# CYBERCRIME IN THE LAND OF EVEREST: UNDERSTANDING NEPAL'S UNIQUE CHALLENGES

*Legal Upanishad Journal (LUJournal.com)*

*Vol 1 Issue 2 | August 2023 | pp- 77-87*

Dr Newal Chaudhary, Advocate, Supreme Court of Nepal; Assistant Professor of Law, Nepal Law Campus, Tribhuvan University, Kathmandu

## ABSTRACT

*Cybercrime is becoming a serious issue in Nepal, with a rising number of cases being reported each year. In response to this growing problem, this article delves into the challenges that Nepal faces in tackling cybercrime as well as the opportunities that are available to address the issue. It provides an overview of the current state of cybercrime in Nepal, including the different types of cybercrime that are prevalent and how they impact individuals, businesses, and the economy. The article highlights the challenges that Nepal is facing in combating cybercrime. These include a lack of awareness about cyber threats, an inadequate legal framework for dealing with cybercrime, and a shortage of skilled cyber security professionals. Furthermore, it identifies the consequences of not addressing these challenges, which could result in serious damage to Nepal's economy and society as a whole. The article also discusses the opportunities that are available to Nepal to combat cybercrime. It highlights the potential for Nepal to become a hub for cyber security services in the South Asian region, which would provide significant economic benefits.*

*The government can also promote the development of a cyber-security industry by offering tax incentives, providing a favourable regulatory environment, and investing in cyber-security research and development. The article concludes by providing suggestions for the government,*

*businesses, and citizens to tackle cybercrime effectively. It emphasises the need for raising awareness about cyber threats, strengthening the legal framework for cybercrime, investing in cyber security education and training, and enhancing international cooperation on cybercrime. Ultimately, the article stresses the importance of a collaborative effort between the government, businesses, and citizens to tackle cybercrime effectively and ensure the safety and security of Nepal's digital infrastructure.*

***Keywords**: Cybercrime, Nepal, Security, Awareness, Legal framework, Cyber-attacks.*

## 1. INTRODUCTION

Cybercrime has become a significant problem in Nepal. As more and more Nepalese people and businesses rely on digital technology, the threat of cybercrime has increased. Cybercrime can have a devastating impact on individuals, businesses, and the economy. The best role in cybercrime is played by computers and devices connected to the internet. The advent of computers has revolutionised our ability to handle and manage information. With their innovative mechanisms, computers have significantly expanded our capacity to store, search, retrieve, and communicate data, making it easier than ever before to access information. As a result, we can now connect with anyone, anywhere in the world, at any time, thanks to the unparalleled accessibility provided by this technology. The General Assembly of the United Nations, by resolutions dated January 30, 1997, followed the version of the Law on Electronic Commerce permitted by the United Nations Commission on International Trade Law[1]. The term "cybercrime" is on the lips of almost everyone concerned with the use of computers and the Internet, whether individual, corporate, organisation, national, multinational, or international. Cybercrime is a type of criminal activity that takes place in the digital world, targeting computers, networks, and other digital devices. It refers to any illegal activity that is carried out using the internet, such as hacking, identity theft, phishing, ransomware attacks, and the distribution of malware. With the rapid advancement of technology and the widespread use of the internet, cybercrime has become a significant threat to individuals, businesses, and governments worldwide. Cybercrime is a word generated with a mix of two words, i.e., cyber and crime, where cyber refers to the subject, which describes anything related to computers, information technology, and the internet, and crime refers to an unlawful act that is punishable by law. So, in combing both words, cybercrime can be referenced as the use of a computer for performing any unlawful act that is publishable by law[2]. One of the primary motivations behind cybercrime is financial gain. Cybercriminals target individuals and organisations in order to steal sensitive information such as credit card numbers, bank account details, and personal identification information. They may use this information to commit financial fraud, such as making unauthorised purchases or transferring money from victims' accounts. Other motivations



[1] DR. J.N.BAROWALIA & DR AARUSHI JAIN., CYBER LAW & CYBER CRIMES (Vinod Publications 2022).
[2] Bivek Chaudhary, What does it take to control cybercrime in Nepal?, ONLINE KHABAR (April 12, 2023, 5:00 PM) https://english.onlinekhabar.com/cybercrime-in-nepal-cyber-crime-laws.html

LUJ | Legal Upanishad Journal
www.lujournal.com
info@lujournal.com

for cybercrime include political activism, espionage, and cyber terrorism. The impact of cybercrime can be devastating. It can cause financial losses, damage to reputation, and loss of privacy for victims. In addition, cybercrime can also have wider social and economic impacts, such as the disruption of critical infrastructure, the spread of disinformation, and the erosion of trust in digital technologies.

Nepal, like many countries around the world, faces significant challenges in addressing the issue of cybercrime. The increasing use of digital technologies, combined with the growing sophistication of cybercriminals, has made it more challenging for law enforcement agencies and policymakers to keep up with the evolving threat landscape. One of the primary challenges in addressing cybercrime in Nepal is the lack of awareness and understanding among the general public. Many individuals and businesses in Nepal are not aware of the risks associated with using digital technologies or the steps they can take to protect themselves from cybercrime. This lack of awareness makes them more vulnerable to cyber-attacks and makes it more challenging for law enforcement agencies to investigate and prosecute cybercriminals. Another challenge to addressing cybercrime in Nepal is the lack of technical expertise and resources. Law enforcement agencies in Nepal may not have the necessary tools, training, or expertise to investigate and prosecute cybercrimes effectively. Moreover, the lack of resources makes it difficult to implement cyber security measures, such as firewalls, encryption, and intrusion detection systems. Furthermore, Nepal's legal framework for addressing cybercrime is still in the early stages of development. While Nepal has enacted laws to address cybercrime, such as the Electronic Transactions Act[3] and the Information Technology Act, these laws may not be sufficient to address the evolving threat landscape adequately. The lack of clear legal frameworks can make it challenging for law enforcement agencies to investigate and prosecute cybercriminals effectively. Despite these challenges, Nepal also has several opportunities to address cybercrime effectively. The increasing adoption of digital technologies in Nepal has led to the emergence of a growing cybersecurity industry, providing an opportunity to build technical expertise and resources to address cybercrime. Moreover, Nepal's strategic location and growing economy can make it an attractive destination for multinational corporations, making it necessary to develop robust cybersecurity measures to protect against cyber threats. Another



[3] Electronic Transactions Act, 2063 (2008)

opportunity for Nepal is to develop international partnerships to address cybercrime. The country can benefit from collaboration with other countries, organisations, and international bodies to develop and implement effective cybersecurity measures. Such partnerships can also provide access to resources, expertise, and training, which can help strengthen Nepal's capacity to address cybercrime.

## 2. THE CURRENT STATE OD CYBER CRIME IN NEPAL

The current state of cybercrime in Nepal is concerning as it is increasing rapidly. Since the advent of technology in Nepal, cybercrime has become a major issue, and many web-based crimes have been committed in Nepal. As the Britannica Encyclopaedia states, cybercrime is 'the use of a computer as an instrument or device to further illegal ends or to perform any illegal activity, such as practising fraud, performing trafficking in child pornography, damaging intellectual property, stealing identities or personal information, or violating the privacy of the individual by leaking its privacy over the internet or networks. [4]As many cybercrime incidents occur, many go undetected or unreported, making it difficult to identify the exact number of incidents that occur. However, there have been several high-profile cases of cybercrime in Nepal that have been reported in the media.



In July 2013, a young woman fell victim to online swindling when she ended up transferring money for an online airline ticket booking. In October 2014, the first known case of cyberbullying was reported at the Kathmandu School of Law. In 2016, Nepal Police caught an 18-year-old operating in the name of Anonymous #Opnep for hacking government websites and defacing them, including the websites of Nepal Telecom and the National Tuberculosis Centre. In June 2017, the official website of the Department of Passports of Nepal was hacked by a group of Turkish hackers and defaced with a threatening note to reveal the government's data. In July 2017, 58 government websites were reportedly hacked by a group called 'Paradox Cyber Ghost,' making it one of the biggest data breaches of all time in Nepal. In October 2017, the SWIFT system of NIC Asia Bank was reportedly hacked by an unidentified hacker. They

[4] 16 HUGH CHISHOLM, THE ENCYCLOPEDIA BRITANNICA (Forgotten Books 2018)

intercepted USD 4.4 million from user accounts in six different countries. The bank claimed they recovered about USD 4 million. In November 2017, Onlinekhabar.com, one of the most popular online news portals in Nepal, was accessed by a third party to install a JavaScript mining application to mine a crypto Currency called Monero. In March 2020, a hacker using the Twitter handle Mr. Mugger hacked and dumped the data of 50,000 users of Foodmandu, including names, mailing addresses, email addresses, and phone numbers. In April 2020, customer data of more than 160,000 Vianet Communication customers was leaked. A hacker using the Twitter handle Narpichas @paapi_kto_mah made public data that included customers' emails, phone numbers, and addresses. This was the second-biggest data breach in Nepal. On April 15, 2020, a group of hackers managed to gain unauthorised access to web pages and data systems in Nepal, launching a cyber-attack. They gained access to the .np domain of Mercantile Communications Pvt. Ltd. These cases of cybercrime highlight the need for stronger cybersecurity measures and greater awareness of cyber threats among individuals and organisations in Nepal. On January 26, Nepal Server data was leaked on the dark web[5]. Likewise, recently in 2023, on April 17, a 21-year-old engineering student named Sagar Dhakal was arrested for allegedly hacking the Nepal Army website[6].



Cybercrime can have a huge impact on people, companies, and the economy. When it comes to individuals, cybercrime can lead to a loss of money, identity theft, and personal data breaches. This can have serious repercussions, such as damaging one's credit score or reputation. It can also cause emotional stress and make people hesitant to use online systems. For businesses, the impact of cybercrime can be devastating. It can result in significant financial losses, lost revenue due to downtime, and harm to the company's reputation. Additionally, cybercrime can result in the theft of sensitive data, which can negatively impact a company's competitiveness and market position. In some cases, cybercrime can even lead to a business shutting down. Cybercrime also has a significant impact on the economy. It can lead to direct costs, such as the expenses of investigating and remediating the attack, as well as lost revenue due to downtime. Indirect costs include lost productivity and innovation, a decrease in online activity due to a lack of trust, and

[5] Nepal Police Server Hacked, THE NEPALI POST (April 12, 2023, 4:30 PM) https://thenepalipost.com/details/29570
[6] 21-year-old engineering student arrested on the charge of hacking the Nepal Army website, ONLINE KHABAR (April 12, 2023, 6:00 PM) https://english.onlinekhabar.com/nepal-army-website-hacked.html

other negative consequences. Overall, cybercrime is a serious threat that should not be taken lightly. It is crucial to take preventative measures to protect against cybercrime, such as using strong passwords, keeping software up-to-date, and being cautious when sharing personal information online.

## 3. TYPES OF CYBERCRIME PREVALENT IN NEPAL

There are various types of cybercrime that are prevalent in Nepal. Some of the most common types of cybercrime in Nepal are as follows:

a. **Hacking**: Hacking is one of the most common types of cybercrime in Nepal. Cybercriminals hack into computer systems, networks, or websites to gain unauthorised access to sensitive information or to cause damage to the system.

b. **Identity Theft:** Identity theft is another common type of cybercrime in Nepal. Cybercriminals steal personal information, such as social security numbers, credit card numbers, and other sensitive data, to commit fraud and other illegal activities.



c. **Phishing**: Phishing is a type of cybercrime that involves sending fraudulent emails or messages to individuals in an attempt to obtain sensitive information, such as login credentials or financial information.

d. **Online Scams**: Online scams are also prevalent in Nepal. Cybercriminals use fake websites, online marketplaces, and social media platforms to scam individuals into paying for products or services that do not exist.

e. **Cyberbullying:** Cyberbullying is a form of online harassment that involves the use of digital technologies to harm, intimidate, or humiliate individuals. It is a growing concern in Nepal, especially among young people.

f. **Cyberstalking:** Cyberstalking is a type of cybercrime that involves the use of technology to track and monitor an individual's online activities. This can include sending threatening messages or harassing the individual through social media or other digital platforms.

g. **Cyber Terrorism**: Cyber terrorism involves using technology to cause fear and panic among individuals or society at large. This can include hacking into critical infrastructure systems or causing disruptions to online services.

## 4. CHALLENGES FACED BY NEPAL IN TACKLING CYBERCRIME

Nepal is among the countries struggling with the challenge of combating cybercrime. This is a global problem that has severe economic and social consequences for many nations around the world. One of the significant challenges is the lack of appropriate legal frameworks. The current laws in Nepal do not cover cybercrime comprehensively, which makes it easy for cybercriminals to exploit legal loopholes and operate without fear of prosecution. Therefore, the government needs to update existing laws and create new ones that address cybercrime effectively. Another major challenge is the limited capacity of law enforcement agencies. Many agencies in Nepal lack adequate training, expertise, and resources to deal with cybercrime effectively. Cybercrime is continually evolving, and it is crucial for law enforcement agencies to stay updated with the latest trends and techniques used by cybercriminals. The government must invest in training and provide adequate resources to law enforcement agencies to combat cybercrime effectively. The majority of Nepalese people lack awareness of cybercrime and the potential risks of using the internet. This exposes them to various cyberthreats and makes them vulnerable to cybercrime. Additionally, there is limited public awareness of the legal remedies available to victims of cybercrime. The government must conduct awareness campaigns to educate the public on the risks of cybercrime and the legal remedies available to victims. Limited cooperation between stakeholders is also a significant challenge. Effectively combating cybercrime requires collaboration between various stakeholders, including law enforcement agencies, the private sector, and civil society. However, in Nepal, there is limited cooperation between these stakeholders, making it challenging to share information and coordinate efforts to combat cybercrime effectively. The government must facilitate dialogue and cooperation between the various stakeholders to combat cybercrime effectively.

Nepal also faces a shortage of experts in the field of cybersecurity. Cybercrime involves the use of sophisticated technology, and it is essential for the government to have the necessary technical expertise to investigate and prosecute cybercriminals. However, Nepal faces a shortage of experts in the field of cybersecurity, making it difficult to investigate and prosecute cybercriminals. The government must invest in developing the necessary technical expertise to combat cybercrime effectively. Lastly, Nepal faces limited international cooperation in combating cybercrime. Cybercrime is a global phenomenon, and it requires international cooperation to combat it effectively. However, Nepal faces limited international cooperation in combating cybercrime, making it difficult to investigate and prosecute cybercriminals who operate from other countries. The government must establish bilateral and multilateral agreements with other countries to combat cybercrime effectively. Nepal faces numerous challenges in combating cybercrime, including the lack of appropriate legal frameworks, limited capacity of law enforcement agencies, inadequate public awareness, limited cooperation between stakeholders, limited technical expertise, and limited international cooperation.



If the challenges faced by Nepal in tackling cybercrime are not addressed, it could lead to severe consequences. One of the major consequences is an increase in cybercrime. If the legal frameworks are not updated, law enforcement agencies lack adequate training and resources, and public awareness is not raised, it will be easier for cybercriminals to operate in Nepal. This could result in an increase in cybercrime-related incidents, which could harm individuals, businesses, and the economy. Another consequence of not addressing these challenges is the loss of revenue. Cybercrime can cause significant economic damage. Businesses can suffer losses due to data breaches, intellectual property theft, and financial fraud. Without effective measures in place to tackle cybercrime, the Nepalese economy could suffer as businesses face financial losses. Furthermore, Nepal's reputation could be at risk if it fails to combat cybercrime effectively. This could deter foreign investment and tourism, which could harm the country's economy in the long run. Additionally, cybercrime can result in the violation of individuals' privacy. Cybercriminals can access personal data and use it for malicious purposes. If the government fails to take the necessary measures to combat cybercrime, individuals' personal data could be exposed, leading to significant harm. Cybercrime can pose a national security threat as cybercriminals can target critical infrastructure, such as government systems, energy grids, and financial institutions. If

cybercrime is not tackled effectively, it could compromise Nepal's national security and leave the country vulnerable to cyberattacks.

## 5. OPPORTUNITIES TO COMBAT CYBERCRIME IN NEPAL

Nepal has several opportunities to combat cybercrime effectively. One of these opportunities is strengthening legal frameworks. Nepal can update its laws and regulations related to cybercrime to create a legal framework that can effectively prosecute cybercriminals and prevent cybercrime activities. Another opportunity is to enhance the capabilities of law enforcement agencies to tackle cybercrime effectively. This can be achieved through training programmes, the provision of resources, and specialised cybercrime investigation units. Public awareness campaigns can also be an effective tool for combating cybercrime. Nepal can initiate such campaigns to educate citizens on the risks associated with cybercrime and how to protect themselves from cyberattacks. Additionally, Nepal can collaborate with other countries to share information and best practises in combating cybercrime. Private-public partnerships can also be leveraged to combat cybercrime. Private sector organisations can provide expertise, technology, and resources to support the government in combating cybercrime. Nepal can invest in research and development to develop new technologies and solutions that can help in preventing and detecting cybercrime activities. By taking advantage of these opportunities, Nepal can create a safe and secure cyber environment that supports its economic growth and national security. Nepal has several opportunities to combat cybercrime effectively. By leveraging legal frameworks, law enforcement capabilities, public awareness campaigns, international cooperation, private-public partnerships, and research and development, Nepal can successfully combat cybercrime and ensure a secure cyber environment for its citizens.



In addition to the opportunities mentioned above, Nepal can also establish partnerships with academic institutions to enhance research on cybercrime. This can help in developing new technologies and solutions that can help in preventing and detecting cybercrime. The government can also invest in building a skilled workforce in the field of cybersecurity through educational programmes and training. Nepal can also consider establishing a dedicated agency or task force

to combat cybercrime. This agency can be responsible for coordinating efforts to prevent, investigate, and prosecute cybercrime activities. It can also work in collaboration with other government agencies, law enforcement, the private sector, and international partners to combat cybercrime effectively. Moreover, Nepal can implement cybersecurity audits and assessments for businesses and government organisations. This can help in identifying vulnerabilities in their systems and networks and developing measures to prevent cyberattacks.

## 6. CONCLUSION

Cybercrime is a serious concern in Nepal that requires a comprehensive and collaborative approach to be effectively addressed. While Nepal faces challenges such as limited resources, inadequate legal frameworks, and a lack of public awareness, the country has opportunities to strengthen its response through initiatives such as enhancing law enforcement capabilities, implementing awareness campaigns, fostering public-private partnerships, and promoting international cooperation. By taking advantage of these opportunities and bringing together key stakeholders from the government, private sector, academia, and civil society, Nepal can make significant progress in tackling cyber threats. It is critical that Nepal prioritise building cybersecurity capacity across technical, legal, and social domains. With a robust national cybersecurity strategy, sufficient investment, and proactive efforts, Nepal can aim to create a safe, secure, and resilient digital environment that supports national security and economic growth. Though addressing cybercrime is a formidable challenge, Nepal is in a position to make advancements in cybersecurity that safeguard its citizens, businesses, and critical infrastructure from escalating cyber risks.