https://doi.org/10.3126/access.v2i01.59002
www.nepjol.info

Cyber-Attack Issues: Laws & Policies and the Role of Librarians

- Kedar Ghimire[1]

Article history: Received: 14 April, 2023; Reviewed: 22 August 2023; Accepted: 4 Sept. 2023.

Abstract

Cybersecurity is the practice of deploying people, policies, processes and technologies to protect organizations, their critical systems and sensitive information from digital attacks. Organizations have become far more vulnerable to cyber threats because digital information and technology are now so heavily integrated into day-to-day work. But the attacks themselves, which target both information and critical infrastructure, are also becoming far more sophisticated. In this scenario, this paper especially tries to trace out major attribute of cyber-attack, common cyber-attacks that are usually seen in Nepal and periphery, laws and policies related to cyber security in Nepal, how we can make the academic environment cyber safe. To cover these issues the study reviews the academic literature dealt with cyber security, cyber security policy, and role of libraries and librarian on the cyber security. Most of the research data are the primary sources of information i.e. articles of the research journals which have been published in the last few years either in hard copy or electronically. Qualitative research method has been applied for the study.

Keywords: *Cyber security, Cybercrimes, Cyber-attacks, Libraries*

1. Introduction:

This development of the information society offers great opportunities. Unhindered access to information can support democracy, as the flow of information is taken out of the control of state authorities. Technical developments have improved daily life, for example, online banking and shopping, the use of mobile data services and voice over Internet protocol (VoIP) telephony are just some examples of how far the integration of ICTs into our daily lives has advanced. However, the growth of the information society is

1. ***Kedar Ghimire*** *is Deputy Director at National Judicial Academy, Nepal. He can be contacted at <kedar_2222@yahoo.com>.*

accompanied by new and serious threats. Essential services such as water and electricity supply now rely on ICTs. Cars, traffic control, elevators, air conditioning and telephones also depend on the smooth functioning of ICTs. The ICTs with the combination of internet technology jointly create the complex environment that is cyberspace. Cyberspace refers to the virtual computer world, and more specifically, an electronic medium that is used to facilitate online communication. Cyberspace typically involves a large computer network made up of many worldwide computer sub-networks that employ TCP/IP (Transmission Control Protocol/Internet Protocol) protocol to aid in communication and data exchange activities. In other words the cyberspace describes any facility or feature that is linked to the Internet. Attacks against information infrastructure and Internet services which is also called cyberspace now have the potential to harm society in new and critical ways.

Online fraud and hacking attacks are just some examples of computer-related crimes that are committed on a large scale every day. The financial damage caused by cybercrime is reported to be enormous. Cyber crime is the biggest threat to the digital transformation and is estimated to cost economies about USD 10 trillion by 2025 (Maheshwari, 2022). Cyber crime reflects a peculiar type of techno-sophisticated criminality having different features. This criminality is posing the challenges to existing national legal system and it appears to be difficult to control and combat these crimes within the existing framework of legal system. Specially, the problem of jurisdiction, identity crises and lack of legal recognition of most of acts make it difficult for legal systems to deal effectively with the crime (Verma & Sharma, 2014). The location and trans-national character of these crimes again added the flavor makes it too dangerous to imagine. Cyber-crime may be categorized in two classes, one where the computer is an instrument and another where computer is an incidental (Cavelty, 2012). It is not difficult to control the cyber-crimes fall in former categories as here, computer is only an instrument and traditional legal system is better to cope up these problems by merely recognizing it, however, it is difficult to deal with the later class of criminality as computer technology is itself new to the legal system and it can't deal with the merely old principles which is territorially sensitive, jurisdictionally responsive, and susceptible to paper based culture and identity.

2. Attributes of Cyber-Attack:

We all are very familiar to the computer and internet directly or indirectly. Initially when man invented computer and then the internet technology for communicating between computers was evolved, he would have never thought that this cyber space could be misused for criminal activities and which required regulations. However, as we all know, everything has its pros and cons and so computers and internet are not an exception. Now almost all of us might have heard the term computer crime, cyber-crime, e-crime, hi-tech crime or electronic crime which is nothing but an activity done with a criminal intent in cyber space.

At the outset, it is necessary to briefly distinguish between a computer crime and a cyber-crime, the rationale being that more often times than not, the two concepts are regarded as one and same, when in fact they are only similar, but are definitely different (Verma & Sharma, 2014). Computer crimes, are those criminal acts perpetrated with the use of a computer; stated in other words, computer crimes includes crimes committed against the computer hardware, the materials contained or associated with the computer which includes the software and data; typical examples of computer crimes includes but not limited to embezzlement, fraud, financial scams and hacking etc. Cyber-crime is an umbrella term used to describe two distinct, but closely related criminal activities: cyber dependent and cyber-enabled crimes, the former are offences that can only be committed by using a computer, computer networks, or other form of ICT. These acts include the spread of viruses and other malicious software, and distributed denial of service (DDoS) attacks. Cyber-dependent crimes are primarily acts directed against computers or network resources, although there may be secondary outcomes from the attacks, such as fraud and the latter, cyber-enabled crimes, are traditional crimes that are increased in their scale or reach by the use of computers, computer networks or other ICT; this includes but not limited to fraud (including mass-marketing frauds, phishing e-mails and other scams; online banking and ecommerce frauds); theft (including theft of personal information and identification-related data); and sexual offending against children (ITU, 2016).

Due to dichotomies in jurisdictions and yet addressing the same concept in legal literature, cybercrimes to date, has no globally accepted definition that could possibly encapsulate all the facets of this novel brand of crime, the definitional problem of cybercrime subsists, but one thing that is certain is that most definitions of cybercrime make reference to the Internet; for the sake overcoming the lacuna, cybercrime has been defined as crime committed over the Internet which might include hacking, defamation, copyright infringement and fraud (Duggal, 2019). On this basis we can listed out the different attributes or characteristic of the cyber-attack.

2.1 Easy to commit, difficult to detect and even harder to prove: The cyber-attacks are easier to commit, difficult to detect and even much harder to prove compare to the physical attack. The preparations for cyber-attack are far less visible than that for conventional warfare. For the latter, preparations are usually evident through a military build-up and mobilization order which are easily detectable, but there are no visible signs of preparations when it comes to cyber-attacks.

2.2 Cyber Attacks are asymmetric: They do not require sophisticated weaponry, and neither do they have to build expensive platforms such as stealth fighters or aircraft carriers, in order to compromise the network of interest and pose a significant threat. Besides state actors, there are concerns that terrorists or organized criminal

groups could stage cyber-attacks that leverage on the low capital outlay required. Sometimes the cyber attackers are inside to territory while many times it may occur from anywhere and any point of the world as these types of attacks are borderless (Duggal, 2019). Even the aircraft and the drone can be controlled from the far remote location that can be used to destroy the human resources and the physical infrastructure as well.

2.3 No Geographical Border: In cyberspace the geographical boundaries reduced to zero. A cyber-criminal in no time sitting in any part of the world can commit crimes in other corner of world. For example, a hacker sitting in Singapore can hack in the system placed in United States.

2.4 Virtual World: The act of cyber-crime takes place in the cyber space and the criminal who is committing this act is physically outside the cyber space. Every activity of the criminal while committing that crime is done over the virtual world

2.5 Difficult to collect evidence: It is very difficult to collect evidence of cyber-crime and prove them in court of law due to the nature of cyber-crime. The criminal in cyber-crime invoke jurisdiction of several countries while committing the cyber-crime and at the same time s/he is sitting at some place where he is not traceable.

2.6 Magnitude of crime unimaginable: The cyber-crime has the potential of causing injury and loss of life to an extent which cannot be imagined. The offences like cyber terrorism, cyber pornography etc has wide reach and it can destroy the websites, steal data of the companies in no time.

3. Common Cyber-Attacks and its impact:

The technology is growing and changing rapidly day by day. As the changed technologies bring easiness on daily human activities the same type of changes are growing in the dark side as the cyber criminals also adopt new technology for different types of attacks. There are hundreds of cyber-attacks if we make count one by one but here we describe some of the common cyber-attacks that we can see repeatedly and their impact in brief.

Types of Cyber-ttack	Impact of cyber-attack
Malware (ransomware, spyware, viruses, worms): Malicious software used by attackers to breach a network through vulnerability, such as clicking a link that automatically downloads the software to the computer (Duggal, 2019).	• Blocks legitimate access to components of the network • Installs additional harmful software • Obtains information by transmitting data from the hard drive • Disrupts components and makes the system inoperable

Phishing: Fake communications (typically through email) appearing to be from a trustworthy source that allow hackers to obtain login information or install malware on a computer when someone interacts with their message (Mann, 2011).	• Obtains a person's confidential information for financial gain • Obtains employee log-in credentials to attack a specific company • Installs malware onto a computer
Man-in-the-middle attack (MitM): Attackers insert themselves into a two-party transaction. Common points of entry include unsecure public Wi-Fi networks and computers affected with malware (Barkha, 2006).	• Interrupts a transaction to steal personal data
Denial-of-service attack (DoS): Attackers flood a site host or network with digital traffic until the target site/service cannot respond or crashes completely. A distributed denial of service attack (DDoS) is when multiple machines are used to attack a single target. Botnets, which are networks of devices that are infected with malware, are often used in DDoS attacks.	• Legitimate users cannot access websites, online services, or devices • Slows down network performance
Structured Query Language (SQL) injection: Attackers use malicious code on vulnerable servers to force the server to reveal information. It can be done by submitting malicious code into vulnerable search boxes on websites (Paranjape, 2010).	• Obtains contents of an entire database, including sensitive information • Allows attackers to modify and delete records in a database
Zero-day exploit: Attackers hack network vulnerability before it is noticed and fixed by a patch or permanent solution. Used by nation-state actors and sophisticated hackers (Paranjape, 2010).	• Allows attacker to plant malware into a system without the victim knowing

4. Major Cyber-Attack Incidents of Nepal :

Cyber-attacks become more and more a daily reality for both companies of all sizes as well as single individuals in each and every country, however yet little is universally known about cyber-crime. There is a general lack of understanding of the different types of attacks, characteristics and possible results, which may pose an obstacle in trying to defend the information security. Several definitions of the terms cyber-attack, cybercrime, etc. can be found among the international literature, all having in common

with the aim to compromise the confidentiality, integrity and availability of data. The technological evolution also brings along the progress of cybercrime, thus new ways to perform attacks, reach to even harder to penetrate targets and remain untracked are developed continuously. However, traditional cyber threats remain the source of the most common attacks. Denial of Service (DoS) attack, DDoS (Distributed Denial of Service attack), Malware Attack, Phishing, Social Engineering Attack, ATM fraud, Attack on Digital Data Bank or Database are the major types of cyber-attacks in the world as well as Nepal too. The following are the major attacks in Nepal that can be taken as a background of this study.

4.1 Nabil Bank ATM Theft (September, 2019)

The Chinese hackers were arrested from a Nabil Bank ATM booth in Durbar Marg while trying to withdraw cash. Acting on a tip-off, the Kathmandu Metropolitan Police Circle caught two Chinese nationals, in the act of withdrawing thousands in cash from the ATM using cloned debit cards (The Kathmandu Post, 2019). Initially the hackers breach a bank or payment processor's systems and then use bank cards to withdraw millions in a short amount of time. The hackers hacked the Nepal Electronic Payment Systems (NEPS), an interface that allows the transaction of money deposited in a bank by using cards issued by other member banks. NEPS has incorporated 11 commercial banks, including Prabhu Bank, Sunrise Bank, Machhapuchchhre Bank, Janata Bank, Siddhartha Bank, Citizens Bank, NIC Asia Bank, Prime Bank, Nepal Bangladesh Bank and Global IME Bank. Seven development banks are also members of NEPS. The failure of banks, especially the Nepal Rastra Bank, to upgrade their digital security measures has meant that Nepal is increasingly becoming a target for hackers from around the world. In addition to cash-out attacks, weak systems are vulnerable to conventional attacks using phishing software and malware, and physical methods like ATM jackpotting.

4.2 Customers' Data Theft from Foodmandu (7th March, 2020)

Foodmandu, an e-commerce company providing on-demand food delivery service across Kathmandu valley encountered data breach on March 7, 2020. According to a statement released by the company a day after the incident, they detected a cyber-attack by a hacker which resulted in unauthorized access of customer data. Names, mailing addresses, email addresses and phone numbers of the users were exposed to cyber-attack, according to CEO of the company (My Republica, 2020). A Twitter handle by the name of Mr. Mugger revealed the dump of data of 50 thousand Foodmandu users and also disclosed the link associated with the data. This shown the loopholes of the applications that are used by the different companies form where the customers entered their personal information.

4.3 Customer's Data theft from Vianet (7th April, 2020)

Personal details, including names, locations, emails, phone numbers and addresses of around 170,000 Vianet customers have been breached and leaked onto the internet. (The Kathmandu Post, 2020) The breach was first announced by anonymous hackers via Twitter on Tuesday, alleging that the user details of around 170,000 customers of Vianet, one of Nepal's leading Internet Service Providers, had been compromised. By issuing an official statement on the same evening, the Internet Service Provider admitted that an unauthorized party had accessed personal data of users', particularly name, location, email address and phone number. The Vianet data breach comes just a month after similar personal details belonging to users of the above mentioned foodmandu data breach.

4.4 Fifty-eight (58) Websites Hacked at a time (24thJuly, 2017)

It is taken as one of the biggest breaches of government computer systems, as many as 58 websites were reportedly hacked by a group that called itself "Paradox Cyber Ghost." The group subsequently posted a status on Facebook, along with a list of government websites, including the Ministry of Defense, Office of the Auditor General and Nepal Law Commission, that it had hacked (The Kathmandu Post, 2017). The hacker's group "Paradox Cyber Ghost" in a Facebook conversation with the Post claimed that the act was just a "vulnerability test" and that it did not have any other motive. The group claimed they have five members and that none of them are Nepalese. They also said that they hacked this system within 3 minutes.

These are only few examples of cyber-attack incidents in Nepal which are reported by the different Media and approved by the concerned agencies too. The similar types of incidents related to cyber-attack were happened frequently, but they did not come to the media due to the potential loss of their reputation of the business.

Not only the case related to the data breach, the case related to cyber pornography, child pornography online, social media spam, online sex advertisement and use of dark web for illegal money transaction due to the lack of proper cyber security infrastructure in Nepal.

5. Cyber-Attack and Libraries

Libraries can be taken as a platform to commit cyber-crime if the libraries are not serious on operating and assigning the ICT devices to the user in a systematic manner. Libraries used to be semi-autonomous organizations; they used systems that just worked in the library setting. Now everything is interconnected and students can reach the library through the university network. At the same time the library can reach out to students, faculty, staff and other libraries, all through a network. This interconnectedness between the library and the institutions is being exploited by cyber criminals. Libraries are facing cyber-attacks due to the large amount of personal and research data that universities and library systems store routinely.

A report published by the National Cyber Security Centre shows that the university sector was the third most vulnerable to cyber-attack. Libraries have to take the responsibility for securing their parts of the system, and be an active participant in the overall cyber security strategy. The library knows the information that it wants and it understands how that information should be appropriately distributed. The IT department will then, based on the library's instructions, make sure only people that are part of the university's network are given access to resources. The IT department will need to authenticate who is out there and determine what their characteristics are. It can then pass along this information to the library, for the library systems to make the decision on whether to grant or deny access to specific parts of the library.

6. Cyber Securities

Cybercrime and cyber security are issues that can hardly be separated in an interconnected environment. Cyber security plays an important role in the ongoing development of information technology, as well as Internet services. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being. Making the Internet safer has become integral to the development of new services as well as government policy (ITU, 2014). Cyber security refers to the strategies, policies, guidelines, procedures, practices, and measures that are designed to identify threats and vulnerabilities, prevent threats from exploiting vulnerabilities, mitigate the harm caused by materialized threats, and safeguard people, property, and information (Walstrom, 2016).

The term cyber security takes on different meanings depending on the audience. Citizens may feel that cyber security is related to protecting personal information, while businesses may view it as a means for providing business continuity. In the policy context, cyber security represents the collective activities and resources that enable citizens, enterprises, and governments to meet their computing objectives in a secure, private, and reliable manner (Burt et al., 2014). Cyberspace is inherently insecure and securing cyber space i.e. cyber security is the protection of internet-connected systems, including hardware, software and data, from cyber-attacks. "Cyber security" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction (Rouse, 2020).

There are basically three components of cyber security they are confidentiality, integrity and availability (Abomhara, 2015). Confidentiality involves any information that is sensitive and should only be shared with a limited number of people. If your credit card information, for example, was shared with a few criminals, your credit rating and your reputation could suffer very quickly. Data integrity is the assurance that digital information is uncorrupted and can only be accessed or modified by those authorized to

do so. Integrity involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle. Availability involves ensuring those who rely on accurate information are able to access it. Availability is often related to integrity, but can also involve things like a cyber-attack preventing people from accessing specific computers, or from accessing the internet.

Cyber security has become one of the major security concerns in many developing and least developed countries. Some of the factors contributing to poor cyber security are poorly secure networks, lack of cyber laws and short of well-trained IT security experts both in private and government agencies. The cyber security experts in Nepal are also in the same line of the above statement. In this context this article also tries to identify the gap between the highly sophisticated countries and Nepal in terms of cyber security.

7. Laws and Policies Related to Cyber Security in Nepal

Here the major legal provisions basically which are important from the perspective cyber security are described in summarized form. That might be very useful for our military organization to combat with the cyber-attack.

7.1 Electronic Transaction Act, 2008 (2063): One of the most important documents related to cyber security in Nepal. It is very important in a sense that it is the first law which touches different issues of the cybercrime and cyber security. The preamble of this Act emphasizes on secured transaction which is carried out by the electronic means by stating "it is expedient to make legal provisions for authentication and regularization of the recognition, validity, integrity and reliability of generation, production, processing, storage, communication and transmission system of electronic records by making the transactions to be carried out by means of electronic data exchange or by any other means of electronic communications, reliable and secured (Electronic Transaction Act, 2008)." Similarly, the Section 5 of this Act provide the legal recognition of the digital signature by stating "Where the prevailing law requires any information, document, record or any other matters to be certified by affixing signature or any document to be signed by any person; then, if such information, documents, records or matters are certified by the digital signature after fulfilling the procedures as stipulated in this Act or the Rules made hereunder, such digital signature shall also have legal validity (Electronic Transaction Act, 2008)." Providing legal validity to the digital signature adds the security level to each and every electronic transaction either it is institutional or it is personal.

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security. A digital signature is intended to solve the problem of tampering and

impersonation in digital communications. Digital signatures can provide evidence of origin, identity and status of electronic documents, transactions or digital messages. Signers can also use them to acknowledge informed consent. Digital signatures work through public key cryptography's two mutually authenticating cryptographic keys. The individual who creates the digital signature uses a private key to encrypt signature-related data, while the only way to decrypt that data is with the signer's public key. If the recipient can't open the document with the signer's public key, that's a sign there's a problem with the document or the signature. This is how digital signatures are authenticated. So, the provision of the digital signature in the electronic transaction act is very important provision related to the cyber security. Similarly, Chapters 5, 6, and 7 of the act provides more procedural aspect of the use of digital signature and it also emphasis on the government use of digital signature (Electronic Transaction Act, 2008).

The other sections of the electronic transaction act which are directly or indirectly related to cyber security can be listed as below. These provisions of ETA not only related to the cyber-crime but in some point the elements of crime are also related to the issues of cyber security just like the provision of section 44 is related to the pirate, destroy or alter of the computer source code which may be the property of any individual and organization and destroying altering and pirating the source code obviously the issue of the cyber security. Similarly, the section 45 which is related to the unauthorized access in the computer or computer system and computer material, section 46 which is related to the damage in computer or computer system are directly related to the cyber security as that type is security issues can be happen from remote by the use of internet and information technology.

Sections	Provisions
44	To pirate, destroy or alter the computer source code
45	Unauthorized access in computer materials
46	Damage to any computer and information system

7.2 The Proposed Information Technology Bill, 2019: In light of the advantages of technological integration among different countries, the Government of Nepal has felt the need for a progressive and updated law on information technology. Accordingly, the new Information Technology Bill, 2075 (IT Bill) has been drafted to replace the erstwhile Electronic Transaction Act, 2006 and provide a comprehensive framework for information technology, cyber security, data protection, and intermediary liability. The Bill seeks to regulate two major areas in

the IT field. First, it seeks to develop, promote and regulate information technology currently covered by the Electronic Transaction Act, 2008 (2063) and regulate the validity, integrity and reliability of records and signatures. The other areas it wants to regulate are cyber-crime and social media and the cyber security. The IT Bill also seeks to address the rise of digitization in Nepal, by recognizing the legal validity of electronic records, electronic contracts and electronic signatures. The provisions relating to the digitalization of public services and creating websites for all government agencies and public entities are also commendable. For the first time the term cyber security is defined in this document. And along with it there are some additional provision related to cyber security which indicates the Nepal Government is now serious on the matter of cyber security to create the secure cyberspace.

The Chapter 12 is overall deals with the cyber security (Proposed IT Bill, 2019). In the same Chapter it describes some provision of cyber security including the provision of the digital forensic lab and other different cyber-crimes. The Section 80 of the Information Technology Bill establishes a computer emergency response team (Proposed IT Bill, 2019) which is very similar practice as compare to the international cyber security legislation. It will be an independent Computer Emergency Response Team (CERT) under supervision and monitoring of Ministry of Communication and Information Technology.

According to the provision it deal with cyber security threats, identify and respond to cyber risks and to collaborate with security operations center teams conducive to establish detection rules and coordinate responses. The CERT is to publish security alerts, perform security audits and assurances, conduct cyber security awareness and training, perform analysis and forensic investigations of cyber incidents, response to cyber security incidents and coordinate with local and global agencies towards cybercrime (Proposed IT Bill, 2019). Likewise, in the Chapter 11 it provides the provision for the data security and the privacy of the individual data. It also emphasizes on the individual data protection and data privacy while handling the digital data by the public organization. Some other important provision of the proposed IT Bill on cyber security and data protection can be listed as follows.

Sections	Provisions
68 (1)	Information Security shall be guaranteed: Data processor, data warehouse operator or service provider shall maintain the privacy and integrity of the information remained in digital form during the exchange, processing and storage of the information in digital form.

68 (3)	Information security should be guaranteed: Government, public, financial or health institution should secure prescribed information while processing, transferring or storing in a way such information shall not be trafficked to the cross-border jurisdiction.
70	Security audit to be done: Government, public, financial institution or an institution that uses health related information should compulsorily conduct annual security audit of the information technology system.
71	Provision Regarding operation of data center and cloud service: Any person or Institution desirous to operate a data center or cloud service within the territory of Nepal should obtain a license from the Department after submission of an application in prescribed form.
73	Data center or cloud service not be run without license: Pursuant to this Act no one shall run data center or cloud service without license
81	Preapproval required for use of certain devices: (1) Before the use of following devices preapproval shall be taken from the Ministry: (a) Any software, electronic system or electronic devices designed to protect the electronic system or can be used for offensive acts, (b) Any kind of passwords, or access codes or data that enable partial or full access upon the electronic system or data.
84	Provision relating to cyber terrorism: Nobody shall, using Information System, undermine the national security, sovereignty, territorial integrity, nationality or national unity, independence, dignity, provincial relationship or obstruct or cause adverse effect to the security of the nation or data system
90	Data to be preserved: The Service Provider has to preserve the data relating to the service they provide for specific time and in specific form as prescribed by law.

The above provisions are additional important provisions related to cyber security and the data protection on proposed information technology bill which are directly or indirectly related to this issue however the different service providers related to ICT and other experts recommended to clarify some provisions and also recommend to delete some among them. In the case of section 68(3), the term "prescribed information" does not appear to be defined in the statute. In order to ensure consistency and ease of implementation of this legislation, this term should be defined and/or cross-referenced to its definition in the Individual Privacy Act. Similarly, in the case of section 70, the term "health related information" has not

been defined. Such a definition is imperative in order to provide clarity on which institutions must comply with this provision. It is also unclear whether the term "institution" includes private parties such as intermediaries or not. Similarly, in case of section 81, the range of electronic devices covered by this is broad enough to make this provision impractical in the present day; it is both lacking in rationale and being difficult to monitor the implementation of such provisions too. Other than above prescribed provision the listed sections are very important sections to ensure cyber security in our country.

7.3 National Cyber Security Policy, 2016 (Draft):

The National Cyber Security Policy was drafted in 2016 and discussed different time by different stakeholders to make it finalized but it is still on draft stage. Many important issues related to cyber security were arisen during draft phase and the discussion phase of the policy which are incorporated in the policy but we should wait more time for its implementation. The key provision can be discussed below. It decided to support the on-going activities to strengthen the use of ICT within the implementation of the ICT Policy by adopting this National Cyber security Policy in addition. The policy builds upon existing policies and sets out the goals, and objectives for Nepal in maximizing safety and security in relation to the use of ICT (Draft Cyber Security Policy, 2016). The policy has been developed by Nepal Telecommunication Authority with technical assistance from International Telecommunication Union (ITU). Discussions were initiated with national, regional and international experts to ensure a broad participation including governmental, non-governmental and open stakeholders' consultations. Prior to the process of drafting the policy the situation in the country as well as expectations from the public and private sector were assessed through different instruments including a questionnaire based approach. The input generated was directly included in the drafting of this document.

The main vision taken by this policy is "citizens of Nepal, businesses and government to enjoy the full benefits of a safe, secure and resilient cyber space, enabling them to get access to knowledge and share information while understanding and addressing the risks, to reduce the benefits to criminals, secure stable economic and social development and protect essential democratic structures (Draft Cyber Security Policy, 2016)." With this vision there are five guiding principles and eleven goals of the cyber security. The concept of Nation Cyber security Strategy Working Group (NCSWG) was also brought on it where the secretary of the Ministry of Information and Communication will be the Chairperson of the Committee with other seven members form public and private sector. The role of NCSWG is to develop a set of specific cyber security guidelines. It should go beyond policy statements and

focus on concrete measures (Draft Cyber Security Policy, 2016). NCSWG will be responsible for the coordination and prioritization of cyber security research and development activities with a focus on building and strengthening a local cyber security research community. It will further more identify minimum requirements and qualifications for information security professionals that will serve as basis for the development of a related curriculum.

The concept of creation of Nep-CERT (Nepal Computer Emergency Response Team) was also brought by this policy as it is also the part of the Information Technology Bill, 2019 later on. It should focus on promoting cyber security; awareness raising; upon request supporting institutions and businesses in prevention, detection and response to cyber-attacks; maintain 24/7 points of contact; carrying out digital forensic investigations; receiving and distributing reports about incidents and auditing and providing special support to critical infrastructure provider. Nep-CERT shall create the necessary infrastructure for conformity assessment and certification of compliance with cyber security best practices, standards and guidelines.

Furthermore, it has focused on the protection of the Critical Infrastructure. The government defines Critical Infrastructure as the essential services that underpin Nepalese society and serve as a backbone of Nepal's economy, security and health. The sectors included in the Critical Infrastructures are but not limited to Healthcare and Public Health Sector, Energy Provider Sector, Water and Wastewater Sector, Transportation Sector, Information and Communication Technology Sector, Food and Agriculture Sector, Financial Service Sector, Government Facility Sector, Emergency Service Sector, Law Enforcement and Judiciary, Defense Forces, Critical Manufacturing Sector and Tourism Sector (Draft Cyber Security Policy, 2016). The government is committed to strengthen the protection of critical infrastructure and especially critical information infrastructure provider with regard to cyber threats. This shall include the owner of critical infrastructure as well as operator of services using critical infrastructure.

7.4 Privacy Act, 2018 (2075):

In September 2018, Nepal passed the Privacy Act. Implementing the constitutional right to privacy (Constitution of Nepal, 2015), the Privacy Act has had a significant impact on legal usage of "personal information (The Privacy Act, 2018 Section 2c)." It stipulates how 'personal information' available and stored with public entities is to be utilized (The Privacy Act, 2018), along with liabilities for breach (The Privacy Act, 2018). Specifically, the Section 25 provides the security and protection for the collected information by saying "the personal information

that has been collected by any public body or remained under the responsibility or control of such a body shall be protected by such body (The Privacy Act, 2018, Section 25)."

8. Role of Librarian for Cyber Security:

The library is a custodian of diverse and multiple sources of information. Before the advent of computers, information technology, the library was primarily a storehouse of books and manuscripts though with a structured and organized collection. The growth to books and manuscripts came after the early ages when information was primarily in carvings, parchments, scrolls, pictorials and the likes. However, with the advent of computers came data/information stored on disks, CD-ROMs, microfilms, etc. The library grew from manually carrying out routines to automated services; to escape the toil of repeatedly performing jobs manually and enhance efficiency of library service delivery. (Shabana, Saleem & Batcha, 2013). The library grew from being automated to going digital; the possibility of the library going digital translates to it being able to hold more information resources without having to seek larger physical spaces. Electronic resources, digital collections and digital services became the way to go. Nearly all services that take place in the physical library can be accessed online: registration of users, access to library catalogue, charging and discharging book loans, current awareness services, reference services, even reading the information materials.

Information management has moved from the computer network-based to cloud computing. With the development comes greater risk of threats and risks associated with the cyberspace. The library must seek to prevent a breach into its systems and networks, users' data must be protected against unauthorized access and use (Adakawa, Al-Hassan & Auyo, 2020). Libraries should strive to update library personnel in other to curb information breaches in university libraries. Seeing the importance of information security in the library, attention should be focus on unveiling those factors that can boost information security compliance of library personnel. The management of the library and the librarians should promote awareness programs in which library personnel should gain more knowledge that will assist them solve information security breaches. The internet safety and security policy should be adopted by the librarians to secure the data of the library and for the security of the digital databases and the personal data protection of the users too.

Similarly, there are different emerging technologies in this particular area, and to enhance cyber security in the different libraries, we should aware in these particular areas. AI and machine learning can play a crucial role in cyber security by automating threat detection and response. These technologies can analyze large amounts of data to identify patterns, anomalies, and potential security breaches. Blockchain offers a decentralized

and tamper-resistant platform that can enhance data integrity, privacy, and authentication mechanisms. Academic libraries deal with sensitive user information, research data, and academic records. Blockchain can enable secure and transparent transactions, protect intellectual property rights, and prevent unauthorized access or modifications to critical data (Zhang, 2019). User behavior analysis involves analyzing user behavior patterns to identify anomalies and potential security risks. By monitoring user activities, libraries can detect unauthorized access attempts, suspicious behavior, or compromised accounts. User behavior analysis systems can provide early warnings and generate alerts for further investigation, thereby enhancing the cybersecurity posture of academic libraries. The mass usage of Internet of Things (IoT) devices in libraries, such as smart sensors, beacons, and self-checkout systems, introduces new security challenges. It is essential to implement strong security protocols, device authentication, and regular patch management to mitigate potential vulnerabilities and prevent unauthorized access (Aregbesola & Nwaolise, 2023).

9. Conclusion:

Universities and libraries are targets for cyber-attacks because their data is vulnerable and valuable. Not only does the personal data of student and staff that libraries hold provide opportunities for ransom attacks, on top of that latest research findings can become a target for international espionage. That's why it is vital for academic institutions to provide resources to cyber-security and protect themselves from potential attacks. To combat from the cyber-attacks the libraries and librarians too are recommended to do the following actions.

- Promote cyber threat awareness amongst varies group of users and enabling the workforce to secure their computers and cell phones and take necessary steps to protect their online identities, privacy, and financial credentials.
- Remind faculties, staff and students of the risks that can come when sharing account passwords and campus credentials, as they are likely linked to other personal information and may unknowingly enable access beyond the single system they are trying to share.
- Design an effective cyber defense strategy which can protect the academic and educational databases that are stored in different academic institutions and libraries.
- Create cooperation between governmental bodies and the private organization and entities that can dominate cyberspace, to share information they deem relevant to cyber threats.
- The collaborating institutions should encourage investment such as funding opportunities and grants in research and development initiatives aimed at enhancing cybersecurity measures for digital collections.

- The library and ICT unit should be in constant communication to discuss ways the library can participate in improving the overall security posture of the institution and the library itself.

- Libraries should form partnerships with cybersecurity experts from within their institutions or external organizations. They should engage with IT departments, cybersecurity centers, or specialized cybersecurity firms to leverage their expertise and guidance. These collaborations can help libraries develop and implement robust cybersecurity frameworks tailored to their specific needs.

- Promote a secure, flexible, and trust wealthy global cyber operating environment that supports international cyber security.

References:

Abomhara, M & Koien, G.M. (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber Security, Vol. 4, 65–88. https://www.riverpublishers.com/journal/journal_articles/RP_Journal_2245-1439_414.pdf.

Adakawa, M. I., Al-Hassan, M., & Ayuo, M. A. (2020, December 12). Now and Future of libraries: the necessity to equip librarians with cybersecurity skills. In Management of Library and Information Centers in the era of global insecurity (pp. 1-18). Retrieved May 17, 2023, from https://www.researchgate.net/publication/346967054_NOW_AND_FUTURE_OF_LIBRARIES_THE_NECESSITY_TO_EQUIP_LIBRARIANS_WITH_CYBERSECURITY_S KILLS/link/5fd530c392851c13fe80f57a/download

Aregbesola, Ayooluwa & Nwaolise, Ekene Lawrence, (2023). Securing Digital Collections: Cyber Security Best Practices for Academic Libraries in Developing Countries, Library Philosophy and Practice (e-journal), University of Nebraska – Lincoln, 2023.

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/.

Cavelty, M.D.(2012). The Militarisation of Cyber Security as a Source of Global Tension. In Daniel Mockli (Ed.), *Strategic Trends 2012: Key Developments in Global Affairs*. ETH Zurich: Center for Security Studies. 103-124. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Strategic-

Trends-2012.pdf.

Cybersecurity Policy Draft.(2016). https://nta.gov.np/wp-content/uploads/2018/05/Nepal-Cybersecurity-Policy-Draft.pdf.

Duggal, P. (2019). Cyber Law: An exhaustive Section wise Commentry on The Information Technology Act along with Rules, Regulations, Policies, Notification etc. Lexis Nexis.

Electronic Transaction Act. (2000). https://lawcommission.gov.np/en/?p=16954.

Elmusharaf, M.M. (2004). Cyber Terrorism: The new kind of Terrorism, http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism/.

International Telecommunication Union (2014). Understanding Cybercrime: Phenomena, Challenges and Legal Responses, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/cybercrime2014.pdf .

International Telecommunication Union.(2016, November). Understanding Cybercrime: A Guide for Developing Countries. https://www.itu.int/ITUD/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf.

Khalifa, E. (2015). Military Cyber Threats: Transformations in Unconventional Security Threats. https://www.academia.edu/10137546/Military_Cyber_Threats _ Transformations_in_Unconventional_Security_Threats.

Li, Yuchong & Liu, Qinghui. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports. https://www.researchgate.net/publication/354346903_A_comprehensive_review_study_of_cyber-attacks_and_cyber_security_Emerging_trends_and_recent_developments .

Maheshwari, A. (2022, March 12). Cyber crime to cost economies $10 trn by 2025: Microsoft India official. Business Standard. https://www.business-standard.com/article/economy-policy/cyber-crime-to-cost-economies-10-trn-by-2025-microsoft-india-official-122031201080_1.html#:~:text=Cyber%20crime%20is%20the%20biggest,India%20official%20said%20on%20Saturday.

Mann, R.J. (2011). Electronic Commerce. Wolter Kluwer Law and Business

My Republica (2028 March 8). Foodmandu's website hacked, 50 thousand users' data dumped https://myrepublica.nagariknetwork.com/news/foodmandu-s-website-hacked-50-thousand-users-data-dumped/.

Paranjape V. (2010). Cyber Crime and Law. Central Law Agency.

Proposed Information Technology Bill (2019).

Reed, C & Angle J. (2014). Computer Law. Oxford University Press.

Rouse,M. (2020). *Definition of cyber security.* https://searchsecurity.techtarget.com/definition/cybersecurity.

Shabana, T. S., Saleem, A., & Sadik, B. M. (2013). Impact of library automation in the development era. IOSR Journal of Humanities and Social Science, 17(5), 20-26. Retrieved August 2, 2023, from https://www.researchgate.net/publication/324829280_Impact_of_Library_Automation_in _the_Development_Era

Singh, Y (2019). Cyber Laws. Lexis Nexis.

The Kathmandu Post (2017, July 25). 58 govt websites 'hacked to test vulnerability. https://kathmandupost.com/valley/2017/07/25/58-govt-websites-hacked-to-test-vulnerability.

The Kathmandu Post (2019, September 1). "Millions stolen by ATM hackers exposes vulnerability of Nepali banks. https://kathmandupost.com/money/2019/09/01/millions-stolen-by-atm-hackers-exposes-vulnerability of-nepali-banks.

The Kathmandu Post (2020, April 8). Vianet suffers data breach, leaking personal customer details online. https://kathmandupost.com/national/2020/04/08/vianet-suffers-data-breach-leaking-personal-customer-details-online.

The Privacy Act. (2018). https://www.lawcommission.gov.np/en/wp-content/uploads/2019/07/The-Privacy-Act-2075-2018.pdf.

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/.

Zhang, L. (2019). Blockchain: The New Technology and its Applications for Libraries. Journal of Electronic Resources Librarianship, 31(4), 278–280. https://doi.org/10.1080/1941126X.2019.1670488.