A Gap Analysis of Nepal's Cybercrime Laws

Thesis · August 2024

CITATIONS
0

READS
236

1 author:

Basanta Acharya
Nepal Sanskrit University
3 PUBLICATIONS **18** CITATIONS

SEE PROFILE

A Gap Analysis of Nepal's Cybercrime Laws.

A Project work/Internship (LAW-525)

Submitted to

Nepal Law Campus
LLB Programme

Tribhuvan University

An Internship prepared in partial fulfillment of the degree of L.L.B. third year.

Submitted by:
Basanta Acharya
L.L.B Third Year
Roll No.
T.U Regd. No:
Exam Roll Number:

Recommendation Letter

Mr. Basanta Acharya, L.L.B Student of this Campus (CRN) has completed this internship/project work (Law 525) with the report entitled "**A Gap Analysis of Nepal's Cybercrime Laws** " under my supervision and guidance.

Assistant Campus Chief: Lecturer Mr.

Date: … … … …

Nepal Law Campus

Tribhuvan University,

Exhibition Road, Kathmandu

ABSTRACT

Cybercrime is on the rise in Nepal, evidenced by numerous incidents of cyber-attacks, online fraud, and related crimes. Despite efforts to tackle this issue, existing laws such as the Electronic Transactions Act, 2008, and others like the and the Copyright Act, 2002, may fall short in providing comprehensive coverage.

Study Objective: This study seeks to evaluate the necessity for a holistic cybercrime policy in Nepal. It examines current legal frameworks, identifies gaps, and proposes solutions. Employing a mixed-methods approach, the study reviews laws, analyzes case studies, and engages stakeholders through interviews.

Findings: The research underscores the urgency for a dedicated cybercrime policy in Nepal to address the evolving threat landscape. While the draft National Cyber Security Policy 2021 shows promise, there remains a need for a more encompassing framework to safeguard citizens and businesses. The proposed policy emphasizes collaborative efforts and international cooperation to fortify the nation's cyber resilience.

Conclusion: In conclusion, the study advocates for bridging the existing legal gaps and implementing a robust cybercrime policy to safeguard Nepal's digital ecosystem. Such measures are imperative to mitigate risks and ensure the security of individuals and enterprises against cyber threats.

ACKNOWLEDGEMENTS

I extend my heartfelt appreciation to lecturer for his invaluable guidance and unwavering support throughout this study. His profound insights and expertise significantly influenced the trajectory and focus of research.

Our gratitude also extends to the Law Campus Chief and staff for their generous assistance and support during every phase of this study. We are truly thankful for the opportunity to conduct our research at the Law campus and for the exceptional resources and facilities provided.

Lastly, we express our sincere thanks to all individuals who contributed to this study. Their invaluable insights and experiences have greatly enriched our understanding of the subject matter and contributed to the success of our research endeavors.

Lists of Abbreviations

CA:	Children's Act
COPA:	Copyright Act
CERT:	Computer Emergency Response Team
CS Policy:	Cyber Security Policy
CrPC:	Code of Criminal Procedure
ETA:	Electronic Transactions Act
IPA:	Individual Privacy Act
IEA:	Indian Evidence Act
IPC:	Indian Penal Code
ISPs	Internet Service Providers (ISPs)
IT:	Information Technology
IT Act:	Information Technology Act
NCSP:	National Cyber Security Policy
NIC:	National Informatics Centre
NITC	National Information Technology Center
SWIFT:	Society for Worldwide Interbank Financial Telecommunication

Table of contents

CHAPTER: ONE
Introduction and Methodology

1.1 GENERAL BACKGROUND:

Cybercrime is on the rise worldwide. It involves criminals using computers and the internet to commit offenses. These crimes can happen from anywhere and target individuals or organizations across the globe. They aim to harm victims' reputation, cause mental or physical damage, or steal confidential data. Cybercriminals exploit modern communication networks such as the internet and mobile phones. Examples include stealing computer code, hacking into systems, damaging computers, spreading false information, violating privacy, and committing fraud.

Cyber Crime is an act of creating, distributing, altering, stealing, misusing, and destroying information through the computer manipulation of cyberspace[1]

1.2 INTRODUCTION

Cybercrime is becoming a serious issue in Nepal, with more incidents reported each year. Common cybercrimes[2] in the country include ATM attacks, ransomware, spear phishing, privacy breaches, and social media-related offenses like harassment, identity theft, child pornography, and spreading false information. Some incidents, such as SWIFT and ATM Switch hacks[3], are considered advanced cybercrimes. Reports and data show a steady rise in IT-related crimes and frauds. To tackle this problem effectively,

[1] M Dasgupta, Cyber Crimes in India: A Comparative Study, 2009.
[2] https://nepalpolice.gov.np/news/trending-news/cyber-crime/ accessed on jan 2024
[3] Kathmandu Post, October 23, 2017, Available at: https://kathmandupost.com/valley/2017/10/23/nic-asia-cash-stolen-in-cyber-heist, accessed on January 2024.

Nepal needs comprehensive laws addressing cybercrime. An assessment of these laws is essential to identify any gaps or weaknesses and suggest improvements.

The assessment will focus on Nepal's legal provisions concerning cybercrime[4], including hacking, cyberbullying, identity theft, and online fraud. It will also examine the state of cybercrime investigation and prosecution in the country, recommending measures to enhance law enforcement agencies' capabilities. Ultimately, the goal is to analyze Nepal's current legal framework for combating cybercrime and propose enhancements to make these laws more effective against the growing threat.

1.3 CYBER LAW

Cyber law[5], also referred to as internet law, pertains to legal matters concerning the use of communication technologies like computers, the internet, and electronic data interchange. It encompasses various political and legal concerns, including intellectual property rights, privacy, freedom of expression, and jurisdiction.

Though not as distinct as fields like property or contract law, cyber law encompasses a broad spectrum of legal and regulatory dimensions associated with the internet and related technologies. It governs the legal aspects of cyberspace, encompassing computer networks, software, hardware, and information systems.

Cyber law is a constantly evolving and dynamic domain that addresses the legal challenges stemming from the rapid advancement and widespread adoption of new technologies. Any legal issue or aspect linked to activities in cyberspace falls under the purview of cyber law..

[4] myRepublica, September 2, 2019, Available at: https://myrepublica.nagariknetwork.com/news/five-chinese-arrested-for-atm-fraud-rs-12-62-million-recovered/, accessed on January 2024
[5] https://www.ankit-poudel.com.np/2023/07/overview-of-cyber-law-in-nepal.html

1.4 STATEMENT OF PROBLEM

The problem that this need assessment aims to address is the increasing incidence of cybercrime in Nepal and the need for effective laws and enforcement mechanisms to tackle this issue. The Electronic Transactions Act, 2008, is Nepal's first cyber law, and before this law came into force, cybercrimes were dealt with under the country's criminal code. However, since the cases of cybercrime have increased, it has become necessary to enact a separate law to address this issue. Other acts that are used to address cybercrime in Nepal include the Children's Act, 1992, the Copyright Act, 2002, and the Individual Privacy Act, 2018.[6] However, there is no separate law that specifically addresses the various aspects of cybercrime, and this may result in gaps or weaknesses in the legal framework for dealing with this issue. Major of the problem statements are as follows:

Identification of the primary problem this assessment aims to resolve.Examination of existing laws in Nepal pertaining to cybercrime. Evaluation of the inadequacies or insufficient implementation of the current legal framework.Analysis of the adverse impacts of cybercrime on Nepalese society and economy.Justification for a comprehensive review of the existing legal structure concerning cybercrime.

Exploration of how addressing the issue of cybercrime through a thorough assessment can contribute to reducing its incidence and safeguarding individuals and organizations from this menace.

[6] Nepal Law Commission, Available at: https://lawcommission.gov.np/en/ accessed on January 2, 2023.

1.5 OBJECTIVE OF THE STUDY

The main objective of this study are as follows:

- To conduct a need assessment of the comprehensive laws related to cybercrime in Nepal in order to identify any gaps or weaknesses in the current legal framework and to make recommendations for improvement.
- To identify the current legal provisions related to cybercrime in Nepal, including those contained in the Electronic Transactions Act, 2008, and other relevant laws and regulations.
- To assess the effectiveness of the current legal framework in addressing cybercrime in Nepal, including the effectiveness of existing laws and the capacity of law enforcement agencies to investigate and prosecute these crimes.
- To identify any gaps or weaknesses in the current legal framework for dealing with cybercrime in Nepal, and to make recommendations for improvement.
- To consider the need for specialized training and capacity-building for law enforcement agencies in Nepal in order to enhance their ability to investigate and prosecute cybercrime cases.
- To assess the potential for international cooperation in addressing cybercrime in Nepal, including the need for extradition agreements and other measures to facilitate the prosecution of perpetrators located outside of the country.

1.6 IMPORTANCE / SIGNIFICANCE OF STUDY

The importance and significance of this study lies in its potential to improve the legal framework for addressing cybercrime in Nepal and to enhance the effectiveness of law enforcement efforts to combat this growing threat.

As the use of technology and the internet continues to expand and evolve, the incidence of cybercrime is also likely to increase. Cybercrime can have serious consequences for individuals and organizations, including financial losses, damage to reputations, and loss of trust in online platforms and services. It can also undermine the security and stability of critical infrastructure and have wider economic and social impacts.

Conducting a need assessment of the comprehensive laws related to cybercrime in Nepal is therefore an important step in addressing this issue. By identifying any gaps or weaknesses in the current legal framework and making recommendations for improvement, this study has the potential to enhance the ability of law enforcement agencies to investigate and prosecute cybercrime cases, and to improve the legal protections available to individuals and organizations in Nepal who may be at risk of cybercrime.

Additionally, this study may be of value to other countries and jurisdictions that are seeking to address cybercrime through the development of comprehensive legal frameworks. By sharing the findings and recommendations of this study, it may be possible to contribute to the global efforts to combat cybercrime and to promote the responsible and secure use of technology and the internet.

1.7 LIMITATIONS OF THE STUDY

The Study is limited to identify the importance of the cybercrime laws, which are has got the following limitations.

1.7.1 Data availability: The availability of data on cybercrime in Nepal may be limited, which may make it difficult to fully assess the current state of this issue in the country.

Expertise: This study will rely on the expertise of the researchers conducting the assessment and the input of stakeholders, but it may be difficult to obtain a complete and comprehensive understanding of the complex and rapidly evolving field of cybercrime.

1.7.2 Time and resources: Conducting a comprehensive need assessment of the legal framework for dealing with cybercrime in Nepal is a complex and resource-intensive task, and there may be limitations on the time and resources available to complete this work. As well as the study report will be submitted within the specified time set by the TU and within the time limit set by the Nepal Law Campus, Kathmandu.

1.7.3 Scope: This study will focus on the legal framework for dealing with cybercrime in Nepal, but it will not be able to consider other important factors that may influence the incidence of cybercrime in the country, such as cultural and social factors, technological developments, or economic conditions.

Implementation: Even if the recommendations of this study are implemented, it may be difficult to assess the effectiveness of these measures in practice due to the dynamic nature of cybercrime and the challenges of evaluating the impact of legal and policy interventions.

1.7.4 Detail: The study may not be sufficient to address the details of the law required to effectively address cybercrime in Nepal.

1.7.5 Forecasting: The study may not be sufficient to accurately forecast the nature of crime related to the use of information technology in Nepal.

1.7.6 Intercountry law: The study may not be sufficient to provide a complete guide regarding the details of fraud related to information technology systems and its interconnection with intercountry law and regulations.

It is important to consider these limitations when interpreting the findings and recommendations of this study and to approach the issue of cybercrime in Nepal with an awareness of the complexity and evolving nature of this issue.

1.9 LITERCHUR REVIEW:

Naresh Kshetri published "Cyber Strategy of Government of Nepal"[7] an analysis of the Cyber Strategy of the Government of Nepal. It outlines the objectives, priorities, and key initiatives of Nepal's cybersecurity strategy, focusing on enhancing the nation's resilience against cyber threats and vulnerabilities. The document discusses the strategic approach adopted by the Nepalese government to address cybersecurity challenges, including policy development, capacity building, international cooperation, and public-private partnerships. It also highlights the importance of promoting awareness and education to strengthen cybersecurity measures across various sectors.

Shailendra Giri published the document titled **"Cyber Crime, Cyber Threat**[8]**, Cyber Security Strategies, and Cyber Law in Nepal"** on ResearchGate. This document likely offers an in-depth exploration of cybercrime, cyber threats, cybersecurity strategies, and cyber laws within the context of Nepal. It likely covers various aspects such as the nature of cybercrimes in Nepal, emerging cyber threats, strategies employed to enhance cybersecurity, and the legal framework governing cyber activities. Additionally, the document may provide insights into the challenges faced by Nepal in addressing cybercrimes and safeguarding its digital infrastructure. For a more detailed summary and analysis, accessing the document directly on ResearchGate would be necessary.

[7] Kshetri, Naresh, Cyber Strategy of Government of Nepal (July 27, 2017). Available at SSRN: https://ssrn.com/abstract=3552143 or http://dx.doi.org/10.2139/ssrn.3552143

[8] Giri, Shailendra. (2020). Cyber Crime, Cyber threat, Cyber Security Strategies and Cyber Law in Nepal. Volume 9. 662-672.

Mis. Neelima Shahi published her research paper in the journal of Lord Buddha Education Foundation, titled **"A Literature Review on Threats and Countermeasures of Cybersecurity: A Cross-Industry Analysis in Kathmandu."**[9] On the research paper discusses the evolving landscape of cybercrimes in Nepal, examining the challenges and opportunities for law enforcement agencies in combating these threats. It explores the various types of cybercrimes prevalent in Nepal, including hacking, identity theft, and online fraud, and analyzes their impact on individuals, businesses, and the government. The document also evaluates the legal framework governing cybercrimes in Nepal, highlighting the strengths and weaknesses of existing laws and regulations. Additionally, it discusses the role of international cooperation in addressing transnational cyber threats and proposes recommendations for enhancing Nepal's cybersecurity posture.

The research paper, **Security Threats and Legalities with Digitalization in Nepal** authored by **Mr. Sushant Acharya** and **Mr.Sudhamshu Dahal** from the Department of Languages and Mass Communication at Kathmandu University[10], explores the escalating cyber security threats faced by Nepal amidst the global digitalization wave, exacerbated by the COVID-19 pandemic. As digital dependency becomes increasingly integral to daily life, cybercriminal incidents have surged, disrupting societal harmony. The paper investigates the Nepalese government's efforts to address these threats, particularly during the tumultuous lockdowns of 2020. Despite constitutional provisions and legal frameworks aimed at regulating digital activities, the study highlights deficiencies in policy implementation, attributed to legislative delays and a lack of awareness and expertise among lawmakers. Consequently, Nepal grapples with a high risk of cyber security breaches, exacerbated by insufficient defense mechanisms against cyber-attacks.

[9] LBEF Journal, VOL. 3 : ISSUE 3 (https://www.lbef.org/journal/3-3/download/3-3-1-11.pdf)
[10] Research Nepal Journal of Development Studies, Year 4th, Issue 2nd, December 2021

Urgent attention and action are imperative to fortify Nepal's cyber security landscape and mitigate the looming threats posed by the digital age.

The National Judicial Academy in Nepal, released a report titled "A Study on Cyber Crime Cases in Nepal: Challenges and Recommendations 2022[11]." The report highlights the escalating cybercrime rate in Nepal, driven by increased technology adoption and the digital transformation spurred by the COVID-19 pandemic. Challenges in prosecuting cybercrimes stem from the absence of specific cyber laws and outdated legislation such as the Electronic Transactions Act (ETA), 2063. Legal ambiguities lead to inconsistent enforcement and hinder effective case resolution. Addressing emerging cyber threats like cyber terrorism and ransomware requires comprehensive legislative updates. The centralized jurisdiction of the Kathmandu District Court exacerbates access to justice issues, particularly for women. To overcome these challenges, reforms such as establishing an Information Technology Tribunal and improving judicial capacity and infrastructure are imperative. This study underscores the pressing need for enhanced cybercrime laws and enforcement mechanisms in Nepal

Mr. Newal Chaudhary had published his research paper titled: **CYBERCRIME-IN-THE-LAND-OF-EVEREST-UNDERSTANDING-NEPALS-UNIQUE-CHALLENGES**[12] In researchget.net and the the paper delves into Nepal's distinctive hurdles in combating cybercrimes, citing limited technological infrastructure, low digital literacy rates, and inadequate legal frameworks. It discusses emerging cybercrime trends like phishing attacks, online fraud, and cyberbullying, impacting individuals, businesses, and the

[11] A Study on Cyber Crime Cases in Nepal:Challenges and Recommendations 2022, National Judicial Academy, Kathmandu, Nepal

[12] Chaudhary, Newal. (2023). CYBERCRIME-IN-THE-LAND-OF-EVEREST-UNDERSTANDING-NEPALS-UNIQUE-CHALLENGES. 1.

government. Assessing Nepal's legal framework, including the Electronic Transactions Act, 2063 (2008), it highlights challenges such as resource scarcity and expertise. Emphasizing public awareness, it suggests initiatives to enhance digital literacy and safe online practices.

1.8 METHODOLOGY OF THE STUDY

The methodology of this study will involve a comprehensive review of the existing legal framework for dealing with cybercrime in Nepal, as well as an assessment of the current state of cybercrime investigation and prosecution in the country.

1.8.1 Legal review: The study will begin with a review of the current legal provisions related to cybercrime in Nepal, including those contained in the Electronic Transactions Act, 2008, and other relevant laws and regulations. This review will involve a thorough analysis of the legal provisions related to cybercrime in Nepal, as well as an assessment of their effectiveness in addressing this issue.

1.8.2 Case study analysis: The study will also include a review of selected case studies of cybercrime in Nepal in order to gain a more in-depth understanding of the challenges and successes in investigating and prosecuting these crimes.

1.8.3 Data analysis: The data collected through the legal review, stakeholder consultations, and case study analysis will be analyzed in order to identify any gaps or weaknesses in the current legal framework for dealing with cybercrime in Nepal and to make recommendations for improvement.

1.8.4 Recommendations: Based on the findings of the study, the researchers will make recommendations for improving the legal framework for

dealing with cybercrime in Nepal and enhancing the effectiveness of law enforcement efforts to combat this issue.

Overall, the methodology of this study will be designed to provide a comprehensive analysis of the current legal framework for dealing with cybercrime in Nepal and to make recommendations for improving the effectiveness of these laws in addressing this growing threat.

CHAPTER TWO
Conceptual Framework of Cyber world

2.1 CONCEPT OF CYBER WORLD[13]

This study's framework will look at how cybercrime is handled by laws and law enforcement in Nepal and other places. We'll review existing research to see how well legal systems deal with cybercrime. This includes looking at laws like Nepal's Electronic Transactions Act, 2008, and similar laws elsewhere. We'll see what works and what doesn't in fighting cybercrime, and identify any problems or areas for improvement.

We'll also examine how law enforcement tackles cybercrime. This involves looking at different methods used to investigate and prosecute cybercrime, such as specialized units and international cooperation. We'll see what works well, what doesn't, and suggest ways to make things better.

2.2 CONCEPT OF INFORMATION TECHNOLOGY [14]

Information technology (IT) is all about using computers, software, and other digital stuff to handle information. When it comes to cybersecurity, IT is super important because it needs to be shielded from bad stuff like viruses, fake emails, and sneaky data breaches.

Cybersecurity is like the superhero that protects computer systems, networks, and gadgets from bad guys trying to sneak in, steal stuff, or mess things up.

[13] https://www.quora.com/What-is-the-definition-of-cyber-world
[14] https://www.comptia.org/content/articles/what-is-information-technology

It's a bunch of actions like spotting threats, checking risks, reacting fast when something goes wrong, and fixing weaknesses.

In IT and cybersecurity, it's crucial to have really good security measures in place to keep data and systems safe. This means using tools like firewalls, special sensors to catch intruders, secret codes to scramble data, and rules to control who gets access to what.

It's also important to build a strong culture of cybersecurity where everyone knows how to stay safe online. That means teaching people about security, training them to spot problems, and making sure they speak up if something seems fishy. This helps cut down on mistakes and stops cyber baddies in their tracks.

In short, IT is a big deal when it comes to cybersecurity. Keeping everything safe means staying one step ahead of the bad guys by using smart security measures and always keeping an eye out for new tricks they might try.

2.3 CONCEPT OF CYBER SPACE AND CYBER CRIME[15]

Cyberspace refers to the virtual environment created by computer networks, including the internet. It is a space in which people can interact, communicate, and conduct transactions without being physically present. However, the anonymity and lack of physical boundaries in cyberspace have also made it an attractive target for criminals[16]. Cybercrime refers to criminal activities that are carried out using digital technologies and the internet.

[15] https://www.vedantu.com/commerce/introduction-to-cyberspace

[16] Cyber Crime, Cyber Space and Effects of Cyber Crime, International Journal of Scientific Research in Computer Science Engineering and Information Technology, Feb, 2021, 3

There are several theories related to cybercrime[17], which provide insight into the motivations and behaviors of cybercriminals.

1. **Rational Choice Theory –** This theory suggests that individuals engage in computer crime because they believe it is a profitable and low-risk activity. In other words, they weigh the potential benefits of committing a crime against the potential risks of getting caught and punished.

2. **Social Learning Theory –** This theory argues that individuals learn to engage in computer crime through observing the behaviors of others, particularly those who are close to them. They may also be influenced by media portrayals of hackers as glamorous and successful.

3. **Strain Theory –** This theory posits that individuals engage in computer crime when they experience strain or pressure in their lives, such as economic hardship or social exclusion. Computer crime may provide a way for them to alleviate their stress or gain a sense of power and control.

4. **Routine Activities Theory –** This theory suggests that computer crime occurs when there is a convergence of three factors: a motivated offender, a suitable target (such as a vulnerable computer system), and the absence of capable guardians (such as effective cybersecurity measures).

5. **Self-Control Theory –** This theory proposes that individuals who engage in computer crime have low levels of self-control, which makes them more likely to act impulsively and make decisions without considering the consequences.

Overall, these theories provide important insights into the motivations and behaviors of cybercriminals, which can be used to develop effective strategies to prevent and combat cybercrime in cyberspace. It is important to implement

[17] https://cod.pressbooks.pub/crimj1165/chapter/module-3/

comprehensive cybersecurity measures and to promote awareness of cybercrime and its impacts to reduce the risk of becoming a victim of cybercrime.

2.4 CONCEPT OF CYBER LAW

Cyber law, also called internet law[18], is the set of rules that controls how we use computers, the internet, and other digital stuff. It covers lots of different legal stuff related to technology, like who owns ideas, how to keep personal stuff private, and what's allowed when we buy things online.

This area of law is always changing because technology keeps getting fancier and people find new ways to use it. Cyber law uses lots of different legal ideas, like contracts and property rights, to figure out what's right and wrong in the digital world.

One big part of cyber law is making sure that people's ideas are safe. This means protecting things like logos, songs, and inventions so that creators and businesses can keep them safe from others copying them.

Another important part is keeping people's private stuff, well, private. Since we're all sharing a lot online, cyber law makes rules about how companies and governments can collect and use our personal information.

Cyber law also covers the rules for buying and selling stuff online, like how contracts work and what happens if something goes wrong. It helps make sure that transactions are fair and safe for everyone involved. And, of course, cyber law deals with cybercrime[19], like hacking or stealing someone's identity online. It sets up rules for catching and punishing people who break the law in the digital world.

[18] https://www.techopedia.com/definition/25600/cyberlaw
[19] https://www.primelawnepal.com/blog/28/cyber-crime-laws-in-nepal.html

Overall, cyber law is super important because it makes sure that we're all playing by the rules when we're online. And as technology keeps changing, cyber law will keep changing too, to keep up with all the new stuff we can do online.

2.5 Cyber laws and cybercrime legislation in Asia

Cyber laws and cybercrime legislation in Asia vary depending on the country. In general, most Asian countries have developed cyber laws and legislation in response to the increasing use of digital technologies and the internet, as well as the growing threat of cybercrime[20].

2.5.1 Nepal has several cyber laws and regulations:[21]

in place to govern the use of digital technologies and the internet. **The Electronic Transactions Act, 2063 (2008)** is the primary law governing electronic transactions in Nepal. This law provides legal recognition for electronic records and digital signatures, and establishes a framework for electronic transactions and e-commerce.

Nepal also has the **Information Technology (IT) Act, 2061 (2004),** which provides legal protections for intellectual property and regulates the use of digital media in Nepal. The IT Act criminalizes several forms of cybercrime, including unauthorized access to computer systems, the distribution of viruses, and the dissemination of fraudulent information online.

In addition to these laws, Nepal has established **the National Information Technology Center (NITC) to provide guidance and support on cyber**

[20] Guillaume Lovet Fortinet, Fighting Cybercrime: Technical, Juridical and Ethical Challenges, VIRUS BULLETIN CONFERENCE, 2009" Available at: http://whitepapers.hackerjournals.com/wp-content/uploads/2009/12/FIGHTING-CYBERCRIME.pdf, Accessed on: Jan 8, 2023

[21] https://www.researchgate.net/publication/368306858_Cyber_Laws_and_Policies_in_Nepal

law issues[22]**,** and to assist in the investigation and prosecution of cybercrime cases.

2.5.2 Indian and China have latest cyber laws: In place to address cybercrime in **India** has the Information Technology (IT) Act, 2000, which provides legal protections for intellectual property and regulates the use of digital media. The IT Act also criminalizes several forms of cybercrime, including hacking, identity theft, and the distribution of obscene materials online.

China has multiple laws and regulations governing cyberspace, including the Cybersecurity Law of the People's Republic of China, enacted in 2017.[23] The Cybersecurity Law aims to protect national cyberspace sovereignty and security, regulate cyber activities, and safeguard the rights and interests of citizens and organizations. It includes provisions related to data protection, network security, critical information infrastructure, and the supervision and management of cyberspace.

2.5.3 Other countries in Asia also have cyber laws and legislation:

Similarly, **Japan** has the Basic Act on Cybersecurity,[24] which provides a framework for cybersecurity and establishes a national cybersecurity strategy. The **Philippines** has the Cybercrime Prevention Act 2012[25], which criminalizes several forms of cybercrime, including hacking, identity theft, and the distribution of malicious software[26]. Malaysia, Singapore, and South Korea lead the national cybersecurity index in APAC. The index measures

[22] https://nitc.gov.np/services/all
[23] https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/
[24] https://www.japaneselawtranslation.go.jp/en/laws/view/3677/en#je_toc
[25] https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/
[26] Republic Act No. 10175 — An act defining cybercrime, providing for the prevention, investigation, suppression and the imposition of penalties therefor and for other purposes". Official Gazette of the Republic of the Philippines. Office of the President of the Philippines. September 12, 2012.

each country's preparedness to prevent and manage cyber threats – all three countries have central government bodies dedicated to cybersecurity in place[27]

Overall, cyber laws and cybercrime legislation in Asia, including Nepal, are critical for regulating the use of digital technologies and the internet, and for providing legal protections and frameworks to address cybercrime. As technology continues to advance and new forms of cybercrime emerge, these laws and regulations will continue to evolve to address new challenges and threats in the digital age.

2.6 THE ELECTRONIC TRANSACTIONS ACT, 2008

Nepal's Electronic Transactions Act, 2008 (ETA)[28] marks the country's first step into cyber law, aiming to regulate electronic transactions and combat cybercrimes. It covers the legal acceptance of electronic records, signatures, and contracts, along with responsibilities for intermediaries like internet service providers.

Key among the ETA's provisions are Chapter-7, Chapter-8, Chapter-9, Chapter-10, and Chapter-11, these chapters tackle cybercrimes by penalizing activities such as hacking, unauthorized data access, and distributing offensive content. The act also allows for monitoring electronic communications and establishes a Cyber Crime Investigation Bureau to coordinate law enforcement efforts.

Before the ETA, cybercrimes were addressed within Nepal's criminal code. However, the rising instances of cyber offenses prompted the

[27] https://www.statista.com/topics/11226/cybersecurity-and-cybercrime-in-the-asia-pacific-region/
[28] The Electronic Transactions Act, 2063 (2008)

need for a dedicated law. Chapter 9 of the ETA focuses on computer-related offenses, including piracy, unauthorized access, data tampering, and fraud, punishable by imprisonment, fines, or both.

Besides the ETA, Nepal has other laws addressing specific cybercrime aspects. For instance, the Children's Act, 2018, tackles issues like child pornography, while the Copyright Act, 2002, handles online copyright violations. The Individual Privacy Act, 2018, also plays a role in safeguarding personal data in the digital realm.

2.7 THE CHILDREN'S ACT, 2018

The Children Act 2018 is a law in Nepal that governs the rights and protection of children. [29]The act was passed by the Nepali parliament on June 12, 2018, and became effective on September 14, 2018.

The act aims to protect the rights of children in Nepal and provide them with necessary support and assistance. It also seeks to prevent and address any form of child abuse, exploitation, and neglect.

Under the Children Act 2018, every child in Nepal has the right to education, health care, and protection from all forms of exploitation and abuse. The act also establishes a child welfare committee in each district, which is responsible for ensuring the welfare of children and implementing the provisions of the act.

[29] The Act Relating to Children, 2075 (2018), Available at: https://www.lawcommission.gov.np/en/wp-content/uploads/2019/07/The-Act-Relating-to-Children-2075-2018.pdf, Accessed on: January 27, 2023

The act also recognizes the rights of children with disabilities and provides for their protection and rehabilitation. It establishes a special court for the trial of offenses against children and provides for the appointment of a child rights advocate to represent children in court.

The Children Act 2018 also provides for the establishment of a national council for the protection of children and their welfare. This council is responsible for formulating policies and programs for the protection of children and for coordinating the efforts of various government agencies and NGOs.

The act recognizes the importance of family and community-based care for children and encourages the use of alternative care arrangements, such as foster care and adoption, where appropriate. It also establishes a system for the monitoring of institutions providing care for children, such as orphanages and child care centers.

Overall, the Children Act 2018 is an important law in Nepal that aims to protect and promote the rights and welfare of children. It provides a framework for addressing issues related to child abuse, exploitation, and neglect, and for ensuring that children in Nepal have access to education, health care, and other essential services.

2.7.1 Nepalese Cyber Law and Children[30]

The internet, otherwise known as the “World Wide Web” is a medium which facilitates the spread of information and communication between people at a global level. The internet is a ‘free’ medium, with no international laws and regulations upon it, therefore it is extremely difficult to both monitor and prohibit transactions that occur within it. Cybercrime is

[30] http://www.iccwtnispcanarc.org/upload/pdf/1792641426Nepalese Cyber Law and Children_2.pdf

regarded to be the computer manipulation of information to the detriment of the focus or victim of said information: “Cybercrime is an act of creating, distributing, altering, stealing, misusing and destroying information through the computer manipulation of cyber space; without the use of physical force and against the will or interest of the victim.” US Department of Justice Although it is a positive tool in many regards, for it can promote the infiltration of knowledge at an educational and liberating level, it allows for illicit transactions such as the availability of child pornography, gambling and inappropriate interaction between minors and adults. The internet has become a breeding ground for child exploitation and pornography. There are few prohibitions within the internet to control exploitative pornography therefore the internet has given rise to an ever increasing pornographic trade – particularly in countries where regulations are at a minimum, such as Nepal. The Council of Europe Convention on Cybercrime (2001) defines child pornography as depictions of individuals who are in fact or who appear to be under 18 years of age engaging in sexually explicit conduct. Child pornography, whether by free choice or against the will, is extremely damaging to minors both emotionally and psychologically. Children, in particular girls, are vulnerable to sexual exploitation facilitated by the open market of the internet within which pornographers and pedophiles flourish. Images of children exposed or in the course of sexual activity, either by or against their own will, are easily accessible over the internet which adults and minors have free access to daily. Both those creating such images and those consuming such images are criminals, yet Nepal currently has no legal framework in order to persecute perpetrators encouraging criminals to continue the victimization of children. In light of the International Conference on Combating Child Pornography on the Internet (Vienna, 1999) which called for a world-wide effort to criminalize the creation, distribution, manipulation and dissemination of child pornography it is even more important for Nepal to become a part of this

global effort. Nepal lacks the laws to criminalize perpetrators and the spread of pornographic material, nor is there a support system to aid victims of pornography with recovery as is required by The United Nations' Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution, and child pornography (2000). This needs to be rectified. In order to fulfill its obligation to its children and to protect them from exploitation, abuse and damage Nepal needs to implement and enforce effective cyber laws which can deter crimes, persecute perpetrators and protect children.

2.8 THE COPYRIGHT ACT, 2002

The Copyright Act, 2002 is a law in Nepal that provides for the protection of copyright and related rights[31]. The Act is divided into nine chapters, which address a range of issues related to copyright, including the types of works that are protected by copyright, the rights of copyright owners, and the exceptions to copyright protection

Chapter 1 of the Act contains general provisions, including definitions of terms used in the Act and the principles underlying the Act. Chapter 2 deals with the types of works that are protected by copyright, including literary, artistic, and musical works, as well as films, sound recordings, and broadcasts.

Chapter 3 of the Act addresses the rights of copyright owners, including the right to reproduce the work, the right to distribute the work, and the right to communicate the work to the public. Chapter 4 deals with the duration of copyright protection and the conditions under which copyright protection expires.

[31] Copyright Protection in Nepal". Solar Law Associates. Retrieved February 18, 2013, Available at: https://lawcommission.gov.np/en/?cat=373, Accessed on: January 20, 2023

Chapter 5 of the Act addresses the exceptions to copyright protection, including exceptions for private use, research and study, news reporting, and the use of works in judicial proceedings.

Chapter 6 deals with the assignment and licensing of copyright, and it includes provisions on the transfer of copyright ownership and the terms and conditions of copyright licenses.

Chapter 7 of the Act addresses the enforcement of copyright, and it includes provisions on the remedies available to copyright owners in cases of copyright infringement, as well as provisions on the powers of the courts to enforce copyright. Chapter 8 deals with the registration of copyright and the role of the Copyright Office in registering copyright and maintaining records of copyright ownership.

Chapter 9 of the Act contains miscellaneous provisions, including provisions on the power of the government to make rules and regulations to implement the Act and provisions on the international obligations of Nepal under international copyright treaties.

Overall, the Copyright Act, 2002 is an important law in Nepal that provides for the protection of copyright and related rights, including in the digital environment.

2.9 THE INDIVIDUAL PRIVACY ACT, 2018

This act is the first legislation in Nepal to protect the right to privacy of its people, and define personal information. It protects the privacy of body, family life, residence, property, and communication. It puts the responsibility on public entities to protect the personal data of

individuals. They cannot transfer such data to anyone without the consent of the owner. The Act prescribes a general punishment for violation of privacy as three years of imprisonment, or a fine of NPR 30,000, or both.

2.10 CURRENT SITUATION:

According to Nepal Police statistics, cyberbullying cases have seen a significant increase since 2014. Instances include data breaches at companies like FoodMandu and Vianet, as well as government departments like the Ministry of Agriculture and Central Library. There have also been reported cases of ATM hacks and cyberbullying on social media platforms. These incidents highlight vulnerabilities in Nepal's cybersecurity system.

Cybercrimes fall under the jurisdiction of the Electronic Transaction Act 2008. To address cybersecurity threats such as hacking and phishing, an expert group called the Computer Emergency Response Team (CERT) operates under the Department of Information Technology. They work alongside security operations centers to establish detection protocols and coordinate responses to cyber threats.

However, the Electronic Transaction Act 2008 doesn't fully adapt to the evolving landscape of cyberspace. To address this gap, the Ministry of Communication and Information Technology has developed a new policy draft called the 'National Cyber Security Policy 2021.'[32] This

[32] Experts Urge to Refine 'Cybersecurity Policy 2021 Draft', say there are Ample Gaps to be Fulfilled, Nikeeta Gautam, Available at: https://techlekh.com/cyber-security-policy-2021-draft/#:~:text=The%20new%20National%20Cyber%20Security,the%20responsibility%20of%20the%20stakeholders/, Posted date: 12 June 2021, Accessed on : Feb 20, 2023

policy aims to modernize and address emerging cybersecurity challenges in Nepal.

2.11 CYBERCRIME LAWS IN INDIA:

In India, cybercrime is governed by the Information Technology Act, 2000. Some of the key provisions related to cybercrime include[33]:

- Section 66: Punishment for hacking with computer system
- Section 66A: Punishment for sending offensive messages through communication service
- Section 66B: Punishment for dishonestly receiving stolen computer resource or communication device
- Section 66C: Punishment for identity theft
- Section 66D: Punishment for cheating by personation by using computer resource
- Section 67: Punishment for publishing or transmitting obscene material in electronic form
- Section 67A: Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form
- Section 67B: Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form
- Section 69: Power to issue directions for interception or monitoring or decryption of any information through any computer resource
- Section 69A: Power to block for public access of any information through any computer resource

[33] Indian Computer Emergency Response Team (CERT-In), Available on: www.cert-in.org.in, Ministry of Electronics and Information Technology , www.meity.gov.in, www.cyberlawindia.net, Accessed on: January 02, 2023.

Additionally, the Indian government has also set up the Indian Computer Emergency Response Team (CERT-In) to respond to and address cyber security incidents.

Some other laws and acts which are associated with cybercrime in India are:

1. The Indian Penal Code, 1860
2. The Code of Criminal Procedure, 1973
3. The Indian Evidence Act, 1872
4. The Prevention of Damage to Public Property Act, 1984
5. The Protection of Children from Sexual Offences Act, 2012
6. The Unlawful Activities (Prevention) Act, 1967
7. The Official Secrets Act, 1923
8. The National Cyber Security Policy, 2013

These acts and laws provide a framework for the Indian government to investigate and prosecute cybercrime, and to protect the rights and interests of citizens in the digital space[34].

2.12 LAWS AND CYBERCRIME IN THE PEOPLE'S REPUBLIC OF CHINA:[35]

There are several other laws and regulations in China that are associated with cybercrime and cybersecurity. Some of these include:

Criminal Law of the People's Republic of China: This law includes provisions related to cybercrimes such as hacking, cyber fraud, spreading computer viruses, and disrupting computer networks. Offenses under this law can result in imprisonment, fines, or other penalties.

Regulations on Internet Security Protection: These regulations, enacted by the Cyberspace Administration of China, aim to protect internet security and combat cybercrimes. They include provisions for monitoring and regulating internet content, as well as measures to safeguard data privacy and prevent cyber attacks.

---

[34] Income Tax Appellate Tribunal, Available at: www.itat.nic.in, Cybercrime Investigation Cell, Available at: www.cybercrime.gov.in, Ministry of Home Affairs, India, Available at: www.mha.gov.in, Accessed on February 20, 2023.

[35] https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/china

Measures for the Security Assessment of Cross-Border Data Transfer: These measures, issued by the Cyberspace Administration of China, regulate the cross-border transfer of personal information and important data. They aim to ensure the security of data and prevent unauthorized access or leakage.

National Intelligence Law: Enacted in 2017, this law allows Chinese intelligence agencies to compel organizations and individuals to assist with intelligence work, including in matters related to cybersecurity and national security.

Regulations on the Protection of the Right to Network Dissemination of Information: These regulations govern online content dissemination and include provisions related to cyber defamation, spreading rumors, and other illegal activities on the internet.

These are just a few examples of the laws and regulations in China that are associated with cybercrime and cybersecurity. The Chinese government continues to enact and enforce measures aimed at maintaining cybersecurity and combating cyber threats in the country.

CHAPTER THREE
Details of the Study

3 DETAILS OF THE STUDY.

The study's aim is to evaluate cybercrime laws in Nepal. It will:

- Look into relevant policies, acts, bylaws, and guidelines, including the Electronic Transactions Act, 2008, Children's Act, 2018, Copyright Act, 2002, and Individual Privacy Act, 2018.
- Identify gaps in these laws and areas needing more laws or guidance to tackle cybercrime.
- Review cybercrime cases from Nepal Police Cyber Cell and news reports to understand the extent and nature of cybercrime in Nepal[36].

Overall, the study seeks to assess Nepal's cybercrime laws comprehensively and pinpoint where more laws or guidance are necessary to effectively address the issue.

3.1 CURRENT STATUS AND CHALLENGES:

According to Nepal Police statistics, cyberbullying cases have risen since 2014. Incidents such as data breaches at FoodMandu, Vianet, Ministry of Agriculture, and Central Library, ATM hacks, NIC Asia SWIFT hack, and social media cyberbullying have been reported due to gaps in Nepal's cybersecurity system.

Cybercrimes fall under the Electronic Transaction Act 2008. The Computer Emergency Response Team (CERT), part of the Department

[36] https://nepalpolice.gov.np/news/trending-news/cyber-crime/

of Information Technology, handles cybersecurity threats like hacking and phishing. They work with security operations center teams to detect threats and coordinate responses.

However, the Electronic Transaction Act 2008 doesn't fully address the evolving challenges of cyberspace. Therefore, the Ministry of Communication and Information Technology has Approved the **'National Cyber Security Policy 2021' t**o govern and tackle cybersecurity issues.

3.2 LEGAL PROVISION ON ELECTRONIC TRANSACTION ACT, 2008.

Nepal has several laws and regulations concerning cybercrime. The main law addressing cybercrime is the Electronic Transactions Act, 2008 (ETA). It covers various offenses related to cybercrime, including:

- Intentionally damaging or pirating computer systems without permission, punishable by up to three years in prison or a fine of two hundred thousand rupees, or both.
- Unauthorized access to computer systems, carrying the same penalty.
- Intentional deletion or damage of data from computer systems, also punishable by up to three years in prison or a fine of two hundred thousand rupees, or both.
- Publishing illegal material in electronic form, which can result in up to five years in prison or a fine of one hundred thousand rupees, or both.
- Committing computer fraud, punishable by up to two years in prison or a fine of one hundred thousand rupees, or both.
  .3L
  j

3.2.1 Gap analysis on Electronic Transaction Act, 2008.

The laws regarding cybercrime in Nepal, such as those outlined in the Electronic Transactions Act, 2008, and other relevant regulations, might have shortcomings that could hinder their ability to effectively tackle cybercrime in the nation. Some possible gaps in these legal provisions could include:[37]:

3.2.1.1 **Limited scope:** Certain legal provisions concerning cybercrime in Nepal might have restricted coverage, failing to include all cybercrimes. The Electronic Transactions Act (ETA) is a case in point, as it solely addresses a limited set of computer and electronic transaction-related offenses. Consequently, it might not adequately address emerging cybercrime types or advancements in technology.

3.2.1.2 **Absence of specific cybercrime legislation:** Nepal lacks a dedicated law solely focusing on cybercrime encompassing all its aspects. Instead, different cybercrimes fall under separate laws and regulations, posing challenges in addressing cybercrime comprehensively and uniformly.

3.2.1.3 **Insufficiency of specialized skills:** Investigating and prosecuting cybercrime cases often demand specialized knowledge and expertise, which may be deficient within Nepal Police Cyber Cell and other law enforcement agencies. This shortfall could impede the efficient enforcement of cybercrime laws in Nepal.

3.2.1.4 **Limited international cooperation:** Nepal might have trouble getting help from other countries for cybercrime cases because they don't have many agreements with them. This could make it hard to deal with cybercrimes that happen across borders. Also, the laws in Nepal might not be strong enough to stop cybercrime well.

---

[37] Electronic Transaction Act 2063, Available at: http://www.tepc.gov.np/uploads/files/12the-electronic-transaction-act55.pdf, Accessed on: March 20, 2024

3.2.1.5 Insufficiency of specialized skills: Investigating and prosecuting cybercrimes involving children may necessitate specific knowledge and expertise, which could be lacking within the Nepal Police Cyber Cell and other law enforcement agencies. This deficiency might impede the effective enforcement of the Children's Act, 2018, regarding cybercrime cases.

3.2.1.6 Restricted international cooperation: Nepal might encounter hurdles in securing international cooperation for cybercrime cases involving children due to the absence of mutual legal assistance treaties or other agreements with other nations. This could hamper the investigation and prosecution of cross-border cybercrimes involving children.

3.2.1.7 Absence of dedicated cybercrime legislation: Nepal lacks a specific law exclusively addressing cybercrime in its entirety. Consequently, the Children's Act, 2018, may need to be supplemented with other laws and regulations to handle cybercrime cases involving children. This could complicate the legal process and hinder the effective resolution of such cases.

Overall, these gaps, along with others in the Children's Act, 2018, concerning cybercrime, may restrict the law's effectiveness in addressing this issue in Nepal.

3.3 GAP ANALYSIS OF THE COPYRIGHT ACT, 2002

The Copyright Act, 2002, which is a law in Nepal that provides for the protection of copyright and related rights, may have certain gaps in relation to cybercrime that could limit its effectiveness in addressing this issue.

Some potential gaps in the Copyright Act, 2002, in the context of cybercrime could include:

3.3.1 Limited scope: The Copyright Act, 2002, may have a limited scope in relation to cybercrime, as it mainly addresses issues related to the unauthorized use of copyrighted material and may not cover other forms of cybercrime, such as online fraud or cyberbullying.

3.3.2 Lack of specialized expertise: The investigation and prosecution of cybercrime cases involving copyright infringement may require specialized knowledge and expertise, which may be lacking within the Nepal Police Cyber Cell and other law enforcement agencies. This could hinder the effective enforcement of the Copyright Act, 2002, in relation to cybercrime.

3.3.3 Limited international cooperation: Nepal may face challenges in obtaining international cooperation in cases of cybercrime involving copyright infringement due to a lack of mutual legal assistance treaties or other agreements with other countries. This could make it difficult to investigate and prosecute cross-border cybercrime cases involving copyright infringement.

3.3.4 Lack of dedicated cybercrime legislation: Nepal does not have a dedicated cybercrime law that addresses all aspects of cybercrime. This means that the Copyright Act, 2002, may need to be used in conjunction with other laws and regulations to address cybercrime cases involving copyright infringement, which could complicate the legal process and make it more difficult to effectively address these cases.

Overall, these and other gaps in the Copyright Act, 2002, in the context of cybercrime could limit the effectiveness of this law in addressing this issue in Nepal.

3.4 GAP ANALYSIS OF THE INDIVIDUAL PRIVACY ACT 2018.

The Individual Privacy Act, 2018 is a law in Nepal that aims to protect the personal data and privacy of individuals. However, it may have certain gaps in relation to cybercrime that could limit its effectiveness in addressing this issue.

One potential gap is the limited scope of the law, as it mainly addresses issues related to the collection, use, and disclosure of personal data, and may not cover other forms of cybercrime, such as online fraud or cyberbullying. This means that the law may not provide sufficient protection against these types of cybercrime, and other legal provisions may need to be used to address them.

Another potential gap is the lack of specialized expertise in the investigation and prosecution of cybercrime cases involving the misuse of personal data. Cybercrime cases often require specialized knowledge and expertise, and the Nepal Police Cyber Cell and other law enforcement agencies may not have sufficient resources or expertise to effectively investigate and prosecute these cases. This could hinder the enforcement of the Individual Privacy Act, 2018 in relation to cybercrime.

A third potential gap is the limited international cooperation in cases of cybercrime involving the misuse of personal data. Nepal may face challenges in obtaining international cooperation due to a lack of mutual

legal assistance treaties or other agreements with other countries. This could make it difficult to investigate and prosecute cross-border cybercrime cases involving the misuse of personal data[38].

Finally, the lack of a dedicated cybercrime law in Nepal could be a gap in the legal provisions related to cybercrime. The Individual Privacy Act, 2018 may need to be used in conjunction with other laws and regulations to address cybercrime cases involving the misuse of personal data, which could complicate the legal process and make it more difficult to effectively address these cases.

Overall, these and other gaps in the Individual Privacy Act, 2018 in the context of cybercrime could limit the effectiveness of this law in addressing this issue in Nepal.

3.5 ADDRESSING THE GAPS IN NEPAL'S LEGAL PROVISIONS FOR CYBERCRIME

In conclusion, Nepal faces significant gaps in its existing legal framework related to cybercrime, necessitating the development of a comprehensive cybercrime policy. While laws such as the **Electronic Transactions Act, 2008, Children's Act, 2018, Copyright Act, 2002**, and **Individual Privacy Act, 2018** address certain aspects of cybercrime, they may not cover all forms adequately.

India, a neighboring country, has established robust cybercrime laws like the **Information Technology Act, 2000**, and the **Cyber Security Policy, 2013**. Nepal could draw inspiration from these policies while tailoring its own to meet specific local challenges.

[38] Cyber Strategy of Government of Nepal, Naresh Kshetri, Lindenwood University, Available at: https://www.researchgate.net/publication/340465310_Cyber_Strategy_of_Government_of_Nepal, Accessed on: February 20, 2023

Given the evolving nature of cyber threats, Nepal urgently requires a well-defined cybercrime policy to guide law enforcement, businesses, and individuals. Such a policy would clarify rights and responsibilities, fortify protection against cyber threats like online fraud and cyberbullying, and safeguard citizens and businesses alike.

Alongside existing laws, Nepal is working on the **National Cyber Security Policy 2023**[39], which aims to safeguard critical information infrastructure, secure electronic communications, and promote the use of secure electronic systems and services. This forthcoming policy holds promise in bolstering Nepal's cyber resilience.

The **National Cyber Security Policy 2023** is geared towards fostering a secure cyber environment in Nepal through a collaborative effort involving the government, private sector, academia, and civil society. It seeks to enhance international cooperation and coordination in cyber security and establish a national incident response mechanism to swiftly and efficiently address cyber security incidents.

In essence, the National Cyber Security Policy 2023 is a crucial initiative aimed at tackling Nepal's cyber security challenges. With effective implementation, it holds the promise of substantially enhancing the country's cyber security resilience and safeguarding its citizens and businesses from the escalating menace of cybercrime.

[39] https://api.giwms.gov.np/storage/22/posts/1691665949_27.pdf

CHAPTER FOUR
Conclusion and Recommendations

4. Conclusions and recommendations

The legal and policy framework for addressing cybercrime in Nepal is not as comprehensive as the framework in place in India. Nepal's first cyber law related to cybercrime was the Electronic Transactions Act, 2008, which deals with offences relating to computers, such as pirating or destroying a computer system without authority, accessing a computer system without authority, and intentional damage to or deletion of data from a computer system. However, this law has limited scope and may not cover all forms of cybercrime.

Other laws that are used to address cybercrime in Nepal include the Children's Act, 2018, which addresses issues such as cyberbullying and the publication of illegal material online, and the Copyright Act, 2002, which addresses issues such as online piracy. Nepal also has the Individual Privacy Act, 2018, which addresses issues related to privacy and data protection.

Overall, Nepal could benefit from a more comprehensive legal and policy framework for addressing cybercrime, similar to the framework in place in India. A dedicated cybercrime policy in Nepal would provide a comprehensive legal framework for addressing all types of cybercrime, and would provide clarity and guidance to law enforcement agencies, businesses, and individuals on their rights and responsibilities in relation to cybercrime.

4.1 CONCLUSIONS:

Key findings from the study regarding the necessity of a comprehensive cybercrime policy in Nepal include:

- Substantial gaps exist in the current legal provisions concerning cybercrime, encompassing laws like the Electronic Transactions Act, 2008, and other pertinent regulations. These gaps may hinder the effectiveness of ongoing efforts to combat cybercrime in Nepal.

- A dedicated cybercrime policy would furnish Nepal with a robust legal framework to address various forms of cybercrime comprehensively, spanning online fraud, cyberbullying, and emerging cyber threats.

- The investigation and prosecution of cybercrime cases often demand specialized knowledge and expertise, which may be lacking within the Nepal Police Cyber Cell and other law enforcement bodies. A cybercrime policy would offer guidance and assistance to law enforcement agencies in handling such cases effectively.

- Nepal might encounter obstacles in securing international cooperation for cross-border cybercrime cases due to the absence of mutual legal assistance treaties or other agreements with foreign nations. A cybercrime policy would establish a framework for international cooperation and collaboration in investigating and prosecuting cross-border cybercrime incidents.Nepal does not currently have a dedicated cybercrime

law that addresses all aspects of cybercrime. A cybercrime policy would provide a comprehensive legal framework for addressing all types of cybercrime, and would provide clarity and guidance to law enforcement agencies, businesses, and individuals on their rights and responsibilities in relation to cybercrime.

Overall, it is clear that Nepal needs a comprehensive cybercrime policy to address the various gaps in the existing legal provisions related to cybercrime and to provide a comprehensive framework for addressing this issue.

4.2 RECOMMENDATION:

Based on the above study, some recommendations for addressing the need for a comprehensive cybercrime policy in Nepal include:

- Develop a dedicated cybercrime policy that addresses all types of cybercrime and provides a comprehensive legal framework for addressing this issue.
- Provide additional resources and training to law enforcement agencies, including the Nepal Police Cyber Cell, to enhance their capabilities in investigating and prosecuting cybercrime cases.
- Establish mutual legal assistance treaties or other agreements with other countries to facilitate international cooperation in cases of cross-border cybercrime.
- Develop a national cyber security incident response mechanism to handle cyber security incidents in a timely and effective manner.

- Increase public awareness and education on cybercrime prevention and safety measures, including measures to protect personal information and prevent identity theft.
- Encourage the use of secure electronic communication systems and services to protect against cybercrime.

Regularly review and update the cybercrime policy to ensure that it is effective in addressing emerging forms of cybercrime and evolving cyber threats.

Bibliography

"Electronic Transactions Act, 2008." Ministry of Law, Justice, and Parliamentary Affairs, Government of Nepal.

"Children's Act, 2018." Ministry of Women, Children and Senior Citizen, Government of Nepal.

"Copyright Act, 2002." Ministry of Law, Justice, and Parliamentary Affairs, Government of Nepal.

"Individual Privacy Act, 2018." Ministry of Law, Justice, and Parliamentary Affairs, Government of Nepal.

"Information Technology Act, 2000." Ministry of Electronics and Information Technology, Government of India. https://meity.gov.in/writereaddata/files/it-act-2000.pdf

"Cyber Security Policy, 2013." Ministry of Electronics and Information Technology, Government of India. https://meity.gov.in/writereaddata/files/cyber_security_policy_2013.pdf

Nepal Law Commission (2021), Draft of National Cyber Security Policy

Gautam, Neekita (July, 2021), Experts Urge to Refine 'Cyber security Policy 2021 Draft, say there are Ample Gaps to be Fulfilled, techlink.com

Indian Computer Emergency Response Team (CERT-In) - www.cert-in.org.in

Ministry of Electronics and Information Technology - www.meity.gov.in

Cyberlaw India - www.cyberlawindia.net

Income Tax Appellate Tribunal - www.itat.nic.in

Cybercrime Investigation Cell - www.cybercrime.gov.in

Ministry of Home Affairs - www.mha.gov.in