Curriculum on Cyber Crime

Co-ordinator

Hon. Tek Narayan Kunwar
Judge, High Court/Faculty Member, NJA

Members

Mr. Babu Ram Aryal, Advocate
Representative : Nepal Bar Association
Mr. Kedar Ghimire, Deputy Director, NJA
Mr. Rajesh Bastola, Officer, NJA

National Judicial Academy Nepal

Manamaiju, Kathmandu

Contents

Session 7	International laws and Conventions relating to cybercrime	
Session 8	Case Study Exercise	
Session 9	Institutions for Cyber Law Enforcement in Nepal and their Role	
Session 10	Investigation and Prosecution on Cybercrime and its Challenges	
Session 11	Cyber Security	
Session 12	Implementing the Cybercrime in Nepal: Panel Discussion	
Session 13	New Areas of Cyber Crime	
References		

Part I
Preliminary

1.1 Institutional Background

The National Judicial Academy is a statutory body established originally under the National Judicial Academy ordinance in 2004 which is now substituted by the National Judicial Academy Act, 2006. The National Judicial Academy works under the guidance of its Governing Council headed by the Chief Justice of Nepal. In the executive level, the Act provides for the Executive Committee which requires representation of all the justice sector actors i.e. the Supreme Court, the Ministry of Law and Justice, the Judicial Council, the Office of the Attorney General and the Nepal Bar Association. The rationale behind the establishment of the Academy is to work towards enhancing competence and professional development of judges, government attorneys, court officials and other officers of the Nepal Judicial Service and private law practitioners. The main functions of the NJA set out in the Act are to conduct training, workshop, seminar, interaction and symposium as per the need; undertake research and publish research works in the area of law and justice and to establish itself as a legal information centre and provide consultation and information service in the area of law and justice etc.

1.2 Introduction to the Course

Cyber law is one of the important branches of the law that basically deals with the cyber related issues and cyber space. It is one of the rapidly expanding and evolving areas of the law that basically deals internet, computer and other means of communication. The 21st century is marked with rapid evolution and development of the information, communication and technology throughout the world. Nepal being the part of the global system is heavily influenced and benefited with internet and cyberspace. However, cyberspace is not free from the threat and challenges.

Nepal enacted Electronic Transaction Act, 2063 was enacted basically to regulate electronic records and the electronic transaction however some sections of the act also tries to regulate some crimes related to computer and digital data but not the cyberspace as a whole

Cyber law being one of the nascent branches of the law with evolution and development of ICT throughout the globe and in the Nepalese context. Various kinds of crimes are being committed via internet and cyberspace. Against the backdrop, it is high time for the judges, private lawyers and public prosecutor to be well equipped with the various nuances of the cyber space and internet in the Nepalese context and global context. The course must contribute for the stakeholders to succinctly understand the various notions and principles of the cyberspace, cyber crime and cyber law to involved in the area of the law and justice.

1.3 Aims and Objectives of the Course

The aims and the objectives of the course will be as follows.

1.3.1 Aims

The main aim of the course is to make the participants confident on the subject matter while paying role either as a public prosecutor, defendant lawyer or judge.

1.3.2 Objectives

The main objectives of the curriculum are:

- To impart the theoretical and practical knowledge of cyber law and cyber crime in national and global context.
- To sensitize all the participants regarding the cyberspace, cyber law and cybercrime.
- To enhance the quality and understanding of the participants regarding principles and nuances of the cyberspace, cyber law and cybercrime.
- To familiarize stakeholders with the contemporary issues in the area of the cyberspace at national and international context.
- To impart knowledge regarding the existing relevant national legislations, foreign legislations and international instruments in the areas of the cyberspace and cybercrime.

1.4 Participation, Number of Participants and Duration of the Training

The training is specially designed for the private lawyers however the Judicial Academy also conduct training for the judges and public prosecutors on the basis of the curriculum. The participation, number of participants and the duration of the training will as following.

1.4.1 Participation

The private lawyers who currently are in practice will be the participants of the training.

1.4.2 Number of Participants

The number of participants for the training shall be 25

1.4.3 Training Duration

The duration of the training would be 5 days.

1.5 Structure of the Curriculum

The curriculum consists of two parts. The first part covers the preliminary contents of the curriculum such as introduction, aims, objectives, target group, and number of the participants, training duration etc. The second part of the curriculum is the vital part of the curriculum which encompasses modules and the sessions of the training.

1.6 Modules and Sessions of the Curriculum

Altogether the curriculum consists of 2 modules and 15 sessions.

1.7 Training Method and Evaluation of the Training

On the basis of the allocated budget the training can be conducted either residential or non residential form. While selecting the trainer/instructor of the training will be selected from the roster of the NJA according to the rules of the institution. The trainer should follow the adult training method while conducting the session. On the way of training the resource persons and the participants both will be evaluated. According to the necessity the pre-training evaluation, the post training evaluation, the session evaluation and the overall training evaluation will be conducted on the prescribed format of the institutions. The resource person will be evaluated

from the participants while the participants will be evaluated from the National Judicial Academy.

Part 2

Modules and Sessions

2.1 Module 1: Introductory

Session	Session Topics	Contents to be covered	Time	Training Methods
1.	Useful terminologies relating to cyber crime	• Computer • Read only memory (ROM) and Random Access Memory (RAM) • Hardware and Software • Operating System • Internet and intranet • Networking • Local Area Network (LAN), Metropolitan Area Network (MAN) and Wide Area Network (WAN) • Internet Service providers (ISPs) • Uniform Resource Locator(URL) • World Wide Web (WWW) • Domain Name and Domain Name System • Internet Protocol (IP) Address • Router/Switches/ Hubs • Browser • Internet of Things (IOT) • Virtual Private Network (VPN) • Cloud • Cloud Computing • Portable Document Format(PDF) • Hyper Text Markup Language (HTML) • Hyperlink • Bookmark • Cookie	1 Hour and 30 Minutes	

Session	Session Topics	Contents to be covered	Time	Training Methods
		• Encryption • Decryption • Firewall		
2.	Cyber Crime and Its Types	• Introduction • Types ○ based on affected party, ○ based on content, ○ based on people involved ○ based on role of computer • Based on affected party ▪ Against any individual- grooming, cyber stalking, phishing, dissemination of obscene material, defamation, hacking/cracking, morphing, Digital Defamation - Publication and republication, Ransomware ▪ Against property- transmitting virus, net trespass, mail bombing, Cyber crimes related with Intellectual Property, Software Piracy, Framing, Linking, Inlining, Domain Name Disputes, Cyber Squatting, Cyber Parasites etc. ▪ Against organization- possession of unauthorized information, Denial of Service (DOS), Distributed Denial of Service (DDOS), Distribution of pirated software, etc. ▪ Against society at large- Pornography especially child pornography, cyber terrorism etc,	1 Hour and 30 Minutes	

2.1 Module 2: Laws and Different Issues Relating to Cybercrime

Session	Session Topic	Contents to be covered	Time	Training Methods
1.	E-Commerce, E-consumers and related cyber crimes	• Concept of e-commerce • Type of e-commerce • Process of e-commerce • Opportunity and Risk • Consumer issues in e-commerce	1 Hour and 30 Minutes	
2.	Privacy and Data Protection	• Issues of Privacy in Cyber space • Digitization, personal data and data industry, Data protection principles • Conditions for processing of personal data • International guidelines for privacy protection: OECD principles • CCTV and RFID tracking • Privacy and Data protection in International Regime • Data protection practice on major jurisdiction • The Privacy Act, 2075 of Nepal	1 Hour and 30 Minutes	
3.	Electronic and Digital Evidence and its Recognition	• Electronic Evidence • Digital Evidence • Characteristics of Digital Evidence • Cyber forensic • Collection of Cyber Forensic • How they are transported • How they are analyzed • Admissibility of digital evidence in the court : International Perspective • Admissibility of digital evidence in the court of Nepal	1 Hour and 30 Minutes	
4.	Offence related to Intellectual Property	• Intellectual Properties in the Cyber Space • Domain Name Related Issues • Cybersquattng • Cyber Parasites • Software Piracy| Source Code Theft	1 Hour and 30 Minutes	

Session	Session Topic	Contents to be covered	Time	Training Methods
		Related Issues • Hard Disk Loading and Related Issues • Copyright Act, 2059 and Cyber Space • The Patent Design and Trademark Act, 2022 and Cyber Space • Cases Related to IP and Cyber Space in Nepal		
5.	Digital Freedom	• Access to Internet and Digital Rights • Freedom of expression • Misinformation and disinformation • Content liability on digital publication and fake news, Internet freedom and their limitation • Digital surveillance	1 Hour and 30 Minutes	
6.	National Laws, Policies and Regulations relating to Cybercrime	• Electronic Transaction Act, 2063 of Nepal • Electronic Transaction Rules, 2064 • Cyber Crime Related Provisions on the Penal Code of Nepal • Proposed Information Technology Bill of Nepal • Provisions related to cyber crime on other Laws of Nepal ○ The Criminal Code, 2074 ○ The Children's Act, 2075 ○ The Patent Design and Trademark Act, 2022 ○ Banking Offence and Punishment Act, 2064 ○ Copyright Act, 2002 ○ Consumer Protection Act, 2075 ○ Telecommunication Act, 2053		
7.	International laws and Conventions relating to	• Cyber crime related laws of ○ India, ○ USA, ○ UK,	1 Hour and 30 Minutes	

Session	Session Topic	Contents to be covered	Time	Training Methods
	cybercrime	○ China, ○ Singapore, • Key features of European Convention on Cyber Crime, 2001(Budapest Convention) • African Union Convention on Cyberspace Security and Personal Data Protection		
8.	Case Study Exercise	• Some cases are distributed prior a day to all participants by dividing participants into different groups. • The facilitator will ask the participant to present their views from each group regarding investigation, prosecution and execution of the cases.	1 Hour and 30 Minutes	
9.	Institutions for Cyber Law Enforcement in Nepal and their Role	• National Information Technology Centre • Internet Service Providers (ISPs) • Nepal Telecommunication Authority • Courts (Kathmandu District Court, High Court Patan and Supreme Court of Nepal) • Nepal Police (Cyber Bureau and Digital Forensic Lab) • Office of Attorney general • Controller of Certifying Authority • Computer Association of Nepal •	1 Hour and 30 Minutes	
10.	Investigation and Prosecution on Cybercrime and its Challenges	• Investigation process (steps) of the cyber crime cases • Method of live traffic data acquisition in the process of investigation • Digital forensic examination of the data and the hardware equipments • Call detail record tracing • Cooperation of other agencies while	1 Hour and 30 Minutes	

Session	Session Topic	Contents to be covered	Time	Training Methods
		investigating • International co-operation while investigating cybercrimes • Difficulties on investigating cyber crimes • Status or Cybercrime Prosecution in Nepal • Co-operation of victim and witness in cybercrime prosecution • Cooperation between investigating authority and prosecuting authority • Trend of judiciary while deciding cybercrime cases • Challenges on cybercrime prosecution • Way forward to mitigate the challenges of cybercrime prosecution in Nepal •		
11.	Cyber Security	• Introduction of Cyber Security • Cyber security and Information Security • Significance of host firewall and Ant-virus, • Management of host firewall and Anti-virus, • Wi-Fi security, • Configuration of basic security policy and permissions. • Setting and configuring two factor authentications in the Mobile phone. • Managing Application permissions in Mobile phone • Installation and configuration of computer Anti-virus. • Wi-Fi security management in computer and mobile • NIDC issue	1 Hour and 30 Minutes	

Session	Session Topic	Contents to be covered	Time	Training Methods
12.	Implementing the Cybercrime in Nepal : Panel Discussion	•	1 Hour and 30 Minutes	Discussion, Question and answers, suggestions and feedback.
13.	New Areas of Cyber Crime	• Artificial Intelligence • Machine Learning, • Big data, Robotics • Crypto currency • Digital cash etc	1 Hour and 30 Minutes	

References:

Laws and Regulations:

- Banking Offence and Punishment Act, 2064
- Consumer Protection Act, 2075
- Copyright Act, 2002
- Electronic Transaction Act. (2063)
- Telecommunication Act, 2053
- The Children's Act, 2075
- The Criminal Code, 2074
- The Patent Design and Trademark Act, 2022
- The Privacy Act. (2075).
- Cybersecurity Policy Draft. (2016)
- Proposed Information Technology Bill (2019)
- Some Public (Crime and Punishment) Act, 1970

International Legal Instruments:

- European Convention on Cyber Crime, 2001 (Budapest Convention)
- African Union Convention of Cyberspace, Security and Personal Data Protection

Text Books and Articles:

- Barkhu& Mohan U .(2006) Cyber Law and Cyber Crime. Asia Law House.
- Burt, D. et al. (2014) Cyber Security Risk Paradox, Microsoft security intelligence, Microsoft Corporation.https://cloudblogs.microsoft.com/microsoftsecure/2014/01/16/the-cybersecurity-risk-paradox-measuring-the-impact-of-social-economic-and-technological-factors-on-cybersecurity/.
- Duggal, P. (2019). Cyber Law: An exhaustive Section wise Commentry on The Information Technology Act along with Rules, Regulations, Policies, Notification etc. Lexis Nexis.
- International Telecommunication Union (2014). Understanding Cybercrime: Phenomena, Challenges and Legal Responses, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/cybercrime2014.pdf .
- Mann, R.J. (2011). Electronic Commerce. Wolter Kluwer Law and Business
- Nandan Kamath, Law relating to computers, internet and e-commerce: a guide to cyber laws and the information technology act, 2000 with rules, regulations and notification, Universal law publishing, Delhi, 2002.
- Paranjape V. (2010). Cyber Crime and Law. Central Law Agency.
- Reed, C & Angle J. (2014). Computer Law. Oxford University Press.
- Singh, Y (2019). Cyber Laws. Lexis Nexis.

Sobti, R., & Geetha, G. (2012). Cryptographic Hash functions - a review. *International Journal of Computer Science Issues, December*.

- Stephen E. Blythe, Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce With Enhanced Security, Richmond Journal of Law and Technology, Vol.11, Issue 2, 2005

- Verma, A. K. & Sharma, A. K. (2014). "Cyber Security Issues and Recommendations." *International Journal of Advanced Research in Computer Science and Software Engineering,* 4(4). 629-634.https://www.ijtsrd.com/papers/ijtsrd.

- Walstrom, M. (2016). "India's Electrical Smart Grid: Institutional and Regulatory Cybersecurity Challenges." https://jsis.washington.edu/news/indias-electrical-smart-grid-institutional-regulatory-cybersecurity-challenges/.