International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-8, Issue-2, Feb 2020 E-ISSN: 2347-2693

High Risk of Cybercrime, Threat, Attack and Future Challenges in Nepal

Shailendra Giri[1], Subarna Shakya[2*]

[1] Dept. of Government of Nepal, Ministry of Federal Affairs and General Administration, Singha Durbar Kathmandu, Nepal
[2]Dept. of Electronics and Computer Engineering, IOE, Tribhuvan University, Nepal

[*]*Corresponding Author: drss@ioe.edu.np, Tel.: 0977-9851232328*

DOI: https://doi.org/10.26438/ijcse/v8i2.4651 | Available online at: www.ijcseonline.org

Accepted: 14/Feb/2020, Published: 28/Feb/2020

Abstract— Government organizations, citizens, businesses are being victimized by cyber-attacks, crimes, and threats. Globally people have been using cyber safety in every sector of daily life but huge numbers of criminal activities are increasing day by day using ICT tools and applications. The purpose of this paper is to explorer the high risk of cyberattacks, crime, threat and future challenges in Nepal. The study was carried out using content analysis, analysis of various survey reports and in-depth interviews with subject experts. The study claims that high risk of a cyberattack, crime, and threat have been increasing unexpectedly in various sector of Nepalese society. It is essential to make a common strategy to reduce the increasing technical risk related to cyber. The risk of cyberattack, crime, and threat is very high. So, IT audit must be made compulsory in each and every organization and original operating system as well as application software used. Strong cybersecurity precautions and technologies ought to be adopted during the installation of ICT automation. The paper claims that not only the banking sector but also the Government of Nepal should appoint cybersecurity personnel in their services so that the expert team will be able to fight against the cyber attack. As time is demanding 'Cyber Army' in Nepal, the Government should not delay forming a new force 'Cyber Army'.

Keywords— Cyber crime, Challenges, Cyber threat, Cyber attack, IT audit, e-governance

I. INTRODUCTION

Governments organizations, citizens, businesses are being a victim by cyberattack, crimes, and threats. Huge numbers of criminal activities are increasing gradually using ICT tools and applications. Government, business, citizens are facing problems due to hacking, intellectual property theft, credit card cloning, phishing, software piracy, cyber terrorism, spyware, ransomware, morphing, defamation, cyber flowers, computer virus, social violence using IT, cyber-bullying, pornography, privacy issue and so on [1].

The development of technology is making the life of a person, society, and nation easy. The development of the internet has made the globe a small village as well as the family. As science and technology are advancing, technological crimes are also increasing rapidly. These days, cybercrime is being a headache of a nation in the world [2]. Hackers enter the secret database and personal information of other stakeholders using a stolen password and use and misuse the hacked data and information [3]. Economic activities depend on information communication and technologies (ICTs). Nepal has been using electronic banking service since few years. Mobile banking service has also started in Nepal which is being popular among citizens but Banks are on target by hackers these days [1].

The everyday life of citizens in modern societies relies on the crucial services provided by government agencies, business organizations, and concern stakeholders. ICTs are being used for ongoing operations, control, and monitoring activities, as well as for interactions involving data exchange from various sources including cloud computing [4]. The government has been paying attention towards the cyber-security for government systems [5]. Cyber attacks are a persistent threat to businesses and charities not only in Nepal but also in the Globe [6]. Cybersecurity expert Saroj Lamichhane states that the government's cybersecurity system is very poor. Data security is major concern to data provider. It is better to use a door delivery system through ICT to protect cyberspace in the future [7].

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 policymaking of securing cyberspace [8]. The hackers, cybercriminals, and terrorists have become more technically sophisticated now. Cyber-security is continually advancing and being refreshed, so as to adjust to the present quick changing situations. The security network must address the underlying drivers of cyber insecurity [9]. In cyberspace, disruptive activities using ICTs are more

complex and dangerous nowadays. Cybercrime not only threatens a person or a nation's security and financial health of an organization but also victimizes the social reputation too [10].

The threat of terrorism forces authorities to address security vulnerabilities related to information technology infrastructures such as power plants, electrical grids, information system and the computer system of government and important organizations. The cybersecurity strategies, policies, plan and law, help to protect e-government systems against threat and attack; and detect abnormal activities. The increase of recent incidents and breaches of cybersecurity demonstrates the challenge all users (governments, organizations and citizens alike) of the Internet face to keep up with the speed of ICT evolution. Cybersecurity is an integral and indivisible part of technological progress. As an application of cybersecurity is a continuous process that needs to match ongoing cybercriminal activities and threat campaigns [11].

The objective of this paper is to explore the high risk of cyber crime, threat and attacks; and future challenges in Nepal**.** This paper discusses about:

1. current scenario of cybercrime in nepal,
2. high risk of cyber attack,
3. future of digital economy and challenges,
4. global cybersecurity index 2018,
5. security to cyberspace and
6. conceptual framework.

Further it deals with result and analysis, discussion; and conclusion and recommendations.

II. LITERETURE REVIEW

A. Current scenario of Cyber Crime in Nepal

Senior Superintendent of Police Nabinda Aryal at the bureau says, 'Some 5 to 20 persons visit the bureau to file complaints on a daily basis, and most of them are girls and women'. Police record shows that incidents of cybercrime have drastically increased in the past three years. A total of 1,318 cybercrime cases were filed in fiscal 2016-17. The number had increased to 1,694 in fiscal 2017-18 and 2,209 in fiscal 2018-19. Comparative data of three years shows that cybercrime grew by nearly 37 percent from 2016 to 2019. Among all the complaints, police record shows that above 90 percent of complaints are related to Facebook, followed by Youtube, Imo and WhatsApp simultaneously [2].

According to a police report, the law enforcement agency filed 85 cases of cybercrime against 93 persons in 2018. Cheating, blackmailing, phishing, identity theft, hacking, spreading hate and inciting violence, circulating lewd photos and videos and cyber grooming were major forms of cybercrime reported to the law enforcement agency. Around 60 percent of the alleged victims were women and unemployed youths [11].

Metropolitan Police Crime Division (MPCD) reported that upwards of 926 cases of cybercrime have been accounted for during the seven months of this fiscal. Even foreign nationals living in Nepal have been found involved in cybercrime. Most of the frauds use foreign mobile numbers to lure the victims into depositing cash in their bank accounts on the pretext of sending those parcels and lottery amount. As all social networking sites are open to all, it is impossible for the police to track down the criminals unless the victims themselves identify them randomly. One way to stay safe from such unsure calls or texts is to inform the police immediately after receiving such calls. People should also avoid entertaining such calls or messages [2].

According to the Metropolitan Police Crime Division, 221 complaints regarding crimes on social media sites were filed in the fiscal year 2015/16. However, this number had increased to 769 complaints in the fiscal year 2016/17. This shows that people are still unaware of the cybercrimes and their impacts on society. According to Kathmandu District Court, a total of 50 cases were filed in fiscal year 2015/16 out of which 19 cases of harassment of women were ported. Only 27 cases were filed in fiscal year 2016/17 out of which 14 cases of harassment were reported [4]

Table 1: Complain about Cyber attract, threat and crime

2074/075		**2075/076**	
Social Media	50	Social Media	70
Hacking	2	Hacking	7
SMS threat	11	SMS Threat	6
Phishing	0	Phishing	9
YouTube	2	YouTube	10
Simple complain	**1482**	**Simple complain**	**1912**

Source: Metropolitan Police Crime Division, 2019.

Table 1 shows that cybercrime is increasing every year compared to past years. Social media like Facebook, Twitter, LinkedIn, WhatsApp, Viber, Messenger are mostly used as a medium. YouTube has also played a key role in the increase in crime and threats. Event of cyberattacks like hacking has also taken place in Nepal from time to time. The government and other organizations' websites, banks server and important data of Nepal police also got hacked in the past [1]

Least a few years later Nepal is also being a victim of cybercrime, threat, and attacks. It is being a great challenge for the nation to control cybercrime in time. Various reports reveal that cybercrime, threat, and attacks are increasing unexpectedly. Cybersecurity and control mechanism is very poor in banks and other organizations. Basically, crimes are being committed using social media and different

technologies that are being hurdled for e-governance implementation. Threat Report 2018 attempts to present an even bigger picture of Cybersecurity in Nepal compared to Threat Report 2017 published last year [12].

B. Global Cybersecurity Index 2018

More than half of the world population is currently using online services. 3.9 billion individuals were utilizing the Internet before the finish of 2018, 51.2 percent of people as well. As per the ITU Connect 2030, expanding the requirement for a more cyber secure space, there will be a 70 percent Internet penetration by 2023. The global average cost of a data breach was up 6.4 percent in 2018. Because of the lift in the utilization of ICTs, the anticipated cybercrime cost will be an expected USD 2 trillion before the finish of 2019. There have been fewer ransomware attacks in hundreds of universities. The global average cost of a data breach was up 6.4 percent in 2018 . At the same time due to the boost in the use of ICTs, the projected cybercrime cost will be an estimated USD 2 trillion by the end of 2019. There have been fewer ransom-ware attacks, but more personal data breaches and critical infrastructure breaches, and this included hundreds of universities [11].

Table 2: Position of Nepal in Global Cybersecurity Index (GCI) 2018.

Member	State Score	Global Rank
Nepal	0.260	109

Source: GCI Report 2018.

The Global Cybersecurity Index (GCI) is an initiative of the International Telecommunication Union (ITU). As stated in table 2, Nepal is ranked 109th in global ranking with state score 0.260, which is not satisfactory in the global map.

C. High Risk of Cyber attack in Nepal

It seems that Nepalese banks are at high risk of international cyber attract and hacking. Former DIG Nepal Police Hemant Malla claims that not only the banking sector but also other sectors of society are at high risk. He further claims that the banking sector is not able to audit cybersecurity and they do not have computer security, response teams. So, the Nepalese digital economy is at high risk. Most of the banks in Nepal have been using traditional techniques and have not been able to increase organizational capability in technology. Most of the banks believe that their ICT management system is very high but practical citizens do not find that. Actually, their ICT management system is very poor. Banking personnel believes that they have been using not only pirated application software but also the operating system too. Assemble personal computers are not upgraded for a long time and their admin password is not changed from time to time [12].

Open border with India and issuing on-arrival visa to the foreigners also cause to increase the cybercrime in Nepal, again he said. The government is giving priority to the digital economy but that is causing technological risk and many challenges to digital security. Most of the tourists are not too able to use mobile for payment. Nepalese banks do not perform cybersecurity audits. In the globe, CIRT is compulsory for police but in Nepal, the government is not paying attention to it. So, hackers are pleasing benefit from it [4]. Due to poor firewalls, ransom-ware may enter the computer and there is a high chance to destroy the personal data, information, and files. Mobile applications are also causing the risk of computing technology due to their poor security system. It is essential to make a common strategy for minimizing the increasing technological risk. It is the fact that we need to hire experts from a foreign country where there is any cybersecurity issue to be solved. The pertaining questions to this issue are that the government still does not believe Nepali cyber experts. [13].

D. Future of Digital Economy and Challenges

The most serious challenges of the 21st century are cyber attack, crime security, and threats. Malicious use of ICT can easily be concealed. The growing sophistication and scale of criminal activity increase the potential for harmful actions [14]. ICT presents one of the most critical modern challenges to global security. With cybersecurity taking center stage globally, it is imperative that nations all over the world implement solutions to provide a safe space for Internet users in their country and stay engaged to improvement according to the incoming challenges [15].

The digital economy is increasing rapidly in the Asia Pacific region, which is demanding digital connection. The digital economy is being an essential issue in the present era. China can be a good example of where a digital payment system is highly developed. Researchers state that tech companies take important decisions on the basis of data and information. But in this context secrecy of the stakeholder is being a major concern and discussion. Tech companies want to increase their business dimensions in different sectors of economic using mobile payment. The burning issue is the control mechanism of the digital economy. Banks should upgrade their systems from time to time. It is not the condition to be far-away from modern information technology [16].

Due to the cyber attack in different sectors of Nepal, it is compulsory to perform cybersecurity audits in each and every government and nongovernment organization. But it is not the banks' priority. IT expert Rajanraj Pant claims that Nepalese banks and government organizations are paying their attention in profit gain, not in cybersecurity [12].

E. Security to Cyber Space

It is essential to pay attention to cybersecurity by recruiting cyber expert employees. The government must conduct a professional analysis of cybercrime, cyber threat,

cybersecurity, and cyber strategies. Over a decade, we have experienced and observed that technologies have evolved more sophisticated being prone to. It shows that our future will not really happy and healthy due to cyber insecurity [1].

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. The organization's cybersecurity level and cybersecurity are verified by independent experts [17]. Cybersecurity regulation designates laws dealing with data protection, breach notification, cybersecurity certification/standardization requirements, implementation of cybersecurity measures, cybersecurity audit requirements, privacy protection, child online protection, digital signatures and e-transactions, and the liability of Internet service providers [16].

F. Conceptual Framework

The ITU framework for international multi-stakeholder cooperation in Cybersecurity aims to build synergies between current and future initiatives, and focuses on the following five pillars [5]:

1. **Legal:** Measures based on the existence of legal institutions and frameworks dealing with Cybersecurity and cybercrime.
2. **Technical:** Measures based on the existence of technical institutions and frameworks dealing with Cybersecurity.
3. **Organizational:** Measures based on the existence of policy coordination institutions and strategies for Cybersecurity development at the national level.
4. **Capacity building:** Measures based on the existence of research and development, education and training programs, certified professionals and public sector agencies fostering capacity building.
5. **Cooperation:** Measures based on the existence of partnerships, cooperative frameworks, and information sharing networks.

These five designated areas form the basis of the indicators for GCI because they shape the inherent building blocks of a national cybersecurity culture.

III. METHODOLOGY

The study was conducted using content analysis, various national and international survey report analysis and in-depth interviews with subject experts. Books, websites, and journals are being supporting materials

IV. RESULTS AND ANALYSIS

The result and analysis are carried out with the help of survey data which is available in different reports. The result is verified with view of subject experts.

Table 3: Cybercrime legislation globally

Yes	91%
No	9%

Data source: GCI Report 2018.

Emerging cyber threats could precipitate massive economic and societal damage, and international efforts need to be agreed and acted upon in response to this new trend [5].

In 2018, cybercrime legislation is globally well implemented. The table 3 reveals that most countries have cybercrime legislation (91%), i.e. about 177 countries, which has improved from 2017 (79%).

Table 4: Global Percentage of National Cybersecurity strategy

Yes	58%
No	42%

Source: GCI Report 2018.

Global national cybersecrity strategy is very essential these days to fight against the cyber crime, threat and attack.

The table 4 shows that 58 percent of the nations agree to set their national cybersecurity strategy together which is a positive point for other countries like Nepal.

Table 5 . Global Percentage of Cybersecurity metrics

Yes	47%
No	53%

Data source: GCI Report 2018.

The global percentage of Cybersecurity metrics is not satisfactory which is found in the table no 5.

Table 5 shows that 47 percentages of countries have metrics to measure cybersecurity development at a national level while 53 percent do not have.

Table 6. Professional training globally

Yes	**63%**
No	**37%**

Data source: GCI Report 2018.

As part of enhancing collaboration in Cybersecurity, the commitment of governments to participate in Cybersecurity events is hereby measured. Such events include regional and international workshops, conferences and trainings.

Table 6 shows that 63 percent of member countries provide professional trainings in security and 37 percent do not offer trainings. That is why people are unknown about cybercrime and security.

Table 7. Participation in international forums globally

Yes	79%
No	21%

Data source: GCI Report 2018.

Table 7 shows the participation of member countries in international forums. According to the table 7, 79 per cent of member countries participate in international forums whereas 21 per cent do not. Participation in international forums and associations dealing with cybersecurity is high (79%).

V. DISCUSSION

It is essential to find the intention of foreigners why there are in Nepal? It is also necessary to analyze their objectives? If so, hackers could not able to enter the banking system and not be able to rob money. Banks and government organizations are being hacked from time to time and they are on target. What type of foreign equipment and accessories is being used in our system? Are our personnel qualified and capable to fight against the cyberwar? These questions have been raised by citizens. The strategy is focused on the three objectives: (a) raise awareness among individuals and small businesses, (b) improve government cybersecurity, and (c) build a strategic relationship to secure critical infrastructure. The United States published an international strategy for cyberspace security [18].

VI. CONCLUSION AND FUTURE SCOPE

Cybercrime is increasing every year compared to past years. Social media like Facebook, Twitter, LinkedIn, WhatsApp, Viber, Messenger are mostly used as a medium. YouTube has also played a key role in the increase in crime and threats. Cybersecurity Index (GCI) 2018 showed that Nepal is ranked 109th in the globe. Training on cybersecurity is one of the key points to control the cyber crime and threat. Now, Participation in international forums and associations dealing with cybersecurity is high. Cybercrime legislation is globally well implemented and it is quite satisfied. Many of the nations are agreed to set their national cybersecurity strategy together which is a positive point for other countries like Nepal.

The paper claims that not only the case of banking but also the government of Nepal has accepted that all-rounder cybersecurity personnel should be appointed in government services so that expert teams will be able to fight against the cyber attacks. By provide knowledge and capacity building training to personnel, they would be able to protect their system, network, and server from attack and hacking. There should not be any delay regarding enhancing the capability of the cybersecurity force. The time is demanding the 'Cyber Army' in Nepal. The Government should not delay forming a new force 'Cyber Army'.

VII. RECOMMENDATIONS

Some recommendations provided by Sunil Karki and Arun Khatri may reduce the high risk of cybercrime, threat, and attacks.

1. Software application and operating systems must be upgraded from time to time automatically or manually. 2. Two levels of the strong and original firewall must be joined in a network connection and used encryption-decryption technology.
3. Antivirus software should be installed during ICT automation in an organization.
4. Zero-day security technology should be connected to the computer to protect email and network.
5. Use Alin felt unified security management, comodo hacker-proof, tripwire IPE 360 software, and devices system should and scan time to time which will help to list the risk on the system.
6. Use a double certification system and do not use expired and blocked software by the software company.
7. Classify data and records properly using different methods and use file integrity monitoring (FEM) and security information and work management (SIM).
8. Apply penetration testing which will block unauthorized accessed in a system.
9. Use distributed denial of service and make aware employees about network security, database management and provide knowledge and capacity building training to personnel.
10. Use mobile device management (MDM), a virtual private network (VPN) and URL filtering in the system and use a web application firewall.

The government of Nepal should not delay to set up Cybersecurity Research and Control Academy in time.

ACKNOWLEDGMENT

This research paper is prepare with the help and support of Government of Nepal, Ministry of Federal Affairs and General Administration, Singha Durbar Kathmandu, Nepal and Rapti Engineering College, Ghorahi Dang Nepal.

REFERENCES

[1] Shailendra Giri. *Cyber Crime, Cyber threat, Cyber Security Strategies and Cyber Law in Nepal.* Pramana Research Journal. **Vol. 9**, **Issue 3**, PP. 662-67, **2019.**

[2] Shailendra Giri and Subarna Shakya. *Cybercrime, Cyber Ethics, Cyber Law and Cyber Security*. Proceeding of International Youth Conference on Science, Technology and Innovation (IYCSTI-2019). Kathmandu, Nepal, **October** 21-23, **pp-594-597**, **2019.**

[3] S. Shriram. *Cyber Security and Related Crimes in Indian Senario.* International Journal of Current Research, **Vol. 6, Issue, 03**. pp.5403-5412, **2014**

[4] Shailendra Giri and Subarna Shakya. *Cloud Computing and Data Security Challenges: A Nepal Case.* International Journal of Computer Trends and Technology. **Vol. 67, Issue 3.** PP 146-150, **2019**.

[5] P. SITBON. *A Cyber Security Approach for Smart Meters at ERDF. Modeling Cyber Security: Approaches, Methodology, Strategies U. Gori (Ed.).* (2009). IOS Press, Netherland. doi:10.3233/978-1-60750074-2-93.

[6] Maurizio Martellini. *Cyber Security.* Springer Cham Heidelberg New York Dordrecht, London, **2013.** DOI 10.1007/978-3-319-02279-6

[7] Shaheen Ayyub, and Devshree Roy. *Cloud Computing Characteristics and Security Issues.* International Journal of Computer Sciences and Engineering. **Vol. 1, Issue 4**, pp. 18-22, **December 2013**

[8] U.S. Army Training and Doctrine command. *Cyber Operations and Cyber Terrorism*, Handbook No. 1.02 P.II-1 and II-3, USA., 15 **August 2005**

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

[10] A.VIDALI. *Striking the Balance: Security vs. Utility.* IOS Press, Netherlands, **2009.**

[11] Global Cybersecurity Index-2018. *International Telecommunication Union.* ITU Publications. Published in Switzerland Geneva, **2019.**

[12] Chuda Bahadur Roka, *Cybercrime and Security in Nepal: The Need For Two-Factor Authentication In Social Media.* Crossing the Border: International Journal of Interdisciplinary Studies, **Vol. 5, Issue 2**, pp. 16-31. **15 July 2017**. DOI: https://doi.org/10.3126/ctbijis.v5i2.18436

[13] D. Kumar and N. Panchanatham. *A case study on Cyber Security in E-Governance.* International Research Journal of Engineering and Technology (IRJET). **Vol 2, Issue 8**, pp 272-275, **2015.**

[14] Elias G. Carayannis and David F.J. Campbell. *Cyber-Development, Cyber- Democracy and Cyber-Defense.* Springer Science+Business Media, New York, 2014. DOI: 10.1007/978-1-4939-1028-1

[15] Shailendra Giri. *E-government Use in Nepal: Issues of Database Management and Data Security*. Journal of Institute of Engineering, Tribhuvan University, Nepal. **Vol. 15, Issue 2**. pp. 226-232 , **2019.**

[16] Obama, B. *International stragegy for cyberspace: Prosperity, security and openness in a network world.* The White House. USA, **2011.**

[17] Keiko Hashizume, Davidd G Rosado, Eduardo Fernandez Mendina and Eduardo Fernadez. *An analysis of Security Issues for Cloud Computing.* Journal of Internet Services and Applications. A Springer Open Journal 4:5 , pp. 1-13, **2013**

[18] Aboul Ella Hassanien and Mohamed Elhoseny. *Cybersecurity and Secure Information Systems.* Advanced Sciences and Technologies for Security Applications. Springer Nature. Switzerland, **2019.** DOI:10.1007/978-3-030-16837-7

Author's Profile

Dr. Shailendra Giri. Executive Director, Government of Nepal. Now, in the Ministry of Federal Affairs and General Administration, Singhadurbar Kathmandu Nepal. Served at Personnel Training Academy-PTA, Jawalakhel Lalitpur Nepal as Executive Director since 2015-2019. Received PhD, M.Sc. IT and PGDIT degrees from Singhania University and Sikkim Manipal University 2020, 2011 and 2010 respectively. I was a lecturer at Mahendra Multiple Campus in Ghorahi Dang. I played the role of Principal at Rapti Engineering College in Ghorahi Dang. Now, Chief member of World Research Council and President of REC Development and Research Center, Nepal. Former Central Committee member of the Computer Association of Nepal. Former President of Computer Association of Dang. Former general secretary of Nepal English Language Teachers' Association. My research areas are Computer Science and Information Technology; Cybersecurity, Cloud Computing, E-Governance and Civil Service of Nepal. I have published 16 articles in international journals and attended 9 conferences in Nepal and abroad. I have received the International Peace award 2019 by RULA for the best researcher of the year 2019.

Prof. Dr. Subarna Shakya. Professor of Computer Engineering. Received MSc and PhD degrees in Computer Engineering from the Lviv Polytechnic National University, Ukraine, 1996 and 2000 respectively. Department of Electronic and Computer Engineering, Pulchowk Campus, Institute of Engineering, Pulchowk, Tribhuvan University. Coordinator (IOE), LEADER Project (Links in Europe and Asia for engineering education, Enterprise and Research exchanges), ERASMUS MUNDUS. website: http://leader.unisannio.it. Member of National Information Technology Advisory Committee, Government of Nepal. Member, Board of Studies (BOS), South Asian University, www.sau.int, New Delhi, India**.** Member, Academic Council, Purbanchel University, Nepal. Chairman, Computer Engineering Subject committee, Ministry of Education, National Curriculum Development Center, Sanothimi, Bhaktapur.

