Cyber Crime, Cyber threat, Cyber Security Strategies and Cyber Law in Nepal.

SHAILENDRA GIRI

Execuritve Director, Personnel Training Academy, Bagdol Lalitpur, Nepal

Abstract

Human life is depending on online services which are making daily life easy and smart but facing various challenges of cyber attract, threat and security. Huge numbers of criminal activities are increasing day by day using ICT tools and applications. Government organizations, citizens, business is being victims by cyber crime and threats. The risks of cyber attract and threat is very high. The cyber security strategies, policies, plan and law, help to protect e-government systems against threat and attack; and detect abnormal activities. The aim of this paper is to explorer cyber crime and cyber threat and security strategies and law. The content analysis and survey methods are used for this research. The study concluded that the government must conduct a professional analysis of cyber crime, cyber threat, cyber security, and cyber strategies. This article has discussed about the legal requirements of cyber security. If we are not able to design systems that secure human life and distinguish that usable solutions are not sufficient and a crucial component of strong security in the future. As we know that within a decade, observe our technology turned against us in continued and being more sophisticated day to day and how it made destructive attacks and threats. It shows that our future will not really happy and healthy due to cyber insecurity.

Keywords: *Cyber crime, cyber threat, cyber security, cyber law, e-Governance, e-Government.*

1. Introduction

One of the fastest growing areas [39] of crime including Information and Communication Technologies (ICT) and internet is Cybercrime. It is today's burning issue of each nation which is making world economic up and down. It is being essential to gain cyber security knowledge and skills, to help protect our digital life. The potential ICTs development and service delivery raises new challenges of the information technology society [51].Huge numbers of criminal activities are increasing day by day using ICT tools and applications. Government, business, citizens are facing problems as hacking, intellectual property theft, credit card cloning, phishing, software piracy, cyber terrorism, spyware, defamation, cyber flowers, computer virus, social violence using IT, cyber-bullying, privacy issue and so on.

The governments organizations, citizens, business are being victims by cyber, attract, crime and threats. According to Pande [32], modern technologies supply so as to commit various varies of criminal activities. These include attacks against computer data and information as well as systems. In 2007 and 2008 the cost of cybercrime worldwide was estimated at approximately

USD eight billion. As for corporate cyber intelligence, cybercriminals have stolen intellectual property from businesses worldwide worth up to USD one trillion [5].

The everyday life of citizens in modern societies relies on the critical services provided by government agencies, business organizations, and concern stakeholders. ICTs are using for ongoing operations, control, and monitoring activities, as well as for interactions involving data exchange from various sources including cloud computing [28-29]. Cyber-security for government systems has recently been gaining a lot of attention towards cyber attract and threat [31]. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are technologies that help to enhance the security environment of government agencies, private sector companies and citizens [2].

The computer networks that individuals and organizations, for the most part, might as well give up in their efforts to protect most of their databases [30]. Securing cyberspace, however, it is defined, is an extremely difficult strategic challenge that requires cooperation between the public and private sectors, military and civilian, of our societies [46]. Data protection is being difficult today. The whole world looking into computer databanks, government, public organization, and citizens have to make careful decisions about data and information security [30] and security is not just a technical issue [18]. Liu [29] have presented work to identify security requirements, Schumacher and Roedig [41] proposed a set of patterns, and Van Lamsweerde [49] defines the notion of anti-models, models that capture attackers, their goals and capabilities.

Hackers and cyber-criminals understand this phenomenon significantly; the majority of the discussions and research surrounding cyber-security are focused on the technical, security strategies and policy making of securing cyberspace [47]. The hackers, cyber criminals and terrorists become more technically sophisticated now. Cyber-security is constantly evolving and being updated, in order to adapt to today's fast-changing scenarios [27] and the security community must address root causes of cyber insecurity [3].

The objective of a cyber attack includes four areas: loss of integrity, loss of availability, loss of confidentiality and physical destruction [47]. The Internet and cyberspace revolution is changing the technology of the workplace and work environment [52]. There is a continuous awareness program to the citizens and training program to ensure people understand security threats, know-how, and to identify potential issues and behave accordingly to maintain secure e-government services [11-13]. Nepal has seen ups and downs in its technology but due to its limited policies and regulation; it is facing a huge hindrance in the coming days. Technology has been passed and Nepal is facing a huge threats and challenges in overcoming the online activities [42].

The cyber law is the law governing the digital world and it governs the security and privacy of information, crimes relating to the damages. The internal sources are the employees of private or public agencies, customers or end users in cyber threat. The external sources are hackers, criminal/terrorist groups or organizations, intelligence and investigating agencies in cyber threat. Threats to the assets may be of different types and of varying intensities and impact values [11-13]. The assets could be internal or external such as data, information, knowledge resources, programs, hardware, network and so on. The threat to security of ICT systems may be from many sources and in different forms.

Cyber laws have become essential in view of the rapid developments in ICTs. The states can respond to computer crime and related criminal law issues associated with these developments [42]. The most serious challenges of the 21st century are cyber attract, security and threats. Malicious use of ICT can easily be concealed. The growing sophistication and scale of criminal activity increases the potential for harmful actions [11-13].

This paper aims provide recommendations for policymakers to draft national cyber security strategies to respond to this growing threat. Paper also explores the competing paradigms for views problems of cyber security, and some of the strategies already implemented to identify best practices in national security strategy and cyber law.

2. Literature review:

2.1Cyber crime:

The term cybercrime refers to a variety of crimes carried out online, using the internet through computers, laptops, tablets, internet-enabled televisions, games consoles and smartphones [22]. It is also defined as technology enabled crime, IT crime, digital crime, electronic crime, virtual crime, net crime, and high technology crime. According to Halder & Jaishankar [10] defined Cybercrimes as: *"Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental hurt, or loss, to the victim directly or indirectly, victimization trendy telecommunication networks like Internet"*.

It is the crime that involves a computer, a network, new technology and devices [33] and the computer may have been used as a weapon of a crime, or it may be the target as well as technology and system [50]. Some forms of cyber crimes, natures and models became high profile, significantly those encompassing hacking, infringement of copyright, unwarranted mass-surveillance, erotica, software package piracy, material possession outlaw, cyber flower, false mail, defamation, and kid grooming [10].

A report revealed in 2014(sponsored by McAfee), calculable that the annual harm to the worldwide economy was $445 billion [8]. Approximately, $1.5 billion was lost in 2012 to online credit and open-end credit fraud within the United States [9]. In 2018, a study by Center for Strategic and International Studies (CSIS), in partnership with McAfee, concludes that on the point of $600 billion, the nearly simple fraction of worldwide value, is lost to crime annually [8].

2.2. Cyber threat:

Cyber attacks and cyber terrorism are the new looming threats on the horizon and the country needs to focus on specific areas to guarantee cybersecurity [6]. The threat to the security of ICT system may be from many sources and in different forms. Some of the internal sources of threat are the employees of private or public agencies, customers or end users of the programs. The external sources of threat **may** hackers, criminal/terrorist groups or organizations, intelligence and investigating agencies. Cybercrime not only threat a person or a nation's security and financial health of an organization but also victimize the social reputation too [44].

Threats to the assets may be of different types and varying intensities and impact values [12]. Threats to cyber security are often nearly divided into 2 general categories: actions geared toward and supposed to break or destroy cyber systems and actions that ask for to take advantage of the cyber infrastructure for unlawful. If you use e-mails connected to the Internet, it's being scanned, probed, and attacked constantly with the production of free hacking tools and cheap electronic devices [9]. Cyber fundamentals help us to guard against the most common cyber threats and demonstrate our commitment to cyber-security [19]. Threat actors will operate with substantial freedom from just about anyplace. Many malicious tools and methodologies originate within the efforts of criminals and hackers [12]. Public key infrastructure providing the required level of authentication. The integrity and to have a continuous awareness as well as training program to ensure citizens understand security threats know how to identify potential issues and behave accordingly to maintain secure Government services in the different parts of the country [12].

2.3. Cyber Security

Cybercrime encompasses any criminal act handling computers and networks; and includes ancient crimes conducted through the web [33]. The activity of protective information and knowledge systems like networks, computers database, data centers and applications with appropriate procedural and technological security measures is referred to as cyber-security. Firewalls, antivirus computer code, and other technological solutions for safeguarding personal data and computer networks are essential but not sufficient to ensure security.

Cyber-security has emerged as a longtime discipline for pc systems. Security helps to ensure the confidentiality, availability, and integrity of information systems by preventing Cyber security attacks [48]. Cyber-security covers physical protection each hardware and computer code of private data and technology resources from unauthorized access gained via technological means that is a challenging issue in the country public-private partnership may be a key element of cyber security. The public-private engagement may take a variety of forms and may address awareness, training, technological improvements, vulnerability remediation and recovery operations [12].

Enhancing cyber-security and protective crucial data infrastructure area unit essential to every nation's security. Cybersecurity plays an important role in the development of IT, as well as internet services. These five basic controls are essential for better cyber security in our organization [19]. 1) Use a firewall to secure your net affiliation, 2) Choose the most secure settings for your devices and software, 3) Control who has access to your data and services, 4)Protect yourself from viruses and other malware and 5) Keep your devices and software up to date. The traditional protections of small size and remote geography do not extend to cyber threats, attract and crime [20] The international recommendations for cyber security often mention human and technological capacity building and development [38].

Cyber security is very important to protect the IT services in the corporate establishment, government organizations as well as the one used by the general public. Developing countries where IT has reached the apex, the security of data compiled, stored and transmitted is almost

important [6]. No country has been able to claim the full understanding of possible reason for cybercrime and possible damages that can come from it. No cyber knowledge can be made controlled fully by security forces [42].

2.4.Cyber Security Strategies:

The inclusion of nasty hidden functions within the IT will undermine confidence in merchandise and services, and have an effect on national security [13]. Making the common subject of the country a lot of tuned in to the threats [6]. The prime concern of every nation is cyber-security today. The security situation of a country is affected by (1) country's own strategy to maintain security and execution of the strategy, (2) increasing globalization trends and (3) use and misuse of ICT practices of the country and global world. Safety and security have become the principal prerequisites and obligations of a sovereign nation. Scientific invention and innovation have altered the world and Nepal too [42].

The strategy's objectives included the reduction of cyber threats, the establishment of international support, capacity building, and public private cooperation [23]. There are competing paradigms for viewing the cyber security problems [34]. The motivations of nations developing national cyber security strategies. The designation of responsibility for cybersecurity within government is varies [24]. The strategy focused on the three objectives: (a) raise awareness among individuals and small business, (b) improve government cybersecurity, and (c) build strategic relationship to secure critical infrastructure. The United States published an international strategy for cyberspace security [45]. The United States divided responsibility between defense and homeland security [40]. Panama focused on six pillars in its strategy: protecting privacy and human rights, prevention and punishment of cybercrime, fortifying national critical infrastructure, building a national cybersecurity, industrial foundation, developing an ethnicity of cybersecurity, and improving the security and response capability of public entities [38].

Cyber-security helps to protect government systems against attack, detect abnormal activities services. Information security practice is needed to protect e-governance projects. Security policy, plans, practices procedures must be in position as well as utilization of security technology [13]. The organization's cyber security level and cyber security is verified by independent experts [19].There is several key recommendations to improve the current cyber-security posture [6].

- Accept cyber terrorism as a viable near term threat, organize for success and establish the new Department of Cyber Security and debate the issues with the Parliament and the public to raise awareness.
- Increase punishment for cyber crimes with terror or death as a motive and finalize the national cyber security plan and implement it.
- Commit Parliamentary functioning to improve cyber security and manpower training to implement the plan effectively.

2.5.Cyber Law:

Cyber law is the law that has a spread of problems associated with the web and different communication technology, as well as belongings and jurisdiction which

control the cyber space. In Nepal cyber law is called as Electronic Transaction Act (ETA) 2063 [15], which were passed in 2004. Cyber law is the law governing the facts that happen in the intangible digital world such as giving legal status to the intangible information in the cyberspace [13]. The cyber laws area unit vital and valid for control cyber matters [4]. The Government needs to be transparent in its function and for the same [26]. It is the accountability of the State to bring in sufficiently strong legislation to discourage cyber crime, threat, attract and put down the abuse of the Internet and other cyber media for any illegal activities [14].

Security is mainly about safeguarding the ICT tools of any organization. The assets could be internal or external such as data, information, knowledge resources, programs, hardware, and networks and so on [13]. Cyber warfare poses a large threat to highly computerized societies and culture. No country has been able to develop a safety policy that guarantee full security in the communication practices within the context of globe [42]. Regulatory changes are required for a host of activities from procurement to service delivery [13]. Different countries have completely different cyber laws and cyber laws control bodies. In Nepal, cyber law is termed as Electronic dealing Act (ETA) 2063 which is available at: http://www.lawcommission.gov.np.

Due to lack of proper mechanism to rule, monitor and policies. The technology may threats the nation by criminal activities [32]. Cyber laws are very important. They provide security not only to the intellectual property of IT companies but also help to maintain the privacy of internet users. It helps to keep us safe and to boost the IT economy in the world.

3. Methodology

Cyber crime is one of the fastest growing areas of crime around the globe. Nepal is not an exception to attract, threat of cybercrime. Increasing internet and computer users and the growth of technology are grooming cyber crime. Nepal faces a huge hindrance due to its limited policies and regulation. Cybercrimes has grown day by day, individuals, organizations, and governments have struggled to find ways to defend against the cyber attract and threat. IT is changing all aspects of human activity and in such case Cyber law is essential now. The survey and content analysis methods are using during this research. The survey data collected from government employees who are on duty at different part of the nation. International journals, books, government reports are also reference of the study.

4. Result and Analysis

Huge numbers of criminal activities are increasing day by day using ICT tools, infrastructure and applications. Government organizations, citizens, business are being victims by cyber crime and threats. Government employees know about cybercrimes, cyber threat, cyber security and cyber law. It is revealed in Table 1. 85.7% of respondents responded that they are aware of cybercrime, threat, security and law.

Table1: Do you know about the cybercrime, threat, security and law?

No	20	14.3 %
Yes	120	85.7 %
Total	140	100.0 %

Fieldwork 2018

How have respondents understood the meaning of cybercrime? An inquiry was made on it. Table 2 gives the meaning of cybercrime as respondents understood: Taking or giving information by unauthentic use of other person's computer (76.4%) stated unauthentic use of other person's computer, mobile, telephone, ATM card (73.69) etc. is found to be taken by the respondent as cybercrime. Similarly, other definitions as understood by respondents include leakage of personal as well as official information (74.3) and unauthentic upload of video, audio and photo in the social media site (72.1%) Offense against the nation using IT (73.6%) Threatening and harassing someone through telephone, mobile, internet, email and other electronic media (72.1 %) and Hacking passwords, Wi-Fi, websites in order to hamper the dignity of a person, family, society, unions, organization and nation (71.4) are the major cyber crime activities.

Table 2 : What is cybercrime in your opinion?

Leakage of personal as well as official information	104	74.3 %
Taking or giving information by unauthentic use of other person's computer	107	76.4 %
Unauthentic use of other person's computer, mobile, telephone, ATM card etc	103	73.6 %
Unauthentic upload of video, audio and photo in the social media site	101	72.1 %
Like, comment, share of other person's statements in social media site	95	67.9 %
Publishing statements and photos that hampers/ maligns someone's personal dignity	100	71.4 %
Exacerbating someone's photo and upload it	97	69.3 %
Misusing photos of children, young and old people and put it in indecent and adult sites	97	69.3 %
Hacking passwords, Wi-Fi, websites in order to hamper the dignity of a person, family, society, unions, organization and nation	100	71.4 %
Threatening and harassing someone through telephone, mobile, internet, email and other electronic media	101	72.1 %
Offense against the nation using information technology	103	73.6 %

Source: Fieldwork 2018

5. Discussion

Cyber security is considered as a national security. An issue of each nation could impact the lives of citizens each day [1]. Implementation of commanding national cyber security strategies must enhance the percentages for fulfillment. Cyber security coverage that inhibits loose expression within the name of safety is inconsistent with human right.

For the protection of e-governance projects, there is a need for information security based practices. Security policies and plan help to protect e-government systems against threat and attack, and to detect abnormal activities services.

UK cyber security method set up a brand new workplace of cyber security inside the cabinet workplace at the side of multi-enterprise cyber security operation middle located within the army headquarters [7]. The U.S. cyber security strategy turned into additional weighted in the direction of national security models [25][35][36][37]. The law deals with problems associated with a

digital signature, belongings, cybercrime, etc. Due to lack of proper monitoring, supervision, and updates, protecting user's online data through cyber law is present.

The global and regional agencies inclusive of the ITU [17], European Union [16], and OECD [43] have posted pointers for national cyber security strategy development. The private sector's function in national safety approach has all started to emerge. The method blanketed recommendations for setting up excessive stage government accountability for cyber-security, establishing a national cyber-security coordinator, and the improvement of training packages for most of the people and the cyber-security workforce [17]. Why not recruit cyber army and make different defense cyber security force?

6. Conclusion

As disruptive activities using ICTs are more complex and dangerous in the cyberspace. The hackers, cybercriminals, and terrorists become more technically sophisticated now. It concludes that the security community must address root causes of cyber insecurity. Actions for securing information and information systems are required to be done at different levels in the e-Governance activities. The responsibility of the State is to herald sufficiently sturdy legislation to discourage and place down the misuse of the web and other cyber media for any nefarious activities. Network services providers (ISP), large businesses and small users/home users are also required to play their role to enhance the security of cyber space within the country. This paper has discussed the cyber crime, threat, security strategies, and legal requirements of Cyber security, security training and awareness in providing a comprehensive e-Governance initiative. Further research is required in the e-Governance vision, policies and strategies. If we are not able to design systems that secure human life and distinguish that usable solutions are not sufficient and a crucial component of strong security in the future. As we know that within a decade, see our technology turned against us in continued and being more sophisticated day to day and destructive attacks and threats. It shows that our future will not really happy and healthy due to cyber insecurity.

7. Recommendations

Department of Information and Technology of Nepal (DoIT) [21] has provided suggestions regarding Cyber security:

- Use strong Passwords and use different user ID. Make the password more complicated by combining letters, numbers, and special characters and change them regularly.
- Don't share it with anyone. Avoid replying unknown emails and do not open emails from unknown sources. Do not respond to emails asking for personal information, credit card number, pin-code, password etc.
- Keeping word/ PIN codes safe and memorize. Read privacy and policy statements before any transaction.
- Surf only through a secure website. Log out immediately after completed online job.
- Check account statement to ensure that unauthorized transaction has taken place or not. Safe online banking and online shopping and safely access Social networking websites.
- Be careful whereas communication with persons met online
- Make friends only known friends. Remove inappropriate information from profile. Do not post personal information on social media. While using the internet at public place remember that

internet browsers like IE, Mozilla Firefox, Gmail, Hotmail etc. will save password on that browser and account may be hacked.

- Firewalls monitor open connections including attachments in an email, block unauthorized inbound and outbound internet traffic and disable internet add-ons such as cookies, pop-ups etc.

Acknowledgement

This work was supported by Rapti Engineering College which is located at Ghorahi-16, Dang Nepal. I would like to express my deep gratitude to Professor Dr. Subarna Shakya my research supervisor for their patient guidance, enthusiastic encouragement and useful critiques of this research work. I am always pleased to Personnel Training Academy-PTA, Bagdol Lalitpur Nepal. I would also like to thank my parents, family and staffs for their support and encouragement throughout my study.

References

[1] A. Klimberg (ed). National cybersecurity framework manual. Trailing, Estonia: NATO CCD COE Publication, (2012).

[2] A.M. Dario SGOBBI and Marco PAGGIO. Intrusion in a Mission Critical Network: A Tutorial on Intrusion Detection Systems and Intrusion Prevention Systems. Modelling Cyber Security: Approaches, Methodology, Strategies U. Gori (Ed.), (2009) IOS Press, doi:10.3233/978-1-60750-074-2-68.

[3] A.VIDALI. Striking the Balance: Security vs. Utility. IOS Press BV Nieuwe Hemweg 6B 1013 BG Amsterdam Netherlands, (2009).

[4] Administration Reform Implementation Report (ARIR). High level administrative reform implementation and monitoring committee, Singhadarbar, Nepal, (2014).

[5] Asian Development Bank Report, (2007).

[6] C. Subramanian. Cyber Security. International Journal of Recent Scientific Research, (2012). 3(3) pp 197-200. Available online at: http://www.recentscientific.com.

[7] Cabinet Office. Cyber security strategy of the United Kingdom: safety, security and resilience in cyber space, (2009). Available at: www.cabinetoffice.gov.uk/media/216620/css0906.pdf, retrieved at 3 February, 2019.

[8] Lewis, James (February 2018). "Economic Impact of Cybercrime -No Slowing Down" (PDF).

[9] Cybercrime— what are the costs to victims - North Denver News". North Denver News. 2015-01-17. Retrieved 15 January 2019.

[10] D. Halder and K. Jaishankar. Cyber crime and the Victimization of Women: Laws, Rights, and Regulations, (2011). Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9.

[11] D. Kumar and N. Panchanatham A study on Cyber law in promoting E-Governance, AE International Journal of Multidisciplinary Research, (2015a), May 2015.

[12] D. Kumar and N. Panchanatham Enforcing Transparency in Indian E-Governance Through ICT, International Journal of Business Management & Research, (2015b), Jan 2015.

[13] D. Kumar and N. Panchanatham. A case study on Cyber Security in E-Governance. International Research Journal of Engineering and Technology (IRJET), (2015). 2(8) pp 272-265. Available at: www.irjet.net

[14] D. Kumar and N. Panchanatham. Strategies for Rebooting the Government in e-Mode. Global Journal for Research Analysis, (2014a). Aug 2014, Vol 3 Issue 8.

[15] Electronic Act 2063.Government of Nepal. Available at: www.lawcommission.gov.np Retrieved at 5 February, 2019.

[16] European Commission. High Representative of the European Union for Foreign Affairs and Security Policy. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and The Committee of the Regions. Cybersecurity strategy of the European Union: An open, safe and security cyberspace, (2013). Available at: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=167.

[17] F. Wamala. The ITU national cybersecurity stragegy guide. Geneva, Switzerland: International Telecommunications Union, (2011). Retrieved from www.itu.int.

[18] H. MOURATIDIS Secure Software Engineering: Developing the New Generation of Secure Systems by Introducing a Security Focus Throughout the Development Lifecycle. Modeling Cyber Security: Approaches, Methodology, Strategies U. Gori (Ed.), (2009). IOS Press.

[19] https://www.cyberessentials.ncsc.gov.uk/ Retrieved at: 05 March 2019.

[20] Ragnarsson, J.K., & Bailes, A.J. (2010). Iceland and cyber-threats. Retrieved from http://skemman/is/stream/get/1946/19284/STJbok-ritstvrt-helld.pdf#page-69.

[21] https://www.doit.gov.np/en/page/cyber-security-awareness. Accessed at 23 February 2019.

[22] https://www.victimsupport.org.uk/crime-info/types-crime/cyber-crime. Retrieved at: 04 March 2019.

[23] Phahamohlaka, L., Jansen van Vuuren, J., & Coetzee, C. (2011). Cybersecurity awareness toolkit for national security: An approach to South Africa's cyber security policy implementation. Proceeding of the South African Cyber Security Awareness Workshop (SACSAW 2011). Retrieved from http://www.csir.co.za/dpss/docs/SACSAWFinal_16Aug.pdf.

[24] Republica de Panama (2013). Elements de la strategia national de seguridad ciberneticay protection de infrastructure critia (Gacta Oficial Digital No. 27289. Resolucion No. 21). 34-43. Panama, Panama: Consejo Naclonal para la Innovation Gubernamental, Republica de Panama.

[25] K. Newmeyer. Who should lead U.S. Cybersecurity efforts?, (2012). Prism, 3(2), 99-120. Available at: http://www.ndu.edu/press/lib/pdf/prism3-2/prism115-126_newmeyer.pdf.

[26] Kumar D. and Panchanatham N. Strategies for Effective E-Governance Management, International Journal on Global Business Management & Research Vol 3 Issue 1, (2014b) , Aug 2014.

[27] L.Serena. A Fuzzy Approach to Security Codes: Cryptography between Technological Evolution and Human Perception (2009). Modeling Cyber Security: Approaches, Methodology, Strategies U. Gori (Ed.) IOS Press, doi:10.3233/978-1-60750-074-2-43.

[28] Lewis, James. "Economic Impact of Cybercrime - No Slowing Down" (PDF), (February 2018).

[29] Liu, L., Yu, E., Mylopoulos, J., Security and Privacy Requirements Analysis within a Social Setting, In Proceedings of the 11th International Requirements Engineering Conference, (2003) pp. 151-161, IEEE Press.

[30] N. AHITUV. Thoughts on the Open Information Society: Does the Concept of "Privacy of an Organisation" Exist?. IOS Press BV Nieuwe Hemweg 6B 1013 BG Amsterdam Netherlands, (2009).

[31] P. SITBON. A Cyber Security Approach for Smart Meters at ERDF. Modeling Cyber Security: Approaches, Methodology, Strategies U. Gori (Ed.). (2009). IOS Press, doi:10.3233/978-1-60750-074-2-93.

[32] Pandey, B. P.(2017), Challenges of the grievance handling in public service delivery and the use of information technology, Journal of Personnel Training Academy. Lalitpur: PTA, Nepal. 5(l). 1, pp. 124-136.

[33] R. Moore. "Cybercrime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing, (2005).

[34] Mulligan, D.K. & Schnelder, F.B.(2011). Doctrine for cybersecurity. Daedalus 140(4), 70-92. Doi:10.1162/DAED_a_00116.

[35] R.J. Harkneet and J. Stever. The cybersecurit triad: Government, private sector partner, and the engaged cybersecurity citizen, Journal of Homeland Security and Emergency Management, (2009). 6(1), Article 79. Doi:10.2202/1547-7355.1649.
[36] R.J. Harkneet and J. Stever. The new policy world of cybersecurity. Public Administration Review, (2011). 71(3), 455-460. Doi:10.1111/j.1540-6210.2011.02366.x.
[37] R.J. Harkneet, J.P. Callaghan, & R. Kauffman. Leaving deterrence behind: War-fighting and national cyber security. Journal of Homeland Security & Emergency Management, (2010). 7(1), 1-24.
[38] False, N., Gavrila, R., Rlenstrup, M.R., Moulinous, K.(2012). National cyber security strategies: Practical guide on development and execution. Retrieved from http://www.enisa.europa.eu/acrivities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strageties-an-implimentation-guide
[39] S. Giri & R. L. Shrestha. Reform of civil service of Nepal with e-government practice. Journal of Personnel Training Academy, (2018) 6(1)6. Pp. 22-36.
[40] Newmeyer, K. (2012). Who should lead U.S. cybersecurity efforts? Prism, 3(2), 99-120. Retrieved from http://ndu.edu/press/lib/pdf/prism3-2/prism115-126_newmeyer.pdf.

[41] Schumacher, M., Roedig, U. Security Engineering with Patterns, in the Proceedings of the 8th Conference on Pattern Languages for Programs (PLoP), (2001). Illinois – USA.
[42] Shrestha, T.M. and Ojha, S.K.(2017). Globalization, ICT and national security issues. Journal of Personnels Training Academy. Lalipur: PTA, Nepal. 5(1),5, 8-29.
[43] Smith, Geoff et al.,. Cybersecurity Policy Making at a Turning Point: Analyzing a New Generation o National Cybersecurity Strategies for the Internet Economy. Organization for Economic Cooperation and Development, (2012). Available at http://www.oced.org/sti/ieconomy/cybersecurity%20polivy%20making. pdf.
[44] Steve Morgan. "Cyber Crime Costs Projected To Reach $2 Trillion by 2019", (2016). Forbes. Retrieved September 22.
[45] Obama, B. (2011). International stragegy for cyberspace: Prosperity, security and openness in a network world. The White House.

[46] U Gori. MODELLING CYBER SECURITY: APPROACHES, METHODOLOGY, STRATEGIES, (2009) IOS Press BV Nieuwe Hemweg 6B 1013 BG Amsterdam Netherlands.
[47] U.S. Army Training and Doctrine command, Cyber Operations and Cyber Terrorism, Handbook No. 1.02 August 15th, 2005 P.II-1 and II-3.
[48] V. Gurusamy and B. Hirani. Cyber Security for Our Digital Life (2018) Proceeding Paper· February 2018. Available at: https://www.researchgate.net/publication/323605373. Retrieved on 1 February 2019.
[49] Van Lamsweerde A. Elaborating Security Requirements by Construction of Intentional AntiModels, Proceedings of the 26th International Conference on Software Engineering, Edinburgh, May, ACM-IEEE, (2004) pp. 148-157.
[50] Warren G. Kruse and Jay G Heiser. Computer forensics: incident response essentials, (2002). Addison-Wesley. p. 392. ISBN 978-0-201-70719-9.
[51] www. unpan1.un.org/intradoc/groups/public/documents/un/unpan021888.pdf.
[52] Z.K. Shalhoub and S. L. Qasimi. Cyber Law and Cyber Security in Developing and Emerging Economie., (2010). Published by Edward Elgar Publishing Limited. The Lypiatts 15 Lansdown Road Cheltenham Glos GL50 2JA UK.