ISSN 2631-2131

Security Threats and Legalities with Digitalization in Nepal

Sushant Acharya and Sudhamshu Dahal

Author(s)	Sushant Acharya and Sudhamshu Dahal
Association	Department of Languages and Mass Communication, School of Ars, Kathmandu University, Hattiban, Lalitpur, Nepal.
Received Date	20th November 2021
Accepted Date	1st December 2021
Email	sudhamshu.dahal@gmail.com

Abstract

As the process of digitalization spreads globally, daily dependence on cyberspace is increasing. With the rise of criminal incidents in cyberspace, it has begun to pose security threats that disrupt peace and order. In a chaotic situation with the global pandemic of Coronavirus disease (COVID-19), digitalization has become a mandatory process in the world. Along with the mandatory process of digitization and increasing trend of digitalization in Nepal, there is also a possibility of security threat. This research paper seeks and examines policies and laws that the Government of Nepal has formulated to reduce the security threat and it explored to find out what types of security threats were seen from cyberspace in Nepal during several lockdown periods during 2020 AD. The study concludes that Nepal has laws to legalize digital activities with constitutional rights to do cyber activity. But does not have enough laws and policies to address the emerging cyber threat environment because of the long process of passing the law and lack of sufficient interest and knowledge on lawmakers. The risk of cyber security in Nepal seems to be high due to non-implementation of the policies and rules issued by the government itself, low level of cyber security awareness among the people, lack of strong defense system and policy on cyber-attacks.

Keywords: Cyber Laws and Policies, Cyber Security Awareness, Cybercrime and terrorism, Digitalization and Security threat,

Introduction

In a chaotic situation with the global pandemic of Coronavirus disease (COVID-19), digitalization has become a mandatory process in the world. Today digitalization is not just about operating a computer from a computer programming language to a binary language. To digitalize daily routine by setting an alarm on our mobile phone to get up in the morning and posting activities on social media is also a digitalization process. With the increased use of the internet in Nepal, there has been an increase in the security challenges that may occur through the internet or within the internet

system. One after another, attacks on government office websites (Kshatri, 2020) or organized anti-government demonstrations via the internet (Government of Nepal Ministry of Home Affairs, 2020). Both are new security challenges posed by digitalization. In this regard, the current cyber laws and policies in Nepal need to study and examines in the context of security threat.

Objectives

The purpose of this research paper is to find out what policies and law have the government of Nepal or its subordinate bodies made regarding cyberspace related security? And what is in the implementation? The second purpose of this research paper is to explore the extent of Nepal's cyberspace policy and law in terms of security challenges and threat on the basis of methodological framework. This study examines and discusses the laws and policies relating to cyberspace security within the cyber system and security threats from cyberspace to society in Nepal. It is an interdisciplinary research in security studies and legal policies studies on the foundation of social science.

Methodology

The research adopts a qualitative content analysis as the text mining methodological approach for the first section of the research. It analyses the text according to text characters or sentences structure for the use of information retrieval and knowledge mining. The first section will find out what kind of rules related to cyber have been given legal legitimacy in Nepal and are in practice. The research applied non probability sampling for the study corpus. The sampling involves selecting the laws and policies regarding the cyber activity in Nepal. The data used and incorporated in this research are from the government websites and various archival resources, publications and data published by various organizations. The indicators used for analysis in the first section are presented in the (Table i).

The second section will find out what kind of cyber threats are seen in Nepal by using the exploratory method. It uses existing literature resources to find out the answer. Based on the first section results and knowledge it discusses and interprets the data. Based on the time period of several lockdowns of 2020 AD, the cyberspace threat and security threats which may hinder sustaining Nepal's peace and safe environment by the use of cyberspace have been explored.

Table i: First section analytical framework

	Indicators	Application
1.	Legal legitimacy	From this, it can be known whether cyber related activity has been legalized in Nepal or not.
2.	What issues and topics are covered by the law and policy?	By looking at the issues covered in Nepal's cyber law and policy, we can know where the limitation of Nepal's cyber law and policy is.
3.	How cyber-related provisions are included in the laws and policies?	An indicator of how cyber-related provisions are included in the laws and policies studied helps to deep analyze Nepal's cyber security provisions.

4.	Interconnectedness of all the laws and policies	Looking at the interconnectedness of all the laws and policies studied here, it helps to understand broadly whether there is clarity in Nepal's policies and laws related to cyber security.

(source: Study, 2021)

Results and discussions

Cyber related laws and policies in Nepal

The legal provisions related to cyber activity in Nepal are guided by the Constitution of Nepal, Acts, Rules, Guidelines, Policies and Bylaws issued by various thematic bodies. It is presented in table 2. An Act and regulation to regulate cyber activity, although limited by numbers and jurisdiction, but that does not directly deal with cyberspace have been transformed into legal instruments to regulate cyberspace with the advent of digitalization.

Apart from the laws to be passed by the Parliament of Nepal, various government bodies have been formulating rules related to cyberspace. Such rules have been given legal recognition by the 10th Amendment to the Interpretation of Law Act, 2010 (1954 AD.). The Ministry of Information and Communications Technology (MoICT), Nepal Rastra Bank (NRB) and Nepal Telecommunications Authority (NTA) have been conducting such exercises.

Table No. ii*. Cyber related laws and policies of Nepal*

Name of the Document	Types (Legal legitimacy)	Background information and Jurisdiction	Cyber Activity and Cyber Security Related Major Provisions
Constitution of Nepal	Constitution		Article 19 provides for the right to communication and Article 27 provides for the right to information as a fundamental constitutional right. Article 19 of right to communication enshrines the right to digital activity as a fundamental right of Nepali citizens. In addition, Article 19 stipulates that no one can ban the digital activity of a citizen but provision has been made to enact laws to prohibit acts that could disrupt the peace and order through digital activities

/Electronic Transaction Act, 2063 (2006 AD.) (ETA 2006).	Act	ETA 2006 is the first act to regulate cyber activity in Nepal since September 2, 2006. Published in Act number 27 of the year 2063.	It has given legal legitimacy to the communication and transaction system of electronic records in Nepal. It has the provision relating to electronic records and digital signature, provision relating to the computer network and network services providers, provision relating to computer-related crimes and punishments and Provision of IT tribunal is defined as the first jurisdictional and appellate jurisdiction. Based on the provisions of ETA 2006, Electronic Transaction Regulation (2007 AD.) (ETR 2007)) and Information Technology Tribunal Procedures Rules 2064 (2007 AD.) have been issued.
Telecommunication Act, 2053 (1997 AD.)	Act	The Telecommunications Act, 2053 (1997) which came into force on January 1, 1997 which was designed to regulate the telecommunications sector, make telecommunication services largely accessible and include the private sector in telecommunication services	With the transformation of the telecommunication industry, the Telecommunication Act, 2053 (1997) has evolved into an active legal instrument to regulate cyber activity. More than 10 directives and rules are issued by the Nepal Telecommunication Authority (NTA) on the basis of Telecommunication Act, 2053 (1997). Chapter 2 and 3 of this Act provide for the establishment and constitution and functions, duties and powers of the NTA. Based on this, NTA has been regulating Nepal's telecommunication sector.

Mobile Device Management Systems Bylaws 2075 (2018) (MDMS Bylaws)	Bylaws issued by NTA		NTA has framed these MDMS Bylaws for the implementation of Equipment Identity Register (EIR) system to ensure national and consumer security, to identify the genuine mobile handsets and make the fake and non-genuine handsets inoperable in Nepal, to enable tracking/blocking of mobile handset that is lost/stolen, to encourage import and sell of genuine mobile handsets and to eradicate grey market. MDMS Bylaws 2018 has given instruction to not to provide service on illegal mobile devices which are not registered in NTA. These Bylaws are not only important for mobile device security and information security but also for revenue collection in Nepal
Online Child Safety Bylaws 2076	Bylaws issued by NTA	NTA has issued online child safety guideline 2076 to minimize and to mitigate child abuse through ICT and to create safe internet for children	This guideline sets out the work to make a safe internet for children that Internet Service Providers (ISPs) / Mobile Network Operators (MNOs) need to do, that families and communities need to do, and NTAs need to do. Under the work to be done by NTA, it is mentioned in the guideline number 26 that 'online child abuses complaints system' will be developed and brought into operation. Also ISPs / MNOs are given instruction to show whether the available content on the Internet is suitable for the age group of children or not.

Cyber security Bylaws 2077 (2020)	Bylaws issued by NTA	During the lockdown of 2020, NTA has issued Cyber Security Bylaw, 2077 (2020) at a time when one after another cyber-attack is taking place in the system of ISPs of Nepal.	NTA has framed this Byelaw for the implementation of cyber security standards and best practices so as to protect ICT Infrastructure and Information Systems of Telecommunication Service Providers of Nepal from various malicious attacks and threats; and build trust and confidence of users towards using ICT technology and services. This bylaw has given a check list for IS audit. This checklist contains 70 checklist questions. This includes questions related to 1) Standards and Practices, 2) Infrastructure/Network Security, 3) Core System Security, 4) Application Security, 5) Data Security/Privacy, 6) IS Audit, 7) Cloud Security, 8) CERT/Incident Response, 9) Security Operations Centre (SOC) 10) Cyber Security Awareness & Capacity Building and 11) Miscellaneous. It has been issued as a tangible document related to cyber security of Nepal. It directs to examine the risks posed by common technical and human error in the field of cyber security.
Secure Password Practice	Guidelines	The Office of the Controller of Certification (OCC) under the MoCIT has issued.	It has issued to the employees working in various organizations of the Government of Nepal by compiling password security criteria and suggestions on what kind of password should be kept in office related work. Under the Enforcement and Penalties of Secure Password Practice, "any employee found to have violated these practices may be subject to disciplinary action. It has been mentioned that this is determined by the code of conduct or policy of the office or organization. Although Secure Password Practice has issued binding suggestions to reduce human error in cyber security in offices under the Government of Nepal, it does not have a legal provision to issue penalties.

National Information and Communication Technology Policy, 2015 (ICT Policy 2015)	Policy	National Information and Communication Technology Policy, 2015 (ICT Policy 2015) is the main policy related to current cyber activity in Nepal. Since the enactment of the Telecommunication Act 1997, the Government of Nepal has adopted a strategy to increase public access to ICT. As a continuation of that strategy, the Nepal Government brought Information Technology Policy 2057 (2000) (IT Policy 2000) in 2000. The second series of IT Policy 2000 is ICT policy 2015.	ICT policy 2015 basically focused on, how to expand ICT to the general public? And how to integrate ICT with development work? This policy envisages "Digital Nepal". Chapter 17 of this policy mentions the assumption and risk. In which it has been mentioned that if there is lack of required improvement in necessary laws and regulatory systems, this may create a weak investment environment of ICT. Strategy 12.21 addresses issues related to cyber security and law in Building Confidence and Security in the use of ICT's. It has included the establishment of the IT Tribunal system which is mentioned in the ETA. Also mentioned is the establishment of a Computer Emergency Response Team (CERT) and a cyber-security cell in the ministry of communication and information technology. It is mentioned that the capacity building program will be conducted for law enforcement agencies and cyber security education programs for publics.
The National Broadband Policy, 2071 (2015)	Policy issued by MoCI	This policy focuses on increasing the access and quality of broadband services in Nepal.	The guiding principles this policy includes digital divide, universal access and service, Adopting the concept of Public Private Partnership for the development of ICT sector, providing necessary legislation and regulation for the expansion of broadband services and to achieve the Government of Nepal's commitment to establish Nepal as a developing country from a least developed country by 2022, and to develop it as a supportive policy Here are 12 goals in this policy and 11 have their deadlines. There are 6 targets to be completed by 2018 and 5 targets to be completed by 2020. One of the six goals to be achieved by 2018 is to maintain that broadband service charges for general consumers at 5% of Nepal's per capita income.

Digital Nepal Framework, 2076	Framework Policy issued by MoCI	Framework issued as a complementary policy to the ICT Policy 2015 and the National Broadband Policy, (2015).	The objectives of this framework are to build the foundations of an information-based society and digital economy, to achieve the goals of development and prosperity by making maximum use of digital technology, and to make public services available to the general public in a simple and easy way. In this framework, 8 major areas have been selected. This includes digital foundations, agriculture, health, education, energy, tourism and finance and urban infrastructure. Under this, 80 initiatives have been identified.
National Security Policy, 2075	Policy issued by Nepal Government	National Security Policy, 2075 is being implemented in Nepal, which needs to cover the overall security issue of the nation	This includes some issues related to cyber space and cyber security. Policy No. 1.7.10 mentions the misuse of science, technology and modern equipment as an element affecting national security. Similarly, 1.9.2.4 of the policy mentions the misuse of modern technology in crimes under law and order related challenges and threats.

(Source: Study, 2021)

Apart from presented in Table 2, some guidelines and directives for conducting various activities related to cyberspace have been issued by MoICT. System Management and Operation Directive, 2071, Mobile Apps Criteria for Government Bodies directives, 2075, Email Management of Government Bodies directives, 2075, and Government Website development and management directives, 2075 are issued by MoICT which are in implementation.

Drafted Cyber related law and its discussion

The laws related to cyber space issued in Nepal, in the current state of rapid development of technology, seem to be inadequate to the concerned bodies. The Information Technology Bill, 2075 (IT Bill) is in the process of being enacted to replace the ETA (2006) as an umbrella act related to cyberspace. The provisions of the ETA (2006) are closely similar to the UNCITRAL Model Law Electronic Commerce (1996) (MLCE (1996)). "UNCITRAL Model Law Electronic Commerce was adopted by the United Nations Commission on International Trade Law, so as to remove unnecessary obstacles to international trade caused by inadequacies to international trade caused by inadequacies and divergences in the law affecting trade" (United Nations, 2020). Although MLCE (1996) was not directly endorsed by Nepal, it can be assumed that the ETA (2006) with similar characteristics was affected by it.

Despite being registered as a bill in the House of Representatives on February 14, 2019, the IT Bill is yet to be finalized (Federal Parliament of Nepal, 2020). This bill has received a lot of discussion in Nepal's public spare and in the media. With the completion of this bill, the current

cyber activity related act will be replaced immediately. This bill is controversial as some of the vague provisions mentioned here and some of the provisions seem to contradict the Freedom of expression (International Federation of Journalists, 2020). This bill is very important from the point of view of the legal system with cyber security. Chapter 12 deals with cyber security. These has include identifying sensitive infrastructure, CERT, jurisdiction and structure, cyber bullying, cyber terrorism and more.

Its chapter 14 is titled 'Arrangements related to social media'. Where the provision of registration of social media networks has been mentioned. Since it is not clearly explained, is it told to the users? Or is it told to the operating company? There was a confusing discussion on social media and in Nepal's public spare. (Lama, 1019) From the point of view of digital sovereignty, it is very important to regulate the social media in Nepal by the government of Nepal.

This bill has mentioned that the IT tribunal will be established at the province level by removing the first jurisdictional and appellate jurisdiction of the IT tribunal which is provided by the ETA. ICT entrepreneurs in Nepal have urged the government to correct the provision on complete ban on data sharing. They have said that it would be difficult to develop the latest technologies like IoT and AI in Nepal after complete banning on data sharing. (Neupane, 2019)

On 09 May 2019, Kathmandu, Kalyani Kumari Khadka, chairperson of the Development Committee of the House of Representatives (Khadka, 2019), said that the law related to the IT sector, including the IT bill, was delayed due to the unstable government in Nepal and her committee including she does not have enough knowledge about IT and law. Also, when defining the whole subject in the IT bill, it will be inconvenient to the executive. In defining the convenience of the executive, she said that the provisions of the IT bill have been vague.

Although some of the important laws related to cyberspace have been drafted in Nepal for a long time, they have failed to get legal fulfillment. One such draft is the Cyber Crime Act which was prepared by the Nepal government and NTA to put the issue of cyber-crime and cyber security in a clear legal framework. The draft was prepared in 2017 but has not yet been able to enter the lawmaking process as a bill. This act will be a strong act for the operation guideline of the IT Tribunal. This draft act clearly explains the incidence of cybercrime rather than the laws in force (Aryal, 2020). In the process of preparing this draft, NTA has built on the basis of ITU's cybercrime guideline (Basukala, 2020).

National Cyber Security Policy 2016 is a policy that could not be implemented even after the draft was prepared. Some of the issues mentioned here are being implemented in the online child safety guideline, 2076 and cyber security bylaw, 2020.This policy has given special emphasis on building CERT and increasing its effectiveness. Also, special emphasis has been laid on the security of critical infrastructure, which is considered as a very important issue in cyber security (Basukala, 2020).

Nepal's cyber laws and policies in contemporary security threat environment and Analysis on Security Perspectives

Looking at Nepal's cyber security policies from an analytical view, the cyber security related agencies here seem to be generally aware of cyber security and the risks it poses, but the risk

of cyber threats is high due to the lack of law and policies recognition of these risk mitigation measures. Nepal does not have clear laws to regulate Internet of Things (IOT), cloud computing, algorithms, etc., which have been gaining popularity in the global market. Policy rules have not been formulated with sufficient understanding of how to regulate things including digital transaction and crypto currencies from the wider national security perspective.

Once the law is made, it is important to be able to implement it. In 2006, Chapter 10, Section 60 of the ETA (2006) provided provision for the Information Technology Tribunal and Chapter 11, Section 66 provided provision for the Information Technology Appellate Tribunal. For its implementation, Information Technology Tribunal (Procedures) Rules, 2064 (2007) was issued on August 6, 2007. Even in the policy number 12.21.8 of the IT policy 2015, it is mentioned that priority will be given to its implementation. The non-establishment of an Information Technology Tribunal in any place other than Kathmandu by 2020, this proof that cyber law is not implemented even by the government.

The online child abuse complaints system provided by Online Child Safety Bylaws 2076, has not been implemented. Also, the targets set by the National Broadband Policy have not been met. One of the six goals of National Broadband Policy to be achieved by 2018 is to maintain that broadband service charges for general consumers at 5% of Nepal's per capita income. As of November 2020, Nepal Telecom, which is owned by the Government of Nepal, has not provided the service as mentioned in the goals (Nepal Telecom, 2020). These grounds provide a basis for questioning the effectiveness of the implementation of the overall laws and policies issued related to cyber security.

The need for CERT to reduce the risk of cyber threat has been identified in cyber security related policies in Nepal but the implementation has not been effective. As an indicator of its effectiveness can be taken as the inability to rescue immediately the website of the Government of Nepal which was constantly attacked and hacked (Kshatri, 2020). Although CERT operates under the MoICT, we did not find any public policy with the Government of Nepal to protect ethical hackers during the study. The government of Nepal has also been obstructing the protection of ethical hackers from the private sector. Also common people are unaware towards ethical hackers (Aryal, 2020). According to Roja Kiran Basukala, Deputy Director, NTA, a draft policy with legal provisions to protect ethical hackers is being prepared and sent to MoICT (Basukala, 2020).

It can be assumed that the failure to protect ethical hackers from the government level could pose a great threat to national security. If the government does not protect ethical hackers, it will be difficult for the government to control the incident if the independent hackers go out of control tomorrow. To estimate this threat, we can study the pre cyber war between the two countries from the civilian level of Nepal-India in May 2020 during the Nepal-India Kalapani border dispute.

In 2020, when the border dispute of Kalapani Lipulekh area between the Government of Nepal and the Government of India, when it reached its climax, the feeling of disillusionment at the grassroots and civilian level was widespread in cyberspace (ICT Frame, 27 May 2020). At this time, the feeling of disgust was not limited to social media, even the cyber-attack had taken shape. Indian hackers hacked more than 45 Nepali websites in Nepal, including the official website of the Civil Aviation Authority of Nepal and the website of the Nepal National Library. By hacking the website of the Civil Aviation Authority of Nepal they placed Indian national flag on the home page. Similarly, Nepali hackers also tweeted by leaking the API key of Indian media ABP (ICT Frame,

2020).

At this time, Nepal Police said it was outside of our jurisdiction, who are working on Nepal's cyber security. According to Nepal Police, without official complaints, authorities can't conduct an investigation into such cases. "We haven't received any official complaint from the victims, so we haven't officially investigated the case," said Deputy Inspector General Niraj Bahadur Shahi, spokesperson for Nepal Police. "However, if we receive any complaint from the victim, then the cyber bureau will investigate and action will be taken. But if a cyber-crime is committed from outside Nepal, we cannot take action as it is out of our jurisdiction. However, in serious cases, we can request the country concerned to take action against such criminals" (Dhungana, 2020).

When it comes to the security threat posed by cyber space, security within cyberspace it cannot be limited. It is equally important to discuss the threats to national security and society through cyberspace. The risk to Nepal's internal security through cyberspace also seems to be high. Cyberspace easily helps to spread the feeling of rebellion against the government and to organize the protests against the government. We can assume that cyberspace seems to be evolving into a major tool for creating urban guerrilla warfare conditions (Marighella, 1969) presented by Carlos Marighella. An example of this threat we can study the demonstration of the 'Enough of is Enough' campaign in some of the major cities of Nepal, from June 9, 2020, when the Government of Nepal is conducting a lockdown for the first time to control the COVID-19 pandemic.

An 'Enough of is Enough' campaign evolved from an Instagram story post by a young man when even after 70 days of lockdown by the government of Nepal, the government was not able to show its exit point of lockdown and the government was gradually losing faith from the public. Ishan Adhikari, who identifies himself as Iih, expressed distrust and rebellion feelings towards the government from his Instagram account, and he created the poll and he asked who is ready to go on strike if it happens now? Based on that poll, he created a Facebook public group on Facebook on June 6 at 3 PM. Preparations are made for the first demonstration on June 9 and the demonstration took place as planned on the Facebook group. The number of people joining the group increases rapidly with the arrival of photos, videos and news on social media. By the time of the first demonstration, the group, which had around 2,000 members, in the speed of per hour thousand people joined the group within 50 hours of the demonstration, and the demonstration took place dozens of times, and in dozens of major cities of Nepal including Kathmandu (Setopati, 2020).

The rapid spread of fake news in cyberspace today, especially on social media, is another major security threat (Guadagno, 2019). Along with the gradual increase in the literacy rate and per capita income of Nepal, the means of ICT have also increased (Sharma, 2016). Here suddenly over-information has entered into the large numbers of people's daily life. Due to lack of knowledge and experience on how to receive information in their daily life and being difficult to control fake news, the risk of security threat is high in Nepal (Khatiwada, 2020).

The cyber security awareness program is included in all the policies and regulations related to cyberspace and cyber security in Nepal, but it can be estimated that the effectiveness is low in public. As a basis for this estimate, according to a survey conducted by the Nepal Army, which is responsible for national security, there is a lack of public awareness about cyber security within the armed forces. In the (Nepal Army, 2019) survey, 29.3% of the respondents felt that they were aware

of the question of 'how literate you are about cyber security and cybercrime?'. The Nepal Army which has adopted Fifth Generation Warfare (5GW) in a military doctrine (Nepal Army, 2014). It gives ground for questioning how it is implementing adequate cyber security policies and practices in Nepal Army. Also based on this, the question can be raised about the level of cyber security awareness among the layman.

Similarly, another report 'IT Audit Report: Legitimacy and Use of Information Technology System in Government Bodies, 2074' which was made public by Office of the Auditor General (OAG), in the 24th number of report under 'Information Technology Literacy', it is mentioned that citizens have no access to information technology and information technology literacy.

Rapid speed of the digitization process has shown the many opportunities, challenges and threats in various sectors. We can assume that for marginalized and excluded communities a new system is always a big hope for them to bridge the inequality gap. Same as, Digitalization is the optimistic object to bridge their gap from exclusion to inclusion in the system. But digital bridge is not an easy task in digitalization (Badal, 2019). One of the negative sides of digitalization is digital divide. 36.8% People don't have digital access in the world (Internet World Stats, 2020) but almost every system of our life is rapidly integrating to the digitalized system. The security risk of insurgency caused by the digital divide cannot be underestimated in Nepal. Its dimension is very large on the social and national security perspective. Digital divide is discussed in both ICT Policy, 2015 and National security policy 2075. The design reality gap (Heeks, 2018) can also be studied as the cause of the revolt seen along with the digital divide. The reason for the revolt is that after a system is digitalized, not understanding the language in the system application and not being user-friendly digitalized technology for marginalized people. An example of this is the non-use of mother tongue in mobile banking apps and on the other hand, banks are urging their customers to use their mobile banking apps to get service (Nepal Bankers Association, 2020).

In this regard, the design reality gap and language related issues are not mentioned in the NRB's IT guideline and policy and are not included in other rules, policies and reports as well (Nepal Rastra Bank, 2020). But the (Office of the Auditor General, 2074) report, discusses the design reality gap in the digitalized service provided by government offices. In the report, the design reality gap of the application related to the examination to be taken by the Public Service Commission is discussed. The 18.2 point of the report is as follows:

"In the digitized system of the Public Service Commission, there is a provision for the user to receive a mobile message after filling in the required details of the form for any examination. Although the Public Service Commission has done the job of sending the message to the mobile, if the mobile message is not received due to the telecommunication company, the user will be deprived of the examination information. Therefore, the Public Service Commission should not be limited to mobile messages but should also provide information through other means of communication such as email, telephone, etc."

Conclusion

Cyber activity related policies and laws have been issued by various concerned bodies of the government of Nepal and some provisions are included in the Constitution of Nepal. The laws and policies that have been issued are not enough to address and regulate in the time of rapid

development of technology and its widespread use in public life. Since the laws and policies issued are not implemented by the government bodies, it is helping to increase the cyber security threat. With the increase in cyber activity in the daily life of the common man and the lack of cyber security awareness, it can be estimated that the risk of cyber security is increasing in Nepal. Nepal's cyber-related policies focus on enhancing cyber utility rather than cyber security. While the Government of Nepal is focused on providing services to the common man through digitized technology, there is also a need to study the sense of insurgency as a national security threat that may arise among the citizens due to digital divide and design reality gap.

Looking at the number of websites being hacked in Nepal, including those under the Government of Nepal, it seems that Nepal does not have a capable defense system for cyber-attacks. Due to the government's delay in protecting ethical hackers, the risk of cyber terrorism and cybercrime by using Nepal's geography in an uncontrolled and illegal manner seems high. The further cyber space related security threats can be analyzed by studying the 'Enough Is Enough' campaign of June 2020 and the cyber-attacks that took place at the civilian level during the Nepal-India border dispute.

References

Aryal, B. R. (2020). Discussions from the Webinar on 'Cyber Security: Are We Protected Enough'. *Legal Literacy, Advocacy, and Research (CLAR)*. Kathmandu: ICT Frame. Retrieved from https://www.youtube.com/watch?v=Qe-kZb4huDg

Badal, B. P. (2019). Tourism: Visit Nepal 2020. *Research Nepal Journal of Development Studies*, *2*(2), 12–32. https://doi.org/10.3126/rnjds.v2i2.29274

Basukala, R. K. (2020). Role of Ethical Hackers for National Security. *Information Security Response Team, Nepal (npCert)*. Kathmandu: ICT Frame. Retrieved from https://www.youtube.com/watch?v=3M1J-qcciwQ&list=PLiyj3AzKSRooVsVxxGourernIu7PvQm70&index=32&pbjreload=101

Dhungana, S. (May 23, 2020). *Nepali and Indian 'hackers' attack websites over 'boundary dispute'*. Kathmandu: The Kathmandu Post. Retrieved from https://kathmandupost.com/national/2020/05/23/nepali-and-indian-hackers-attack-websites-over-boundary-dispute

Federal Parliament of Nepal. (2020, November 14). *House of Representives of Nepal*. Retrieved from https://hr.parliament.gov.np/np/bills/Za1OEE23

Government of Nepal Ministry of Foreign Affairs. (2019, August). Nepal Foreign Affairs Annual Report (2018-19).

Government of Nepal Ministry of Home Affairs. (2020, june 11). Press Relase.

Guadagno, R. E. (2019). Fake News and Information Warfare: An Examination of the Political and Psychological Processes from the Digital Sphere to the Real World. In S. A. Innocent E. Chiluwa, *Handbook of Research on Deception, Fake News, and Misinformation Online* (pp. 167-191). IGI Global.

Heeks, R. (2018). *Information and Communication Technology for Development (ICT4D)*. Routledge.

ICT Frame. (25 May 2020). *Cyberthreat Prevails as Indian Hackers Hack 45+ Nepali Websites.* Kathmandu. Retrieved from https://ictframe.com/cyberthreat-prevails-as-indian-hackers-hack-45-nepali-websites/

ICT Frame. (27 May 2020). *Border Issue Increase Cyber War Between Nepal and India.* Kathmandu. Retrieved from https://ictframe.com/border-issue-increase-cyber-war-between-nepal-and-india/

International Federation of Journalists. (2020, January 06). *International Federation of Journalists*. Retrieved from International Federation of Journalists Web Site: https://www.ifj.org/media-centre/news/detail/category/press-releases/article/nepal-parliamentary-committee-passes-controversial-it-bill.html

Khadka, K. K. (2019). Interaction On IT BILL 2075. *ICT Frame.* Kathmandu: Internet Society Nepal.

Khatiwada, N. (2020). *Beware the fake news on Facebook.* Kathmandu: Annapurna Express. Retrieved from https://theannapurnaexpress.com/news/beware-the-fake-news-on-facebook-2531

Krippendorff, K. (1980). Content analysis an introduction to its methodology. London: Sage.

Lama, S. (February 13, 2019). *Nepal government tightens screws on social media.* Kathmandu: The Kathmandu Post. Retrieved from https://kathmandupost.com/national/2019/02/13/government-proposes-law-to-punish-those-writing-improper-things-on-social-media

Nepal Rastra Bank . (2020, November 04). Press News. गभर्नर अधिकारी सार्कफाइनान्स ग्रुप मिटिङ्गमा सहभागी.

Nepal Rastra Bank. (2020). *Payment Systems Oversight Report BS 2076/77.* Kathmandu: Nepal Rastra Bank.

Nepal Rastra Bank. (2076, January 10). Notice. सामाजिक सञ्जाल र अनलाईन मार्फत गरीने विज्ञापन प्रकाशन तथा प्रशारण बापतको भूक्तानी तथा प्राप्ती अनौपचारीक माध्यमबाट गरेमा गैरकानुनी हुने बारेमा नेपाल राष्ट्र बैंकको सूचना.

Nepal Telecom. (2020, November 13). *Nepal Telecom*. Retrieved from https://www.ntc.net.np/tariff/ftth-tariff

Nepal Telecommunications Authority (September, 2020). *Nepal Telecommunications Authority MIS Report* (16th ed., Vol. 188, Ser. 140, Rep.). Kamaladi, Kathmandu: Nepal Telecommunications Authority.

Nepal Telecommunications Authority. (2020, November 14). *Nepal Telecommunications Authority*. Retrieved from https://nta.gov.np/ne/nirdeshika/

Neupane, S. (2019). Interaction On IT BILL 2075. *ICT frame.* Kathmandu: Internet Society Nepal.

Office of the Auditor General. (2018). *Office of the Auditor General Annual Repoer.* Kathmandu.

Office of the Auditor General. (2020). *Office of the Auditor General Annual Report.* Kathmandu: Office of the Auditor General.

Office of the Auditor General. (2074). *IT Audit Report: The Legitimacy and Use of Information Technology Systems in Government Bodies.* Kathmandu: Office of the Auditot General.

Thirumal. P., G. M. (2011). India's Dalits Search for a Democratic Opening in the Digital Divide. In P. R. Leigh, *International Exploration of Technology Equity and the Digital Divide: Critical, Historical and Social Perspectives* (p. 20). IGI Global. doi: 10.4018/978-1-61520-793-0.ch002 Setopati. (11 June 2020). ईशानको फेसबुकबाट सुरू भएर बालुवाटार हुँदै देशभरि सल्केको आक्रोश *(the outrage started from ishaan's facebook and spread across the country through Baluwatar).* Kathmandu: Setopati.com. Retrieved from https://www.setopati.com/politics/208775?fbclid=IwAR0nt7PYyMFRe2ehiKDHx_o6wNSsmZz46CVdV3LaDGVkNFgsT92Kk9Q2Uro

Sharma, A. (2016). Information Communication Technology Development in Nepal. doi:10.18350/ipaid.2016.25.1.101

Sharma, G. (22 May 2019). *Nepal says bans WeChat Pay, Alipay.* Reuters. Retrieved from https://www.reuters.com/article/us-china-nepal-digitalpayments-idUSKCN1SS19N

United Nations. (2020, 12, 01). Retrieved from

United Nations Commission On International Trade Law: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce

World Internet Users Statistics and 2020 World Population Stats. (2020, October). Retrieved November 09, 2020, from https://www.internetworldstats.com/stats.htm.