJE. Economy of news and information access in the digital age: Challenges and prospects

[26] ER MILIND. An overview of cybercrime & cybersecurity. CYBER CRIME &, page 25.

[27] Tania Ixchel Atilano and Tania Ixchel Atilano. Interpretation of international criminal law principles by the mexican judiciary. International Criminal Law in Mexico: National Legislation, State Practice and Eflective Implementation, pages 151–204, 2021.

[28] Russell Buchan, Daniel Franchini, and Nicholas Tsagourias. The changing character of international dispute settlement: Challenges and prospects. 2023.

[29] Cristos Velasco. Cybercrime and artificial intelligence. an overview of the work of international organizations on criminal justice and the international applicable instruments. In ERA Forum, volume 23, pages 109–126. Springer, 2022.

[30] Firman Aziz, Nanny Mayasari, Sabhan Sabhan, Zulkifli Zulkifli, and Moh Fatah Yasin. The future of human rights in the digital age: Indonesian perspectives and challenges. Journal of Digital Law and Policy, 2(1):29–40, 2022.

[31] Monica Vidaurri, Alia Wofford, Jonathan Brande, Gabriel Black-Planas, Shawn Domagal-Goldman, and Jacob Haqq-Misra. Absolute prioritization of planetary protection, safety, and avoiding imperialism in all future science missions: A policy perspective. Space Policy, 51:101345, 2020.

[32] Johan Alfred Sarades Silalahi. The application of criminal law in the digital age: A litera- ture review of challenges and opportunities. Innovative: Journal Of Social Science Research, 3(2):3658–3668, 2023.

[33] Katie Logos, Russell Brewer, Colette Langos, and Bryce Westlake. Establishing a framework for the ethical and legal use of web scrapers by cybercrime and cybersecurity researchers: learnings from a systematic review of australian research. International Journal of Law and Information Technology, 31(3):186–212, 2023.

[34] Naeem Allahrakha. Balancing cyber-security and privacy: Legal and ethical considerations in the digital age. Legal Issues in the Digital Age, 4(2):78–121, 2023.

[35] Charlotte Warner. Law enforcement and digital policing of the dark web: An assessment of the technical, ethical and legal issues. pages 105–115, 2023.

END OF THE PAPER

Global Journal of Politics and Law Research
Vol.12, No.1, pp.78-88, 2024
ISSN: ISSN 2053-6321(Print),
ISSN: ISSN 2053-6593(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Global Journal of Politics and Law Research
Vol.12, No.1, pp.78-88, 2024
ISSN: ISSN 2053-6321(Print),
ISSN: ISSN 2053-6593(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Global Journal of Politics and Law Research
Vol.12, No.1, pp.78-88, 2024
ISSN: ISSN 2053-6321(Print),
ISSN: ISSN 2053-6593(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Global Journal of Politics and Law Research
Vol.12, No.1, pp.78-88, 2024
ISSN: ISSN 2053-6321(Print),
ISSN: ISSN 2053-6593(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Global Journal of Politics and Law Research
Vol.12, No.1, pp.78-88, 2024
ISSN: ISSN 2053-6321(Print),
ISSN: ISSN 2053-6593(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Global Journal of Politics and Law Research
Vol.12, No.1, pp.78-88, 2024
ISSN: ISSN 2053-6321(Print),
ISSN: ISSN 2053-6593(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Global Journal of Politics and Law Research
Vol.12, No.1, pp.78-88, 2024
ISSN: ISSN 2053-6321(Print),
ISSN: ISSN 2053-6593(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Global Journal of Politics and Law Research
Vol.12, No.1, pp.78-88, 2024
ISSN: ISSN 2053-6321(Print),
ISSN: ISSN 2053-6593(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK