VOLUME 4 | ISSUE 1

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

NEPALESE JUDICIARY'S VITAL ROLE IN COMBATING CYBERCRIME: CONFRONTING CHALLENGES, EMBRACING OPPORTUNITIES, AND CHARTING FUTURE PATHWAYS

- Dr. Newal Chaudhary[1]

Abstract:

As the world becomes increasingly digitized, cybercrime has emerged as a major threat to the security and well-being of individuals, organizations, and nations. The need for an effective response to cybercrime has led to the development of legal frameworks and policies, with the judiciary playing a central role in their implementation and enforcement. This journal article aims to explore the critical role of the judiciary of Nepal in combating cybercrime. It examines the various challenges faced by the judiciary of Nepal in dealing with cybercrime, including jurisdictional issues, lack of technical expertise, and the rapid evolution of cyber threats.The article also analyze to discuss the opportunities available to the judiciary of Nepal to effectively combat cybercrime, including increased collaboration with law enforcement agencies, the development of specialized cyber courts, and the use of innovative legal approaches, such as the application of artificial intelligence in cybercrime investigations.Finally, the article considers the future directions of the judiciary's role in combating cybercrime, including the need to adapt to emerging cyber threats and the development of international legal frameworks to address transnational cybercrime.The article identifies the lack of technical expertise as a significant challenge faced by the Nepal judiciary in dealing with cybercrime. The article suggests that the judiciary needs to develop specialized cyber courts and increase collaboration with law enforcement agencies to effectively combat cybercrime. The article also highlights the use of innovative legal approaches, such as the application of artificial intelligence in cybercrime investigations.Overall, this article provides a comprehensive analysis of the critical role of the

[1] Advocate, Supreme Court of Nepal ; Assistant Professor , Nepal Law campus, Tribhuvan University, Exhibition Road, Kathmandu, Nepal.

judiciary of Nepal in combating cybercrime and offer insights into how the judiciary can effectively tackle this growing challenge.

Keywords: Hacker, Judiciary, cybercrime, internet.

Introduction:

In recent years, the digitization of the world has revolutionized the way people live, work, and communicate. Cybercrime is crime performed through online access of the internet as by using computer or any devices connected with internet.According to Katyal, cybercrime can be defined as the use of a computer to perpetrate or facilitate a criminal offense either through electronic attacks on the computer or network devices or by using the computer to commit traditional crimes[2].However, the increased reliance on digital technology has also brought about a new set of challenges, including cybercrime. Cybercrime has become a major threat to the security and well-being of individuals, organizations, and nations. Nepal, like many other countries, has seen a significant rise in cybercrime incidents in recent years. To combat this growing challenge, an effective response is necessary, which requires the development of legal frameworks and policies. The Nepalese judiciary plays a crucial role in implementing and enforcing these legal frameworks and policies. The judiciary plays a critical role in combating cybercrime in Nepal. Cybercrime is a complex and ever-evolving phenomenon that poses significant challenges to law enforcement agencies and policymakers. Cybercrime can affect individuals, organizations, and the nation's security and economic well-being.In 1997, the United Nations General Assembly adopted the Law on Electronic Commerce, which was previously approved by the United Nations Commission on International Trade Law[3]. Since then, the term "cybercrime" has become a common topic of discussion among individuals, corporations, organizations, and governments at the national, multinational, and international levels, particularly in relation to the use of computers and the Internet.Likewise, judiciary plays a crucial role in implementing and enforcing legal frameworks and policies to combat cybercrime. This includes investigating and prosecuting cybercrime cases, providing legal redress to victims, and ensuring the rule of law is upheld in the digital space. The judiciary also plays a vital role in shaping legal and policy frameworks to address emerging

[2]KATYAL, CRIMINAL LAW IN CYBERSPACE, at 12-13, (2001).
[3] J.N.BAROWALIA (DR.) et al., CYBER LAW & CYBER CRIMES, at 411, (1st ed. 2022).

cyber threats and ensure that they align with international norms and standards. In addition, the judiciary's role in combating cybercrime is critical in maintaining public trust and confidence in the justice system. As cybercrime becomes more prevalent, the public expects the judiciary to provide effective responses to combat cyber threats and protect their rights and interests in the digital space. The judiciary's ability to deliver timely and fair justice in cybercrime cases can have a significant impact on the public's perception of the justice system's efficacy and legitimacy. The importance of the judiciary in combating cybercrime cannot be overstated. The judiciary's role goes beyond legal enforcement, as it also contributes to building public awareness, promoting research and innovation, and enhancing cooperation and coordination among different stakeholders. By ensuring that the rule of law is upheld in the digital space, the judiciary can play a significant role in safeguarding Nepal's national security, economic prosperity, and public welfare. However, the rapidly evolving nature of cyber threats and the lack of technical expertise and jurisdictional challenges pose significant challenges to the judiciary's efforts. Despite these challenges, the judiciary has the opportunity to effectively combat cybercrime by collaborating with law enforcement agencies, developing specialized cyber courts, and utilizing innovative legal approaches, such as artificial intelligence.This journal article provides a comprehensive analysis of the critical role of the Nepalese judiciary in combating cybercrime, highlighting the challenges, opportunities, and future directions for the judiciary to effectively tackle this growing challenge.

Challenges faced by the Nepalese judiciary in combating cybercrime:

The Nepalese judiciary faces several challenges in combating cybercrime, including jurisdictional issues, lack of technical expertise, rapid evolution of cyber threats, and insufficient legal frameworks and policies. It is often stated by McConnell International that cybercrimes are. “Harmful acts which are committed from as or against a computer or a networks or networking devices with modes of internet[4]. Cybercrime is a complex and technical field, requiring specialized knowledge and expertiseCybercrime is a growing threat globally, and Nepal is no exception. Jurisdictional issues arise when cybercrime is committed across borders, and the perpetrator and victim are located in different countries. This makes it difficult for the Nepalese judiciary to investigate and prosecute such cases effectively. Additionally, the rapid evolution of cyber threats means that the judiciary must constantly

[4] McConnell, International LLC 1 (2000).

adapt to new methods used by cybercriminals to avoid detection and prosecution.The lack of technical expertise is another significant challenge faced by the Nepalese judiciary. Although the constitution grants the right to privacy, it seems impractical to expect complete privacy on the internet as, India has robust laws to regulate and penalize cybercrime offenders, in Nepal, cybercriminals either remain unpunished or face nominal consequences[5].The judiciary often lacks this technical expertise, making it challenging to investigate and prosecute cybercrime cases effectively. Furthermore, the judiciary may not have access to the latest technological tools and resources necessary to tackle cybercrime effectively.Another challenge faced by the Nepalese judiciary in combating cybercrime is the insufficient legal frameworks and policies. Cybercrime laws and policies may not be adequately updated to address the rapidly changing nature of cyber threats. There may also be gaps in the legal framework, making it difficult to prosecute cybercriminals. Furthermore, there may be inconsistencies in the interpretation and application of cybercrime laws by the judiciary, leading to further confusion and difficulties in prosecuting cybercrime cases.Overall, these challenges highlight the need for the Nepalese judiciary to prioritize the development of technical expertise, access to technological resources, and a robust legal framework to combat cybercrime effectively.Nepal has enacted several laws to combat cybercrime, including the Electronic Transaction Act, 2063, The Computer Crime Act, 2064, and The National Information and Technology (NIT) Policy, 2075. The Electronic Transaction Act, 2063 provides a legal framework for electronic transactions, recognizes electronic records as legal evidence, and defines cybercrime offenses such as unauthorized access, hacking, and online identity theft. The Computer Crime Act,2064 criminalizes computer-related offenses such as unauthorized access to computer systems, interception of data, and dissemination of computer viruses. The NIT Policy, 2075 provides a strategic framework for the development and promotion of Nepal's information and communication technology (ICT) sector, including measures to enhance cyber security and combat cybercrime.While the laws governing cybercrime in Nepal exist, the judiciary faces several challenges in effectively combating cybercrime. The challenges include the lack of technical expertise, resources and infrastructure, rapid evolution of cyber threats, and challenges related to international cooperation and cross-border cybercrime. Addressing these challenges will require a multi-stakeholder approach, including collaboration between the

[5] Chaudhary Bivek. "Cybercrime in Nepal: Cyber Crime Laws." Online Khabar English. Accessed February 23, 2023. https://english.onlinekhabar.com/cybercrime-in-nepal-cyber-crime-laws.html.

judiciary, law enforcement agencies, and other stakeholders. Moreover, investing in technical capacity building, resource mobilization, and international cooperation can help enhance the judiciary's ability to effectively combat cybercrime in Nepal.

Opportunities available to the Nepal judiciary to combat cybercrime:

The rise of cybercrime has created new challenges for law enforcement agencies and the judiciary in many countries, including Nepal. Cybercrime involves the use of computers, networks, and the internet to commit crimes such as identity theft, fraud, hacking, and cyberbullying. As cybercrime in today sense are only seen in privacy. Violation of privacy is equals to rise of cybercrime but in real sense it different. Somehow as in today's worlds people use social media , sometime there social get hacks and their internal and external privacy gets reviled and which directly makes connection with cybercrime Dignity is the quintessential quality of a personality, for it is highly cherished value[6]. Cybercrimes are complex and require specialized knowledge and expertise to investigate and prosecute. Formulating laws is not always an option for combating cybercrime. In regard with laws there should be the clear observation what opportunities the country can create in order to control the additional rising negative and positive effect of cybercrime. Cyber-attacks can threaten finical system in regard with privacy of individuals or any state. The rapid development of information and communication technologies over the past decade has revolutionized both business and individual practices. While there are challenges to combating cybercrime in Nepal, the judiciary has opportunities available to it to improve its capacity to tackle this problem. As the opportunities can be illustrated as:

A. **Technology**:

One of the key opportunities for the Nepalese judiciary is the use of technology. Technology has great role in facilitating traditional crimes such as organized crime, drug trafficking, and human trafficking[7]. Technology as it stands for the application of scientific knowledge for practical purposes, especially in industry. It includes a wide range of tools, systems, and devices that are designed to help individuals and organizations accomplish various tasks more efficiently and effectively.Technology is

[6] J.N. BAROWALIA, &A JAIN, CYBER LAW AND CYBER CRIME. New Delhi: Vinod Publication,at 176, (2021).

[7] "The Routledge Handbook of Technology, Crime and Justice" edited by M. R. McGuire and Thomas J. Holt.

made through a process of research and development, which involves the application of scientific knowledge to create new tools, systems, and devices. This process typically starts with an idea or a problem that needs to be solved. Researchers then study the problem and gather information to help them develop potential solutions.Once researchers have identified a potential solution, they begin to create a prototype or a model of the technology. This prototype is then tested and refined until it meets the necessary specifications and requirements. Throughout this process, researchers may also seek feedback from potential users and stakeholders to ensure that the technology meets their needs.After the prototype has been refined and tested, it is ready for production. This involves scaling up the production process to create a larger number of the devices or tools. In some cases, the technology may need to be modified or adapted to suit the specific needs of different users or markets.Once the technology has been manufactured, it is typically marketed and distributed to potential users. This entails figuring out the goal marketplace and growing an advertising approach to attain the ones users. The technology may be sold through various channels, such as retail stores or online marketplaces.Overall, the process of creating technology is a complex and iterative one that involves multiple stages of research, design, development, and testing. It requires a team of skilled researchers, engineers, and designers working together to bring new ideas to life and solve the problems of our modern world.The judiciary can leverage technology to improve its ability to investigate and prosecute cybercrime cases. This includes adopting advanced digital forensics tools and software to collect and analyze digital evidence. The judiciary can also use technology to facilitate online dispute resolution, which can improve the efficiency and accessibility of the justice system.

B. Collaboration:

Collaboration is another important opportunity for the Nepalese judiciary to combat cybercrime effectively. Cybercrime is a complex and evolving threat that requires a coordinated and multidisciplinary approach to address. By working with other stakeholders, such as law enforcement agencies, government departments, and the private sector, the judiciary can pool resources, share information, and develop strategies to combat cybercrime more effectively.For instance, law enforcement agencies can provide the judiciary with the necessary technical expertise and investigative skills to help

prosecute cybercriminals. Government departments can offer support in terms of policy development, regulation, and funding, while the private sector can provide insights into emerging threats and potential vulnerabilities. Collaboration with civil society organizations can also help to raise awareness of the risks associated with cybercrime and educate citizens about how to protect themselves.In addition to collaborating with other stakeholders, the Nepalese judiciary can also work to strengthen international cooperation in combating cybercrime. This involves developing relationships with law enforcement agencies and other stakeholders in other countries to share information and coordinate efforts to combat cybercrime on a global scale.To facilitate collaboration, the Nepalese judiciary can establish partnerships, networks, and working groups that bring together stakeholders from various sectors. These partnerships can facilitate the sharing of information and expertise, as well as the development of joint initiatives and programs. Collaboration presents a significant opportunity for the Nepalese judiciary to combat cybercrime more effectively. By working with other stakeholders, including law enforcement agencies, government departments, and the private sector, the judiciary can pool resources, share information, and develop strategies to address the challenges posed by cybercrime. By embracing collaboration, the Nepalese judiciary can build a stronger, more resilient response to cybercrime that is grounded in a coordinated and multidisciplinary approach.

C. Capacity building:

Capacity building is another important opportunity available to the Nepalese judiciary to combat cybercrime. The judiciary can invest in training and development programs that focus on cybercrime investigation and prosecution. By providing training to judges, prosecutors, and other stakeholders, the judiciary can improve its expertise in this area and ensure that stakeholders are better equipped to handle cybercrime cases. The training can focus on different aspects of cybercrime, such as cybercrime investigation, digital forensics, and cyber law. This can help to bridge the technical knowledge gap that exists among some stakeholders and ensure that they have a deeper understanding of the challenges posed by cybercrime. In addition, the training can help to develop best practices and guidelines for handling cybercrime cases. This can include developing protocols for the collection and preservation of digital evidence, establishing standard

procedures for cybercrime investigations, and providing guidance on how to handle different types of cybercrime. Moreover, the judiciary can also work to raise awareness of cybercrime and its impact on society. This can include developing educational programs for the public, particularly vulnerable groups such as children and the elderly. By educating citizens about cybercrime and how to protect themselves, the judiciary can play a proactive role in preventing cybercrime from occurring in the first place. Capacity building is an important opportunity for the Nepalese judiciary to combat cybercrime more effectively. By providing training on cybercrime investigation and prosecution, the judiciary can improve its expertise in this area and ensure that stakeholders are better equipped to handle cybercrime cases. The judiciary can also work to raise awareness of cybercrime and its impact on society, thus playing a proactive role in preventing cybercrime. By embracing capacity building, the Nepalese judiciary can build a stronger, more resilient response to cybercrime that is grounded in expertise and knowledge.

D. Legal framework:

Improving the legal framework for combating cybercrime is another important opportunity available to the Nepalese judiciary. The existing laws in Nepal may not be fully equipped to address the constantly evolving nature of cybercrime. As Nepal has laws that deals with cybercrime i.e. The Electronic Transaction Act,2063 seems more to be amended,observing the various section, as in Section 46, it has criminalized the act of damaging any computer and information system. If any person knowingly and with a mala-fide intention to cause wrongful loss or damage to any institution destroys, damages, deletes, alters, disrupts any information of any computer source by any means or diminishes value and utility of such information or affects it injuriously or causes any person to carry out such an act, such a person shall be liable to the punishment with the fine not exceeding two thousand rupees and with imprisonment not exceeding three years or with both[8], but it may not address all forms of cyber extortion, such as ransomware attacks and distributed denial-of-service (DDoS) attacks. Seeing today's areas DDos is the rising cybercrime in today's history. Recently in 2023,all the government websites being attacked simultaneously and those website were down which

[8] ELECTRONIC TRANSACTION ACT,Sec.46, 2063

affected the various national and international works of Nepal[9]. This was only one example of section 46 of present laws of Nepal, there are many sections which are in regard necessary to get amended. Therefore, the judiciary can take steps to review and update existing laws to ensure that they are relevant and effective in dealing with emerging cybercrime threats. This can involve identifying gaps and weaknesses in the current legal framework and taking steps to address them. For instance, the judiciary can work with lawmakers to amend existing laws or develop new ones that are better suited to deal with cybercrime. The laws should also take into account the specific challenges and nuances of investigating and prosecuting cybercrime. Furthermore, the judiciary can work to establish legal precedents in cybercrime cases. This can help to clarify legal standards and provide guidance to judges, prosecutors, and other stakeholders in future cases. Establishing legal precedents can also help to deter cybercriminals by sending a clear message that cybercrime will not be tolerated. In addition, the judiciary can also work to promote international cooperation and coordination in combating cybercrime. This can involve collaborating with other countries to develop and implement common legal frameworks, share intelligence, and provide mutual legal assistance in cybercrime investigations and prosecutions. In conclusion, improving the legal framework for combating cybercrime is an important opportunity for the Nepalese judiciary. By reviewing and updating existing laws, working with lawmakers to develop new laws, and establishing legal precedents, the judiciary can ensure that it is better equipped to deal with emerging cybercrime threats. By promoting international cooperation and coordination, the judiciary can also help to create a more cohesive and effective global response to cybercrime.

Future Directions for the Nepalese Judiciary in combating Cybercrime:

Modern Technology has enabled courts to enhance the quality and effectiveness of the administration of justice[10], but in modern technology is seeing in practice but still till 2023 its showing up in the area of cybercrime administration of justice is lacking behind. The future directions for the Nepalese judiciary in combating cybercrime will likely involve a

[9]"Government websites going down question Nepal's cyber security status" Online Khabar English. Last modified November 23, 2021. https://english.onlinekhabar.com/nepal-government-websites-down.html.

[10]J.N.BAROWALIA &A JAIN, CYBER LAW AND CYBER CRIME, New Delhi: Vinod Publication, at 17, (2021).

combination of the opportunities discussed earlier, such as capacity building, collaboration, and legal framework improvement. Additionally, emerging technologies and cybercrime trends will require the judiciary to adapt and innovate its approach to combatting cybercrime. In present time, the cases related with cybercrime are only heard in Kathmandu district court of Nepal. So one potential future direction is the development and implementation of specialized cybercrime courts or tribunals. The judiciary can establish specialized cybercrime courts to handle cybercrime cases.These specialized courts could be staffed with judges and prosecutors who have expertise in cybercrime investigation and prosecution, and could help to streamline and expedite cybercrime cases.Another direction could be the increased use of technology in the investigation and prosecution of cybercrime. This could include the use of advanced digital forensics tools and techniques, as well as the development of new technologies to combat emerging cybercrime threats.The judiciary may also need to work closely with other countries and international organizations to combat cross-border cybercrime.This will require the development of effective cooperation mechanisms, as well as the sharing of information and best practices.The use of innovative legal approaches, such as the application of artificial intelligence (AI) in cybercrime investigations, can also be taken as references as important in combating cybercrime. AI can assist in analyzing large amounts of data, identifying patterns and anomalies, and detecting potential threats. It can help law enforcement agencies and the judiciary to quickly identify and respond to cybercrime incidents.One example of AI being used in cybercrime investigations is the development of predictive policing algorithms. These algorithms can analyze data on previous cybercrime incidents and predict where future incidents are likely to occur. This information can be used to target resources and investigations more effectively.Another area where AI can be useful is in the analysis of digital evidence. AI can be trained to recognize patterns in data, such as images or text that may indicate the presence of criminal activity. This can help investigators to quickly identify relevant evidence and build stronger cases against cybercriminals.However, the use of AI in cybercrime investigations also presents some challenges. One concern is the potential for bias in AI algorithms, which can lead to unfair or discriminatory outcomes. Another challenge is the need for specialized expertise to develop and deploy AI systems in law enforcement and the judiciary.Despite these challenges, the application of AI in cybercrime investigations has the potential to significantly improve the effectiveness of law enforcement and the judiciary in combatting cybercrime. As technology

continues to evolve, it will be important for legal systems to keep pace and incorporate innovative approaches like AI to stay ahead of cybercriminals.Finally, it will be important for the judiciary to continue to raise awareness among the public about the risks and impacts of cybercrime. This could involve the development of targeted awareness campaigns and educational programs, as well as the promotion of safe and secure online practices.Overall, the future directions for the Nepalese judiciary in combating cybercrime will require a comprehensive and collaborative approach that leverages emerging technologies and best practices to address the evolving cybercrime landscape.

Conclusion:

To address the increasing issue of cybercrime in Nepal, it is recommended that the government establish a specialized agency, such as a cyber-police unit, to operate 24/7 and take immediate action against cybercriminals. However, it is important to ensure that this agency is well-equipped with skilled personnel and the necessary technological resources to effectively combat cybercrime. Moreover, the government should also focus on raising awareness among citizens about ways to protect themselves from becoming victims of cybercrime. It can be achieved through regular educational campaigns and hacker hunt operations, which can help to identify vulnerabilities in cyberspace and take appropriate measures to prevent cyber-attacks. In addition to establishing a specialized agency and promoting awareness among citizens, the government should also prioritize hiring skilled IT professionals to bolster their cybercrime-fighting capabilities. By ensuring that they have the necessary human resources, the government can better protect Nepalese citizens from cybercrime. It is important to note that while amending laws related to cybercrime is a step in the right direction, it is not sufficient in controlling cybercrime in Nepal. Aggressive and proactive steps, such as those outlined above, are necessary to effectively combat this issue and secure the cyberspace in Nepal.

In conclusion, cybercrime has become a major threat to Nepal's security and economic prosperity, and the Nepalese judiciary has a critical role to play in combating it. The challenges faced by the Nepalese judiciary in this regard are significant, including a lack of resources, technical expertise, and adequate legal frameworks. However, there are also many opportunities available, including collaboration with other stakeholders, capacity building through training, and improvements to the legal framework. Looking to the future,

the Nepalese judiciary must continue to adapt and evolve to meet the ever-changing landscape of cybercrime, through the establishment of dedicated cybercrime agencies, public awareness campaigns, and ongoing efforts to improve the legal framework. Ultimately, the success of these efforts will depend on theNepalese judiciary's ability to stay ahead of cybercriminals, and its commitment to upholding the rule of law in the digital age.