Cybersecurity in Foreign Policy: Nepal's Outlook and Considerations on Cyber Space and Cybersecurity

A Dissertation

Submitted to

Department of International Relations and Diplomacy (DIRD)

Faculty of Humanities and Social Sciences

Tribhuvan University

In Fulfilment of the Requirement for the

Master's Degree

In

International Relations and Diplomacy

By

SANDHYA NEPAL

Roll No.: 182804027

T.U. Regd. No.: 6-2-432-53-2014

DIRD, TU

Kathmandu, Nepal

2022

Letter of Recommendation

I certify that this dissertation entitled "Cybersecurity in Foreign Policy of Developing Countries: Nepal's Outlook and Considerations on Cyberspace and Cybersecurity" was prepared by Ms Sandhya Nepal under my supervision. I hereby recommend this dissertation for final examination by the Research Committee, Department of International Relations and Diplomacy, Tribhuvan University, in fulfilment of the requirements for the Degree of MASTER'S IN INTERNATIONAL RELATIONS AND DIPLOMACY.

_____

Asst. Prof. Apekshya Shah

Letter of Approval

Declaration

I hereby declare that this dissertation is my own work and that it contains no materials previously published. I have not used its materials for the award of any kind and any other degree. Where other authors' sources of information have been used, they have been acknowledged.

Signature:

Name: Sandhya Nepal

Date:

Acknowledgement

Foremost, I would like to express my sincere gratitude to my dissertation supervisor Asst. Prof. Apekshya Shah for the continuous support of my Master's study and research, and for her patience, motivation, enthusiasm, and immense knowledge.

I would also wish to express my appreciation to Prof. Dr. Krishna Raj Acharya, Head of Department International Relations and Diplomacy, Tribhuvan University for his support and encouragement.

I also take this opportunity to thank the dissertation's external examiner, Asst. Prof. Pitambar Bhandari, and internal examiner Asst. Prof. Gaurav Bhattrai for their important comments and feedback.

I also express my sincere thankfulness to all the teachers, classmates and the administrative staff members of the Department of International Relations and Diplomacy, Tribhuvan University for their assistance in two-years of the journey in the institution. I specially thank my classmate and research scholar Manish Jung Pulami for encouraging and assisting me in my research works and helping me in finding useful research materials.

Importantly, I'd like to thank my loved ones for creating the environment conducive for me to study continuously and for the research work, and I express my thanks to the people who have contributed indirectly.

Abstract

The global digital revolution has undeniably empowered the world to seek new horizons of growth and development by fostering innovations and facilitating positive change. It has also been helpful in spreading democratic values and creating immense opportunities in multiple sectors. However, the digital revolution has also been the harbinger of newer threats to the national security of the states. In the early time of digital adoption, cybersecurity and cybercrime were mainly viewed as technical matters rather than strategic issues, due to which firm government actions and proper security measures covering the digital aspects were missing. This posture started to change when significant cyber-attacks like the 2007 Estonia cyberattack and the 2010 Stuxnet worm attack began to make headlines.

The cybersecurity has been part of foreign policy and national security of many developed countries, but many developing countries, because of structural constraints, have not been able to incorporate this into their national strategies. Realizing this research gap in the previous studies, the research explored the cybersecurity aspects of developed countries like the USA, China, Russia, and other SAARC countries. As qualitative research, the study is a systematic and holistic approach towards viewing different aspects of cybersecurity and relating to the Nepalese context. Notably, the research explained the cybersecurity concerns of Nepal, pointing out several cyberattack incidents. It also elaborated on Nepal's different attempts or initiatives on cybersecurity. The study critically analyses the essentiality and significance of cybersecurity policy for Nepal as a developing country. The research focuses outlook and considerations of Nepal towards cybersecurity and recommends some strategies for comprehensive cybersecurity policies.

Keywords: Cybersecurity, Foreign policy, Nepal and cybersecurity, Cyber strategies, Developing countries.

List if Tables and Figures

List of Tables

Table (i): Characteristics of Cyberspace

Table (ii): National Cyber Security Index, Digital Development, and Differences between SAARC Countries

Table (iii): Data of Cyber Security Cases in Kathmandu

Table (iv): General Nature of Cases in Nepal

Table (v): Nepal's Cyber Security Initiatives

Table (vi): Languages Spoken in Nepal

Table (vii): Cyber Crime Cost and Cyber Crime Loss

List of Figures

Figure (i): Conceptual Framework of the Research

Figure (ii): Total Removal Request Received by Google, 2009-2021

Figure (iii): Government Request to Remove Content under the Pretense of National Security

Figure (iv): National Cyber Security Index of SAARC Countries

Figure (v): Graphical representation of different attacks in the banking sector of Nepal

List of Abbreviations

ACA	Afghan Cyber Army
ADB	Asian Development Bank
ATM	Automated Teller Machine
BRI	Belt and Road Initiative
CBI	Central Bureau of Investigation
CERT	Computer Emergency Response Team
CGSC	Global Commission on Stability of Cyberspace
DDL	Digital Development Level
DDoS	Denial Service Attack
DOS	Denial of Service
e-GMP	e-Government Master Plan
EIR	Equipment Identity Register
ETA	Electronic Transaction Act
ETR	Electronic Transaction Regulation
EU	European Union
GDP	Gross Domestic Product
GIDC	Government Integrated Data Centre
GNM	Government Network of Maldives
IBG	Industry Botnet Group
ICT	Information and Communications Technology

IoT	Internet of Things
ISP	Internet Service Providers
IT	Information Technology
ITU	International Telecommunication Union
LTTE	Liberation Tigers of Tamil Ealam
MCIT	Ministry of Communications and Information Technology
MDMS	Mobile Device Management System
MiTM	Man in The Middle
MNOs	Mobile Network Operators
MoCIT	Ministry of Communications and Information Technology
MoU	Memorandum of Understanding
NATO	North Atlantic Treaty Organization
NCFTA	National Cyber-Forensics and Training Alliance
NCIT	National Centre for Information Technology
NCSI	National Cyber Security Index
NITC	National Information Technology Centre
NNSW	Nepal National Single Window
NPR	Nepalese Rupees
NRCCC	National Response Centre for Cyber Crimes
NTA	Nepal Telecommunication Authority
NTRO	National Technical Research Organization

OEWG	Open-Ended Working Group
OTA	Online Trust Alliance
PISA	Pakistan Information Security Association
PLA	People's Liberation Army
PPP	Public-Private-Partnership
SAARC	South Asian Association for Regional Cooperation
SDG	Sustainable Development Goals
SLCERT | CC	Sri Lanka Computer Emergency Readiness Team | Coordination Centre
SMS	Short Message Service
SSF	Strategic Support Force
UN	United Nations
UN GGE	UN Group of Government Experts
UNGA	United Nations General Assembly
US/USA	United States of America
WME	Weapons of Mass Effect

Table of Contents

Letter of Recommendation ii

Letter of Approval iii

Declaration iv

Acknowledgement v

Abstract vi

List if Tables and Figures vii

List of Abbreviations viii

Table of Contents xi

CHAPTER I 1

1.1 Introduction 1

1.2. Statement of Problem 3

1.3. Research Questions 4

1.4. Research Objectives 4

1.5. Delimitation of the Study 4

CHAPTER II 6

LITERATURE REVIEW 6

2.1 Cyberspace 6

2.2. Cyber Threat, Cyber Attack, and Cyber Security 7

2.3. Non-Traditional Security Threats and Rise of Cyber Crimes 10

2.4. Multilateral Efforts (Cyber Space and Global Governance: What are the Countries Doing to Cooperate in Cyber Space) 12

2.5. International Regime on the Issue of Cyber Security 12

2.6. Nepal and Cyber Security 14

CHAPTER III 17

CONCEPTUAL FRAMEWORK AND RESEARCH METHODOLOGY 17

3.1. Conceptual Framework 17

3.2. Research Method 18

3.3. Research Design 18

3.4. Nature/Sources of Data 18

CHAPTER IV 20

National Security and Cyber Security 20

4.1. Cyber strategies of different countries 22

4.1.1. Cyber Security Strategies of USA 23

4.1.2. Cyber Security Strategies of China 25
4.1.3. Cyber Security Strategies of Russia 27
4.2. Cyber Security Strategies of SAARC Countries 29
4.2.1. Afghanistan 32
4.2.2. Bangladesh 32
4.2.3. Bhutan 33
4.2.4. India 35
4.2.5. Pakistan 37
4.2.6. Sri Lanka 38
4.2.7. Maldives 39
CHAPTER V 41
CYBER SECURITY CONCERNS OF NEPAL 41
5.1. Cyber Attack Incidents in Nepal 42
5.2. Nepal's Initiative for Cyber Security 45
5.3. Analyzing Nepal's Cyber Security as a Developing Country 51
5.4. ICT as a Critical Infrastructure in Nepal 52
5.5. Digital Divide in Nepal 53
5.6. Digital Sovereignty 55
5.7. Capacity Building for Nepal 57
5.8. International Cooperation by Nepal for Cyber Security 57
5.9. Cyber Defense 59
CHAPTER VII 61
FINDINGS AND CONCLUSION 61
7.1. Findings 61
7.2. Conclusion 64
REFERENCES 66

CHAPTER I

1.1 Introduction

The world has evolved a great deal in the 21st century, with it the pattern of trade, politics, security, globalization and technology. Especially in terms of technology, things that were considered impossible just a few decades ago have made it into our everyday life today. The faith in technology has led humankind of this era to believe that anything is possible. The notion of security as perceived since the Westphalian international system is undergoing a visible paradigm shift. A variety of private and civil actors expand their influence and even possess the capability to shape world politics, ultimately bringing up newer challenges ranging from human security, terrorism and globalization, human rights issues, environmental issues, and the most recent cyber issues.

Today discussions about "Cyber" are conspicuously growing in the debates of international and national security agendas. Transcending from the technical realm, cyber concerns are now being viewed from geopolitical and strategic vantage points, inducing the considerations for responsible state conducts in cyberspace as cyberspace could not only spell a threat to national security but also could be a distinguishing factor in terms of military or strategic advantage, particularly to the early adopters and top-tier cyber powers. (Broeders & Van Den Berg, 2020) . We can find that countries put different emphases on recognizing the role of digitization in foreign policy. Some countries are ahead in adapting digital aspects into their foreign policies and have even developed comprehensive digital foreign policies. For example, in 2020, Switzerland launched its Digital Foreign Policy Strategy 2021-24 to follow the Swiss Foreign Policy Strategy 2020-21. Australia, Denmark and France are also a few countries that have defined digital foreign policy (Diplo, 2021). Countries such as China, Russia, the United Kingdom and the United states have invested rigorously in foreign intelligence capacity and the military to tap into the opportunities in cyberspace. Even countries like North Korea, Iran and Israel are following in their footsteps, albeit in their suitable pattern and different degrees to create a cyber-landscape in which their cyber capacities and cyber powers are unevenly divided among other nations (Broeders & Van Den Berg, 2020).

According to the International Telecommunication Union (ITU) estimation, more than half of the world's population was online by the end of 2018 (ITU 2018). If we see the records of internet users in the last 15 years, we can observe the dramatic change in demography. For example, in 2000, 17% of the world's population who belonged to developed nations represented 82% of the world's internet users, whereas, by 2017, developing countries with 84% of the world population overtook the majority and represented 73% of internet users (World Bank, 2019). Even though developing countries are still under-represented among internet users, this gap is narrowing quickly.

From the context of internet access, the remarkable rise in the subscription of mobile broadband in developing countries indicates the growth of internet usage in which regions that have the most developing countries, such as Africa, Arab States and Asia-Pacific regions, have had the most significant expansion in internet usages owing to the acceleration in broadband subscriptions (ITU, 2018). Notably, states of the Global South generally managed to bypass fixed-phone infrastructure by investing directly in wireless technology (Schia, 2017). Even though developing countries seem to be catching up with the technology, the digital infrastructure keeps evolving. Developing countries usually fall for the pattern of using older-generation technology, which renders them even more susceptible to cyber-attacks (Shaik, Seifert, Borgaonkar, & Niemi, 2016). Insufficient strategic measures, below-par legal frameworks and a lack of human resources are some of the structural factors that add to the peril of developing countries in tackling cybersecurity problems.

Today, digitalization is considered a prerequisite to economic well-being, which is also one of the fundamental factors for achieving the UN's Sustainable Development Goals (SDGs). While the whole world is already on the bandwagon of digital transformation (from the digitalization of financial services to the provisions of e-government), many developing countries have begun encountering cyber threats that jeopardize the economic environment and, equally, the national security too. The threats are bound to increase as developing countries become a large section of the global cybersecurity landscape.

In a world where various cyber-attacks have started making headlines, Nepal, even though a small country, needs to start navigating the power divide in cyberspace as

the cases of Nepal being subject to cyber-attacks have already begun emerging. Nepal, as a country that only recently graduated from the least developed nation, could be more vulnerable to cyber-attacks considering its limited resources to defend cyberspace. Cybersecurity has started becoming an underlying element of comprehensive national security for many nations. It refers to a state's "ability to protect itself and its institutions against threats, espionage, sabotage, crime and fraud, identity theft and other destructive e-interactions and e- transactions" (Choucri, 2019). Defining the scope of regulation in cyberspace will help clarify the appropriate form of activities. Individuals or groups in nations with cyber access need to have a balanced cyberspace that is not disrupted by undemocratic control or random policing.

With the hope of contributing to the awareness of national-level cybersecurity issues, this study intends to understand the complexities of cyberspace for developing nations and delve further into the policy aspect of where cybersecurity fits in the foreign policy strategies for a developing country such as Nepal.

1.2. Statement of Problem

With digitalization spreading in every country today, the ubiquity of ICT in everyday life has also magnified the impact of cyber-attacks. The time to put appropriate measures into place has come, and many countries have begun taking active steps towards it, considering the possibilities of inter-state conflict which could be triggered via cyberspace. Developing countries, too, are advancing developments incorporating ICTs owing to the relevance of ICTs in bringing new opportunities and transforming society through economic growth. However, developing countries tend to have relatively weak ICT capabilities and resources, making them even more vulnerable to cyber-attacks. If developing countries such as Nepal want to reap the full benefits of the digital age, it is important to be concerned about cybersecurity, while cyberspace for these countries is already expanding in scale and depth. This study attempts to map cyber concerns in the foreign policy of several countries with an emphasis on cybersecurity to explore how the tools for diplomacy and foreign policy are being adapted in the current digital age. Nepal is taken as the case study for developing countries; hence a thorough analysis of how Nepal recognizes the role of digitalization and its priorities to incorporate cyber strategies in its foreign policy will be studied.

1.3. Research Questions

With regard to Nepal's policy aspects, the research questions include the following:

- Why is cybersecurity a pertinent issue for governments around the world?
- Is Cyber security a matter of national interest for Nepal?
- What is Nepal's posture as a developing country in the global discourse of cyber governance?

1.4. Research Objectives

As per guided by the research gap and the research questions, the main objectives of the study are:

- To explore why cyber security is a pertinent issue in today's world
- To evaluate the cybersecurity concerns of developing countries like Nepal and how cybersecurity is a national interest for Nepal.
- To examine how up-to-date Nepal's foreign policy goals are and its participation in the global discourse of cyber governance.

1.5. Delimitation of the Study

The study's degree of boundaries and limitations are:

- There is no prominent scholarly work related to cybersecurity in Nepal
- The site of the study will be limited to the researcher's access to works of literature available and interviews of the scholars and experts, in which the variables of the study, Cybersecurity, is subject to change under the explanation by different scholars and political environment.
- The study will mostly rely on knowledge transferability and the combination of pieces of literature through the limited literary works of scholars and experts.
- The explanation and analysis of the objectives of the study will be limited to the time frame of the completion of the study, and the research will not accommodate future developments in the study.

- The study will be focused on the policy aspect of cybersecurity and hence will be limited in the ability to explain the technical aspect of its field of origin, i.e. computer science.

CHAPTER II
LITERATURE REVIEW

The topic of cybersecurity is incredibly expansive, although the applicability of international law in cyberspace is commonly accepted now (Tsagourias, 2020). The following sections in this chapter summarize some critical literature related to the study by recapping some significant developments specifying key concepts such as cyberspace and cybersecurity from political perspective.

2.1 Cyberspace

Typically, the spatial embodiment of cyberspace can be described as having at least three layers: the technical, which is concerned with the technological infrastructure of cyberspace; the geographical, thus the topology of ICT networks formed by the location of their nodes and hubs; third is the social layer, which is concerned with the spatial organization of people using the ICT networks (Fourkas, 2004). The characteristic features of cyberspace stand in sharp contrast to our traditional conceptions of social systems and the state system in particular (Choucri, 2019). Table 1.1 draws attention to seven critical features of cyberspace and defining features of the state system, at least from a user perspective.

Temporality	Introduces near instantaneity in human interaction
Virtuality	Transcends constrains of location and geography
Permeation	Penetrates boundaries and jurisdictions
Fluidity	Sustains shifts and reconfigurations
Participation	Reduces barriers to activism and political expression
Attribution	Obscures actor identity and links to action
Accountability	Bypasses established mechanisms of accountability

Source: (Choucri, 2012)

Table (i): Characteristics of cyberspace

Cyberspace is a constructed space which has, over time, evolved into a ubiquitous and pervasive space independent of any territorial boundaries and the management of this space, for the most part, is entirely managed by the private sector at the global level (Choucri, 2019). Governments worldwide have very little control over cyberspace

management, and the novelty of this space in political considerations has also caused many governments to view cyberspace as a source of instability, insecurity and even threat. When the development of cyberspace was in the early stage, states treated this development with “benign neglect” (Broeders & Van Den Berg, 2020). However, once the digital economy started reigning in the markets, governments’ interests were piqued, and cyberspace discussions eventually became a matter of high politics through security and economic dimensions (Klimburg, The darkening web: The war for cyberspace, 2018). Some states have even declared the cyber domain to be another critical domain of warfare after air, sea, land, and space. Some states' military and intelligence operations investment have increased in the pretext of being prepared for cyberwar” (Kello, 2019). The emergence of a new threat (Cyber threat) signals new vulnerabilities (cybersecurity) and the emerging policy discourses on national and international levels also indicate the growing politicization of cyberspace.

2.2. Cyber Threat, Cyber Attack, and Cyber Security

Developing countries have certain distinct factors which shape as well as affect their security landscape. Some common factors are (1) poor “digital hygiene”, that is, simple software updates and setting up essential malware protection is one of the most common reasons for facing cyber threats; (2) The leapfrogging of technology is not well understood where individuals can conduct financial transactions with smart phones even in regions which have not been penetrated by web or credit card technology; (3) Overwhelming exposure to the internet where novice users are not sufficiently aware of the social and security risks and the difficulty of governments in educating these groups and in disseminating necessary schemes; (4) The use of unverified software or pirated systems which do not have security support from the provider; (5) lack of knowledge or limited understanding of enemies of cybersecurity (Ben, et al., 2011).

Cybersecurity is generally understood as the ability to control access to networked systems and the information they contain to make cyberspace a “reliable, resilient, and trustworthy digital infrastructure” (Bayuk, et al., 2012). However, the cyber-capacity of nations varies; therefore, Nations do not share a consensus regarding the particular ways in which cybersecurity threats are defined (Romaniuk & Manjikian, 2021). As per the International Telecommunications Union, more than fifty percent of

the world's nations have not formally implemented a cybersecurity strategy. Although, this does not mean that they have not begun addressing issues related to cybersecurity, but instead that there is no one clear, coherent guiding strategy, nor is there an institutionalized set of responses to be deployed if the nations were to be the subject of cyber-attack (Rayome, 2017).

A consensus report as a result of the 2009/2010 session of the UN Group of Government Experts (UN GGE) outlined some of the main threats which are emerging from the increasing development as well as the use of ICTs to the peace and security of international harmony including "terrorist use of ICTs". According to the report, ICTs can easily be used as a medium of warfare or gathering intelligence. The threat from ICTs is further fostered by attribution issues where state or non-state actors could use ICT tools as a proxy and the growing dependence on digital technology from economies' critical infrastructures. The disparities in ICT capacity among different nations could threaten the nations with weak cyber capacity. The threat also extends to the ICT supply chain, where the lack of security could disrupt the global economy (UNGA 2010).

Any illegal or hostile activities in cyberspace can be categorized as cybercrime and labelled as a cyber-attack. A cyber- attack could cause consequential economic costs, which could not only affect society but also hamper economic growth. The effects of cyber-attacks could go beyond indirect disruption or temporary inconvenience by inflicting chaos and confusion across societies by disrupting daily life and, in extreme cases, even causing human casualties (Shackelford, 2010). Owing to the limitation of this study, the selection of cyber-attacks has been limited to the kinds of attacks that have had a major strategic and economic impact on the countries discussed. Some of the common cyber-attacks that are discussed are:

- **Malware, Ransomware and Spyware**

  Anything malicious to software is categorized as Malware. It could be anything from a Trojan, Spyware, and Virus to Ransomware which can cause damage to the computer system. Ransomware is another type of malware which covertly encrypt the data of the victim's data in order to demand some form of payment or "ransom" (usually in cryptocurrencies) for the offer to restore access by the victim (Fruhlinger, 2018). Ransomware like Wannacry

affected more than 300,000 victims (Europol, 2018), by locking their computers and encrypting their files. The attack impacted more than 150 countries, and the global economy bore a loss of around US$4 billion (Beer, 2018). Malware is also known to cripple critical infrastructures. For example, in 2019, one of the major electricity suppliers in south Africa, Johannesburg, was attacked by ransomware encrypting all of their databases and networks, which caused a blackout for the residents for many hours (BBC, 2019).

Spywares are other malware which is developed to spy on users. Pegasus is one of the spyware that can surreptitiously infect an electronic device in order to harvest information. This spyware can even covertly activate the microphone and camera without the user noticing. Edward Snowden blew the whistle regarding the secret mass surveillance operation conducted by the US National Security Agency which used Pegasus spyware developed by an Israeli company to conduct unsanctioned and unethical surveillance against its citizens and other foreign actors (Lewis, 2021).

- **Denial of Service Attack (DDoS)**

  A distributed attack where multiple computer programs simultaneously drive an authorized user of internet access, e.g., flooding a network or a server with high traffic is known as a Denial-of-Service attack (Suman, 2021). Much evidence of politically motivated DDoS attacks can be found. The 2007 DDoS attack was one of the prominent examples when the Estonian government faced a denial -of service attack in which their networks were severely compromised by foreign actors who were most likely working for the Russian government (Center for Strategic and International Studies , 2022).

- **Data Breaches**

  A data breach is stealing information by an unauthorized party with objectives such as identity theft, whistleblowing or espionage. Information in itself can be a great asset- for example, for certain valuable information, instigators can exploit cyberspace to their advantage to run various cyber espionage campaigns to attain strategic knowledge (Świątkowska, 2020). While most data breaches are financially motivated to steal financial resources (Verizon, 2018), the case of whistle-blower Julian Assange is also one of the examples

relevant from a political context. Assange published confidential US military logs from Afghanistan and Iraq and US diplomatic cable leaks from his media company called “WikiLeaks” and is facing charges from the US government under the US Espionage Act (Aljazeera, 2020).

There are also several other security threats, such as Phishing, Man in Middle Attacks (MiTM), Attacks on IoT Devices, Credit Card fraud etc. which can cause damaging consequences in the cyber environment of a country.

2.3. Non-Traditional Security Threats and Rise of Cyber Crimes

The technological developments of the twenty-first century have made it necessary to reconsider traditional notions of security (Choucri, 2012). Despite being a new and constructed domain, cyberspace has concisely managed to embed the social, economic and political environment. There are visible instances of using cyberspace as a “conduit of power” and even as a “conduit of intervention” by employing new coercive tools that are suitable to cyberspace apart from the traditional tools of diplomacy and politics (Johnson & Post, 1996). Cyberspace exceeds physical space rendering it territorial, given the phenomenon of data mobility and interconnectedness. Such a phenomenon indeed constitutes a challenge to typical notions of jurisdictions necessitating a new approach or a reconceptualization of the concepts of sovereignty (Daskal, 2015).

It has only been over a decade since the severe discussions about cyberspace regulations started. The incident of the distributed-denial-of-service (DDoS) attack against the Estonian government in 2007 was the trigger point for the discussion (Tikk, Kardi Kaska, & Liss Vihul, 2010, pp. 14-35) as this incident demonstrated the vulnerability of the ICT -reliant state to the international community (Aaviksoo, 2010). Calls for cyber governance to maintain the security and stability of cyberspace also gained momentum in several international avenues after the Stuxnet incident in Iran in 2010, in which a state-sponsored politically motivated cyber operation neutralized the nuclear facilities of Iran.

The reach, effects and scalability in cyberspace certainly pose a threat to the sovereign authority of a nation (Tsagourias, 2020). There remains confusion in the territorial sovereignty in cyberspace as cyberspace is not limited to physical space and or a

certain territory. The traditional notion of sovereignty is limited in addressing the challenges of sovereign intrusions facilitated via cyberspace (Corn & Taylor, 2017). The evidence of such intrusions can be found in the cases of cyber espionage and cyber tension between US and China. In 2013, from news related to Chinese hacking major American media to evidences of Chinese economic espionage using unauthorized computer access came forth. The involvement of Chinese Military hackers in hacking key industrial entities led US to release executive order against the China representing "one of the first ever charges against a state actor for hacking" (Rollins, 2015). This incident also resulted in the first bilateral Cyber Agreement between U.S and China.

There are even several prominent incidents of electoral interference that have highlighted the challenges in sovereignty in state of affairs, such as The Russian cyber interference in the 2016 US presidential election. For example, it invoked the principles of non-intervention in the cyber domain critically because it demonstrated how cyberspace could be a domain where states cannot only compete but can also exert power by leveraging the scalability, reach and effect of intervention via a cyber environment. For instance, the cases of deep fakes and manipulations of videos, voices and images of politicians during an electoral campaign to distort the will of the voters pose a novel yet severe threat from external interference. Such external interference through disinformation can potentially undermine or even inverse the expression of authority (Ohlin, 2018).

The sovereignty of a state can also be challenged by Surveillance activities in cyberspace. The Snowden revelations of US NSA's clandestine surveillance gave us the glimpse of threat to the privacy of a state as a whole with enormous scale and scope (Obar, 2015). Similarly, the 'backdoor' surveillance through 5G network equipment supply by Chinese actors has also raised concerns regarding human rights and sovereignty (Becker & Nanni, 2022).

The novelty of considering cyberspace sovereignty has certainly brought out non-uniform state practice. These prominent cases have made the state actors in some developing parts of the world more paranoid to the pervasion of cyber space but at the same time the multilateral efforts towards formulating global cyber strategies helps provide a positive outlook.

2.4. Multilateral Efforts (Cyber Space and Global Governance: What are the Countries Doing to Cooperate in Cyber Space)

The concerns concerning the potential negative impact of the use of ICT on global peace and security were initially flagged by Russia in 1998 with the submission of a resolution on "Developments in the field of Information and Telecommunications in the context of International Security" to the UN's First Committee, which is responsible for dealing with matters of disarmament and international security (UNGA, 1999). Later in 2004, the considerations materialized in establishing the UN Group of Governmental Experts (UNGGE) process, which was created to debate cyber issues at the UN level (UN GGE, 2021). So far, there have been five iterations of the UNGGE process, out of which a consensus report has been produced three times, and these reports predominantly yield to the principle that international law is applicable in cyberspace. The 2015 consensus report also yields the formulation of several nonbinding norms in order to assure responsible state behaviour (UN General Assembly 2010, 2013, 2015). Shortly after 2017, reports of the "death of the norms process" started appearing when the UN GGE 2017 round failed to achieve consensus (Grigsby, 2017). The disagreement among the parties of UN GGE resulted from another new competing and parallel resolution in 2018, in which the first one was proposed by the United States and voted by the "like-minded" states calling for the continuation of the GGE meetings. In contrast, the second was proposed by Russia, calling for an altogether new Open–Ended Working Group (OEWG) for the discussions of the same issue (Broeders & Van Den Berg, 2020). Both resolutions were presented at the General Assembly, and since both resolutions received significantly overlapping votes, the UN-sanctioned this twin process in 2019.

2.5. International Regime on the Issue of Cyber Security

International organizations and Governments are beginning to acknowledge the importance of civil society and industry involvement in matters of cyberspace at the multilateral level, traditionally led by the state. Such development is validated by the initiatives such as the "UN Secretary General's High-level Panel on Digital Cooperation" and "Paris Call for Trust and Security in Cyberspace," which calls for consultations from the representatives of relevant industries and civil societies. (Klimburg & Faesen, A Balance of Power in Cyberspace, 2020).

According to Joseph S. Nye, when it comes to cyberspace, the intertwined but diverse cyber activities that are conducted within the constructed technical reality naturally form a mixed approach to the governance process, which as Nye describes as a "regime complex":

> "This regime complex is only partially influenced by state actors and by the bilateral, regional, or multilateral process. The private sector and civil society both generate products, common practices, and norms of behaviour largely separate from government involvement, although these developments can have significant impacts on state-led processes and discussions on international peace and security. Despite the state's traditional dominance over all questions related to international peace and security, governments make up only one out of three actor groups in the overall cyber regime complex, and its role within it is no greater than that of the private sector or civil society. The state-oriented regimes do not necessarily have the ability to speak on behalf of other equally crucial regimes. This creates a situation unique in international peace and security, where governments cannot decide on all aspects of the international cybersecurity domain itself, as responsibility and ownership for this domain are shared with non-stated with non- state actors." Given the complexity of cyberspace where too many independent operational stakeholders requiring the participation of diverse interest groups implicitly demonstrates that cyberspace is a multistakeholder domain". (Nye, 2014)

Several cyber-norms have emerged in recent times owing to the consistent diplomatic process on a multilateral level among countries under the sponsorship of the UN. There has also been serious academic initiation for the discussion of cyber governance. The Tallian Manual process is a good example of such academic efforts, which was initiated by the then newly formed 'NATO Cooperative Cyber Defence Center of Excellence', in 2008 in Tallinn, Estonia. The Tallinn Manual process was catalyzed after the Stuxnet incident in Iran in 2010, which provides "one of the strongest academic voices in the discussion revolving around the application of international law to cyberspace and operations" (Adamson, 2020).

The role and contributions of non-state actors who provides technological service, including the production of software and hardware, cannot be ignored when observing

the development and expansion of cyberspace. It is a known fact that the private sectors are the most responsible for steering the global cybersecurity norms; however, their prominence hasn't been sufficiently highlighted in academic endeavors (Hall & Biersteker, 2002). The magnitude of cybersecurity incidents can easily extend to the transnational level. After the failure of UN GGE 2016-17 to agree on a consensus report, many non-state actors have noticeably initiated programs or campaigns in order to foster responsible behaviour in the cyber domain, particularly after major cybersecurity incidents such as Wanna cry and Petya/Not Petya (Hern, 2017). Among many examples, some of them are: "Global Commentary on voluntary, Non- Binding Norms for Responsible state Behavior in the use of Information and Communication Technology" initiated by the University of Leiden and ICT4Peace Foundation (ICT4Peace Foundation, 2018), "Digital Geneva Convention" proposed by Microsoft including its adoption of "Cybersecurity Tech Accord", the support provided for the "Paris Call for Trust and Security in Cyberspace" and its campaign initiation for "Digital Peace Now" (Smith, The need for a Digital Geneva Convention, 2017), and Global Commission on Stability of Cyberspace's (CGSC) calls for "Protection of the Public Core of the Internet, the Safeguarding of Electoral infrastructures and the release of Singapore Norms Package" (Global Commission on the Stability of Cyberspace, 2018), (Smith , 2018).

2.6. Nepal and Cyber Security

In Nepal, cyberspace management and regulation can be a matter of unexpected complexities and a "strategic challenge that requires cooperation between the public and private sectors, military and civilians of our societies" (Giri, 2019). Nepal's contemporary view of National Security can be obtained primarily from the national document called National Security Policy issued by the Ministry of Defense (Ministry of Defense, 2016), which has not yet acknowledged the cybersecurity aspect. So far, there has been several policies/laws that acknowledge cybercrime indirectly addressing cyber issues, including the Electronic Transaction Act (ETA 2008); Banking Offence and Punishment Act 2008; Children's Act 1992; The Patent, Design and Trademark Act 1965; Copyright Act 2002 and Consumer Protection Act 1998.

However, the government has started developing cyber-specific policies. In 2019 the government proposed a Digital Nepal Framework initiative which outlines "one

nation, eight sectors and 80 digital initiatives" (cite Digital Nepal Framework), which means Nepal is already on the path to laying down the digital foundations. One of the initiatives relating to the cyber security proposed by this framework is the formation of an independent Computer Emergency Response Team (CERT) to deal with cybersecurity threats, identify and respond to cyber risks and collaborate with security operations center teams to establish detection rules and coordinate responses. The aim of the CERT would be to publish security alerts, conduct cybersecurity awareness and training, perform analysis and forensic investigations of cyber incidents, perform security audits and assurances, response to cyber security incidents and coordinate with local and global agencies towards cybercrime (MOCIT, 2019). Another major stride towards acknowledging cybersecurity concerns by Nepal is demonstrated by the recent introduction to Cyber Security Byelaw 2020 framed by Nepal Telecommunication Authority (NTA, 2020).

With regard to international cooperation, Nepal is a member of a multilateral alliance against cyber – threats called ITU- IMPACT initiative and has access to relevant cybersecurity support in resources or expertise (ITU, 2009). Nepal ranks 128th in ITU Global Cybersecurity Index that "measures the commitment of countries to cybersecurity in order to raise cybersecurity awareness", 98th in the National Cyber Security Index, 140th in the ICT Development Index and 118th in Networked Readiness Index as per the latest data maintained by e-governance academy.

Cyberspace has started becoming a political avenue for propaganda, political promotion, activism and voicing protests. Tons of personal information, intellectual property, and confidential or top-secret information is uploaded online. "Internet and the hundreds of millions of computers the Internet connects, the institutions that enable it, and the experiences it enables — has become a fundamental feature of the world we live in and has created a new reality for almost everyone in the developed world and for rapidly growing numbers of people in the developing world" (Choucri, 2012, pp. 4-5). Since the internet is just a network of computers, this information could get into the hand of unintended users without permission via hacking or other forms of cybercrimes. The growing importance of cyber security concerns in the global agenda shows us the relation between cybersecurity and politics. This inevitable connection between cyber security and politics in cyber space clearly has

great importance and implications for the politics of the ‘offline’ world, opening the window for updates in security policies (Fontana, 2017).

The scope of cybersecurity is still appearing to be in the nascent stage for Nepal, and the lack of sufficient literature based on the perspective of Nepal in this emerging topic of cybersecurity adds to one of the biggest justifications for this study with the hope that an academic effort the insights generated through this study could perhaps be adapted further to consider agenda setting for cybersecurity policymaking.

CHAPTER III
CONCEPTUAL FRAMEWORK AND RESEARCH METHODOLOGY

3.1. Conceptual Framework

Making foreign policy involves the majority of considerations of domestic interests allowing countries to have a clear stance while representing in international relations either in diplomacy or war. National interest can be subject to change as the priorities of a country change. Cybersecurity has been prominent in recent times to be seen as a sphere to protect the national interest. There is also a great deal of interest in cybersecurity internationally. Hence, it should be a natural phenomenon for countries to elaborate and improve their foreign policy extending to contemporary issues like cybersecurity. Therefore, this research is based on the conceptual framework of analyzing, evaluating and establishing complementarity between the aspects of national interest and foreign policy. To do so, this study analyzes the cybersecurity of Nepal from the National Security lens in which components like critical infrastructures, policy and legal measures, the concept of digital sovereignty for Nepal, international co-operation, level of cyber defence and capacity development are studied.

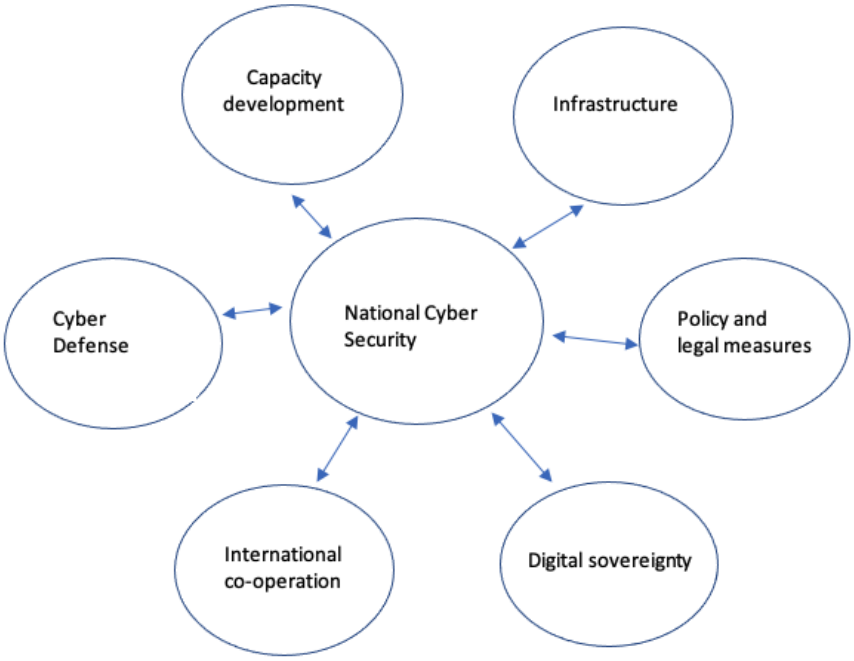


Figure (i): Conceptual Framework of the Research

Based on: A conceptual Model for the Development of a National Cybersecurity Index: An integrated Framework (Koong & Yunis, 2015)

3.2. Research Method

In the research, descriptive, methods were employed. The methods included the process of tracing, congruence testing and counterfactual to create an empirical and interpretive study of Cybersecurity as a Foreign Policy Agenda for Developing Countries. The aspects of the Case Study Research Methodology have been used in the research where Nepal is a case to interpret the adaptation process of policies in contemporary issues such as Cybersecurity. As a historical analysis, the global level developments in addressing cybersecurity challenges were done, a retrospective and diachronic case study methods were applied to the research and linked to the theoretical perspective of Agenda-Setting in Policy Making for a detailed qualitative account. This study's evaluative, comparative and analytical methods involve ideas, assumptions and analysis from different International Relations theories. The theoretical pillars of the methods in the study have included constructivist ideas, a realist approach and cultural theory claims.

The facts and relationship have been rigorously examined and explained using an explanatory methodology. Qualitative information was acquired and utilized to arrive at a fair conclusion. Direct methods, such as scientific observation and expert interviewing, have also been utilized for this research project. Empiricism, observation, critical analysis, and exploratory approaches have been highlighted in order to contextualize the study's topic.

3.3. Research Design

The research design of this study is qualitative. A systematic, subjective and holistic approach was taken into consideration, primarily by an inductive process of organizing data into categories and identifying the pattern among the categories to complete the research objectives.

3.4. Nature/Sources of Data

The study has mainly taken secondary into consideration. Data, such as government and semi-government publications from online official online portals, the Ministry of Information Technology, the UN and other authorized agencies, were employed during the research. Similarly, the media interview of experts in international

relations, diplomacy, culture, political science, and military (strategic studies) were also considered to conduct the research. Along with the primary sources of data, secondary sources such as books, academic journals, magazines, theses, reports on analysis and evaluation of military strategy documents, and books have been mainly used to navigate the holistic presence of cyber issues in the international domain.

CHAPTER IV

National Security and Cyber Security

The traditional focus of national security has always been the protection of state borders against any military or other offensive intrusions, and with the changing time, this basic principle was also refined to form a more holistic view of security. Furthermore, the responsibility of governments has also expanded their security agenda with the emergence of new threats owing to the link associated with developing policies for evolving agenda is also tied to the stability or failure of the state. To simplify, to secure the stability or even survival of any state, the state must build a vision which not only essentially seeks border protection but also views security and sustainability by converging the elements of government capacities with social viability.

Over time the world economy has increasingly transferred from physical, electronic infrastructures like telegraphs and telephones to more virtual infrastructures such as public or private internet. Many infrastructures which were not possible to access without physical presence, such as power plants and pipeline control systems, have now theoretically become accessible from any part of the world. The virtual networks, which have merged with other electronic networks, such as electronic financial transactions via the internet, have made cybersecurity a political concern for today's governments (Libicki M. C., 2007). State systems and non-state entities, for profit or not, face new imperatives and a new set of security threats while constructing cyberspace. The extent of potential damage, considering the scale and scope of cyberspace, was beyond anyone's predictions.

Additionally, the perpetrator's anonymity could threaten both the traditional notion of security, such as borders and defence, as well as the revised notion of security, including the security of society and the environment. Thus, industrial and developing states have become focused on cyber security as part of their overarching security, and effective management of the issue would require a multilevel approach to international relations to effectively handle this issue at global, transnational and international levels (Chouchri, Madnick, & Ferwada, 96-121). Cyberspace has become a powerful tool for governments to extend their reach and exert their power

and influence while pursuing the security of their own countries. An illustration of this emerging dynamic is shown in the figure (ii) and (iii) below, which shows the number of individual data removal requests Google has received from states.

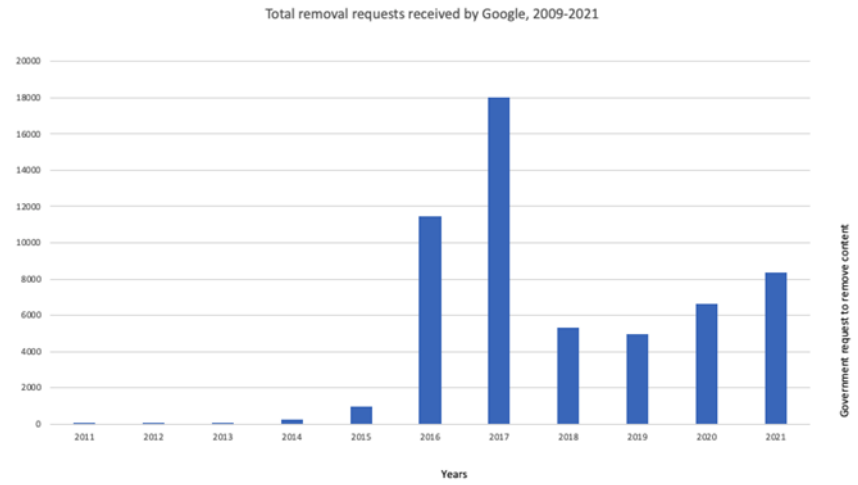
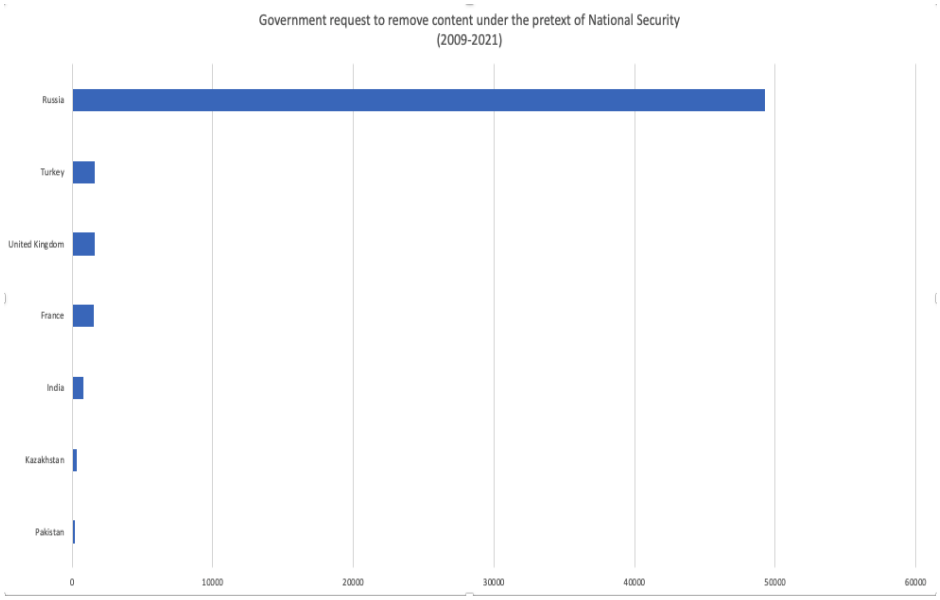


Figure (ii): Total Removal Request Received by Google, 2009-2021



Source: Google's Transparency Report (Google Inc, 2021)

Figure (iii): Government Request to Remove Content under the Pretense of National Security

Cyberspace today is under threat from the designing, developing and standardizing of infrastructure and protocols by corporations of nondemocratic states

(Yannakogeorgos, 2012). Typically, the discussion of cyber security largely centres around headline-grabbing exploits caused by ad hoc networks and nation-state-sponsored corporate espionage. However, the cyber conflict has another aspect that could pose a much graver threat to national security: the "friendly" side of cyber conquest as described by Martin Libicki where he points out that in order to conquer the internet in a friendly manner, one must be able to dominate both the technical and public policy issues related to it.

As a result, it is essential to have an in-depth grasp of the aspects of strategic-level internet governance, which are equally vital as an understanding of how may be exploited by attackers to cause national security incidents (Yannakogeorgos, 2012). Not all nations have sufficient capabilities when it comes to combatting and pre-empting cyber events, either domestically or internationally. Even though nations today are divided regarding whether the provision of a nation's cybersecurity is best approached as a national or international project, by viewing the emerging cybersecurity strategies of different states and regional organizations, we can explore how cybersecurity issues related to their national security concerns and accordingly how it affects international relations.

4.1. Cyber strategies of different countries

National vulnerabilities vary depending on the political history and culture of a nation. However, the truth of the time is that no nation is immune from cyber-attacks, irrespective of the significance of their impact. Some states are already in the stage of having a unified program in order to implement cybersecurity policies, while others still don't have clarity regarding their vulnerabilities or sufficient resource to devise a comprehensive strategy. Today nations are rapidly onboarding in an online environment exposing them to new kinds of vulnerabilities to the extent which could compromise their national security. Cyber threats are not stand-alone threats; thus, cybersecurity is increasingly entangled with all the aspects of national security, be it political, economic or defence. Understanding how different nations have attempted to integrate cybersecurity into the aspects of their national planning shows us examples and prospects for how cyber conflicts can be managed. At the same time, observing how some of these nations, individually or collectively, make international

efforts will also give us a glimpse into how a safer world could be created through regulated cyberspace.

4.1.1. Cyber Security Strategies of USA

The creation of the internet itself is accepted to be US-led due to its massive funding and research in an effort to create an interconnected system for carrying data which began in 1966. The ARPA net project under the US Defense Department's Ballistic Missile Program connected various research facilities (civilian, non-civilian, academic). When the technology gradually spread to include overseas nodes, in 1990, the US military withdrew from its controlling position within the internet. However, the US government continued to offer financial support to international groups like the Internet Society and the International Commission for the Assignment of Network Names (ICANN) through funds administered by the United States' National Science Foundation (Manjikian M. , 2021).

The US first drew up its National Strategy to Secure Cyberspace in 2003 and established a first national military Cyber Command in 2009, asserting the online domain as one of its strategic domains. The concept of utilizing technology for offensive purposes (WME or Weapon of Mass effect) also has its roots in the US as a result of the US strategic Deterrence Joint Operating Concept of 2004. The Unites states are also credited for developing one of the first cyber weapons in 2005 when it jointly created the Stuxnet Worm to target and damage Iran's nuclear program.

With regard to cybersecurity posture, the US has enjoyed certain built-in advantages. For example, by setting standards for issues like data storage and data transmission protocols, the US has historically acted as a norm giver in setting behavioural expectations in the online domain. The "American Flavor", which promotes principles such as minimal state interference and minimal regulation, can similarly be found in US foreign policy initiatives aimed at extending the internet's reach globally that are also often intertwined or linked with foreign policy goals such as overcoming global poverty, including information poverty as well as causes such as press freedom and freedom of information (Manjikian M. , 2020).

Despite the leading position as a developer of cyberspace and doctrines, the United States is not immune to cyber-attacks and has confirmed in several US National

Cyber Strategy notes that Russia, North Korea and Iran have all launched cyberattacks against the US, as well as a large- scale industrial espionage from China (DeVore & Lee). The seeming inability of the United States to defend against Russian attacks on its electoral system in 2016 shows that even big power like the US could be poorly equipped when it comes to defending in cyberspace (Dévai, 2019). Believing that the United States enjoyed a commanding lead in both cyberspace defensive and offensive capabilities, America's defence community failed to recognize the fact that social media represented an undefended flank which was ripe for attack by America's adversaries (Riotta, 2019). The 2018 United States Department of Defense Cyber Strategy notes that the US is engaged in "long-term strategic competition with China and Russia" (United States Department of Defense, 2018).

Key non-state actors (such as Google, Facebook, Twitter and Microsoft) who are able to shape the online environment are housed in the US, although their stance and individual policies are not always in alignment with the rules and procedures of their territorial host. However, to manage the cooperation with these actors, the US, through the creation of public-private partnerships (PPP), have devised several programs to combat digital crime. Such public-private partnerships include the Online Trust Alliance (OTA) and the Industry Botnet Group (IBG). In addition, groups like the National Cyber-Forensics and Training Alliance (NCFTA) – with more than 80 businesses – provide cyber threat intelligence to national and international CERTS (U.S senate, 2014).

There is growing evidence that the United States is losing any unique advantages in cyberspace that it may have enjoyed during its initial leadership position in this field as new competitors in cyberspace increase in power and numbers (Gilli, 2018). The 2013 revelations by Edward Snowden regarding the extent of internet surveillance had a significant impact on US "soft power" both within and outside of cyberspace. Even though the US fully disinvested itself from direct control over the Internet, the American effort to guide or steer cyberspace politically, culturally and economically has been viewed with suspicion.

4.1.2. Cyber Security Strategies of China

China boasts the most significant number of internet users in the world, and accordingly, it also faces an increasing number of cyber-attacks (Chen & Romanuik, 2021). Trojan horses, botnets, mobile networks, distributed denial of service (DDOS), software and hardware bugs, and security loopholes in websites are identified as the most common security issues (Chen & Romanuik, 2021). China deems cybersecurity as a global issue that challenges national security, economic development, domestic politics, and society and places emphasis on the defence of sovereignty, political order, and social stability (Raud, 2016). For China, political stability remains the dominant priority for the establishment of policies and measures related to cybersecurity (Chang, 2014).

In contrast to the United States, China's government is able to filter and control internet content going into and out of China, as well as seeking to roll-back the anonymous nature of the internet (as traditionally understood) in favour of building a more restrictive domestic internet in which citizens are not anonymous but rather registered, with their digital and real identities closely linked (Segal, 2018). In spite of the efforts of the United States and other democracies, China continues to tighten its Internet controls each year through the Great Firewall, thus making it the largest and least accessible entity on the Internet (Freedom House, 2017). China has managed to transform its domestic Internet into the world's largest censorship apparatus through the Great Firewall (Bloomberg, 2016).

For China today, the development of cutting-edge technology is at the heart of economic development and national security (Chen & Romanuik, 2021). Informatization is currently at the core of China's 13th Five-Year Plan (2016–2020), which entails the application of advanced ICT in the political, economic, military, health, agriculture, and environmental sectors (Austin, 2016). Chinese President Xi Jinping noted cybersecurity and informatization are closely linked and related to national development, "there is no national security without cybersecurity, and no modernization without informatization" (Cyberspace Administration of China, 2016).

Over the years, China has developed cybersecurity laws and policies compatible with its national interest. Highlighting some of the main ones; In 2015, China's State

Council released China's Military Strategy and emphasized the potential threat of penetration, subversion, and cultural erosion by Western countries through the exploitation of the internet (Kowalewski, 2017). Noting the strong impact such attacks may have on national security, the cyber division of the PLA is tasked with monitoring open information networks and preventing cyber espionage and attacks (The State Council of the People's Republic of China, 2014). As part of a military reform In December 2015, Xi Jinping established the Strategic Support Force (SSF) - a new operational force that will provide strategic support for the PLA on issues concerning outer space, cyber space, and electromagnetics, and plays a critical role in realizing integrated joint combat with other traditional forces (Costello, 2016). In the National Law adopted in 2015, Clause 59 proposes that China should establish surveillance institutions and mechanisms for national security and carryout security reviews for foreign investment, specific resources, key technologies, and ICT products (National People's Congress, 2015). Through the National Security Law, for the first time, China clearly introduced the concept of "cyber sovereignty", or the extension of state sovereignty to the internet. Yet the question of how the state can execute jurisdiction in cyberspace remains unclear (Bennett, 2015). In 2016, Beijing released its Cybersecurity Strategy, which elaborates on China's determination to realize related laws and norms concerning cyber space and achieve effective governance. After the adoption of the Cybersecurity law in 2017 in full force, China strives to make the distinction between domestic and foreign space. This law also demands foreign businesses store all personal information and data produced in China within the country and that they cooperate and provide information to the government in the circumstance of investigations. In other words, in the eyes of Beijing, even though the internet may be global, when it comes to the issue of jurisdiction, state governments should still take the lead (Zhou, 2015).

In terms of the international aspect, cyber sovereignty has become China's leading position on Internet (SCIO, 2010). At the Budapest Conference on Cyberspace in 2012, the Chinese delegation proposed sovereignty as the first of five principles for international cyber cooperation, and at the first World Internet Conference in 2014, China proposed sovereignty as the second item in the Wuzhen Declaration (Creemers, 2020). China, in particular, has also articulated its desire to "catch up and overtake" the United States in cyber power rankings, describing its wish to "leapfrog" over

existing powers to take the lead (Brenner & Lindsay).In response to China's slowing economy in recent years, Chinese President Xi Jinping proposed the Belt and Road Initiative (BRI), an initiative aimed at integrating the Eurasian continent and expanding the outlets and opportunities for China's excess production. Through this initiative, China has engaged in a long-term, coordinated effort to build influence within the region of Asia through investment, including the creation of a so-called Digital Silk Road, which would stretch throughout Southeast Asia to Pakistan, aiming to improve the internet infrastructure of the stakeholders and beneficiaries (Manjikian M. , The United States : A declining hegemon in Cyberspace?, 2021). Such kinds of initiatives can also be instrumental in supporting Chinese technology businesses, further consolidating China's position from "norm takers" to instead being "norm setters" in the international environment (Zeng, 2017).

4.1.3. Cyber Security Strategies of Russia

As compared to western approaches, the Russian approach places a greater emphasis on information security. Russian doctrine of information security emphasizes the importance of technology, protection of communication infrastructure, and free access to information. It demonstrates how the government is responsible for securing the information itself and, ultimately, national sovereignty (Sharikov, Alternative Approaches to Information- Age Dilemmas Drive US and Russian Arguments about Interference in Domestic Political Affairs., 2020). The first Doctrine on Information Security was established in Russia in 2000, which is a strategic document that formulates the notion of info-security from the national security angle, where the national interest plays the critical role (Stadnik, 2021). The first area of this document highlights the concept of "information Weapons" and elaborates on the provisions relating to the prohibition of the development and its proliferation. Russia has evolved a great deal in the last ten years in the state policy towards the Internet and information and has come up with specific laws to legislate activities in cyberspace on the federal level.

By the end of 2016, the Russian president had signed the new "Doctrine on Information Security." A disclaimer in the introductory part of the document states that the Doctrine is a document that builds upon the provisions of Russia's national security strategy published in 2015. (Stadnik, 2021). On May 2019, Russia adopted a

law aiming to control the Ru-net infrastructure, “the law on Sovereign Ru-net”, as named by the public. This law aims to regulate the national segment of the Internet using fragmenting and restrictive tools, particularly in the telecom sector. The essence of “Ru-net” champions data localization by storing data within the country border to resist the data concentration in transnational data storage facilities, particularly in the United States. When it comes to information regimes, in the United States, companies own data, while in the EU General Data Protection Regulation framework, ownership belongs to the individual; in Russia, it belongs to the state and must be strictly controlled by it (Sharikov & Stepanova, 2019). However, the law is yet to come into force. On the domestic front, the Russian cyber narrative represents a disruptive tool for regime stability, a view that was strengthened by the Arab Spring's realization of the power of social media, as evidenced by the magnitude of anti-regime protests in Russia in 2012 (Pingman, 2019). It can be noted that while western countries are concerned with communication security, the Russian government is concerned with the control of information content, as information may be used to influence social and humanitarian decisions (Nocetti, 2015).

- **Russia-Ukraine Cyber Security Aggression**

Russia has been justifying its invasion of Ukraine, claiming its purpose to protect the Russian-speaking population despite the referendum of 1991, where Ukrainian citizens in Crimea and eastern Ukrainian territories voted to be a part of independent Ukraine (Zapoeozhets & Syvak, 2020). Due to its strategic location in the midst of Russia and NATO member former soviet nations Hungary, Poland, Slovakia and Romania, Ukraine has been at the edge of diplomatic discomfort, ultimately triggering aggression with Russia. Russia now occupies about 8% of Ukrainian territory, which has now come to become a field of new hybrid war and a lab for Russian cyberattack training, which presented Ukrainians with unlimited opportunities to develop, update, and perfect informational defence and cybersecurity systems (Zapoeozhets & Syvak, 2020). From informational attacks to infrastructure attacks via cyberspace, the Ukrainian government adopted and implemented several cyber defence laws so as to adequately meet its cybersecurity challenges.

In the international sphere, Russian behaviour in global diplomacy is characterized by aspirations to become a great power, revisionist power games, and threats to liberal

democracy (Kurowska, 2020). Russia's international conduct is primarily determined by its demand for status recognition (Weber, 2018) .In shaping the global cyber governance debate, Russia 2018 adopted a competitive resolution to the US-sponsored UN Group of Government Experts (UN GGE) by sponsoring the Open-Ended Working Group (OEWG), which marks the breakdown of consensus on the issue (General Assembly, UN, 2018a). As an alternative to the Budapest Convention on Cybercrime, Russia also sponsored a resolution on Cybercrime in the Third Committee of the General Assembly (General Assembly, UN, 2018b), since it allows intelligent services to access data transnationally during cybercrime investigations. Recently, a new resolution in the UN's Third Committee supported Russian advocacy for a cybercrime treaty, which is seen as a tool for Russia to extend state control over the internet and curtail individual political rights (Nakashima, 2019).

Russia has been promoting dedicated and legally binding instruments in cyberspace, which can be seen as a twofold strategy: On one hand, Russia pursues strong "securitization" of cyberspace, while on the other, it assumes the role of a responsible great power which can be consulted upon, thus acting simultaneously as spoiler and saviour (Kurowska, 2020). From a broad point of view, Russia promoting and defending international law in issues of cyberspace expresses the aspirations of containing liberal hegemony.

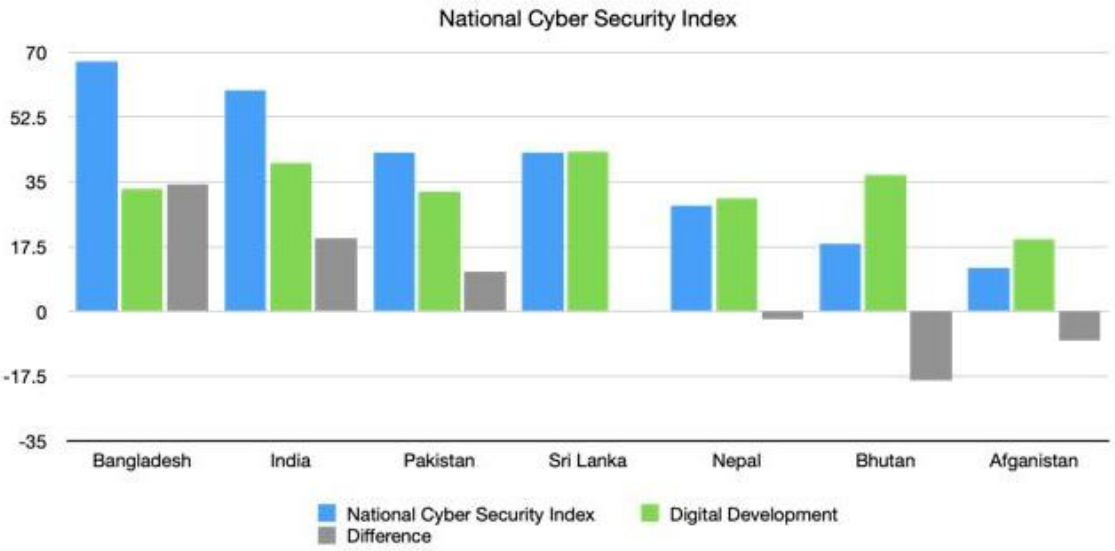
4.2. Cyber Security Strategies of SAARC Countries

SAARC nations focus their activities mainly towards fostering the economic relationship among the eight member states. The prevalent internet connectivity is acknowledged and utilized to boost economic development. However, the existence or non-existence of cyber laws of SAARC or the member states individually could affect trade relations. Cyber laws across different nations stifle barrier-free communications, resulting in a relatively underused Internet-based communication channel. As social media popularity has continued to grow and the cyber demography has grown, so has the easy access to Internet services, particularly mobile internet through smart phones, which has led to a strong effort by South Asian governments to monitor and control Internet usage aiming to gain political power (Begum, 2018).

SAARC, as a regional organization in South Asia, has an enormous trade potential, but limited regional cooperation has resulted in insignificant intra-regional economic integration. (Kumar, 2018). The countries of the South Asian region -Afghanistan, Bangladesh, Bhutan, India, Maldives, Nepal, Pakistan, and Sri Lanka are among the nations that are significantly underrepresented in the use of the Internet (Kumar, 2018). Despite being one of the most populous regions, representing about 22.4% of the world population, SAARC lags backwards with regard to cyber technology penetration. Nevertheless, cyber wars have been detected in India, Pakistan, Afghanistan, and Bangladesh. For example, an Indian police investigation agency, the Central Bureau of Investigation (CBI), was hacked by a group called Pakistan Cyber Army on 4 December 2010. Likewise, several websites belonging to the Pakistan Army and other ministries were hacked by an organization called the Indian Cyber Army, which operates independently of a nation-state and conducts terrorist activities through cyberspace. In addition to the Ministry of Foreign Affairs, the Ministry of Finance, the Pakistan Computer Bureau, the Ministry of Education, the Council of Islamic Ideology, etc., other websites were hacked by the Indian Cyber Army. As an act of vengeance for Mumbai's terrorist attacks (Etribune, 2011).

In the recent past, SAARC nations have held several cyber security dialogues, although SAARC has not officially devoted any resources to the development of a cybersecurity framework to support member states in managing their cyber risks or any collaborative tools to defend against cyber-attacks. However, some of the member states have begun creating policies in sectors such as military cybersecurity and combatting online crime, even though they are not yet in alignment with broader regional goals or requirements. The data available on National Cyber Security Index (NCSI) can help us compare the preparedness of SAARC countries to prevent cyber threats and observe how they manage cyber incidents. The table and the chart below show us NCSI scores for the SAARC countries in 2022. The data also provide Digital Development Level, and the difference between NCSI and DDL illustrates their relationship. A positive result indicates that the country is ahead of or in line with its digital development, while a negative result indicates that the country’s digital society is ahead of its cyber security development on a national level. Cyber security development is in accordance with, or ahead of. Its digital development and negative

result show that the country's digital society is more advanced than the national cyber security area.



Source: National Cyber Security Index 2022

Figure (iv): National Cyber Security Index of SAARC Countries

	National Cyber Security Index	Digital Development	Difference
Bangladesh	67.53	33.11	34.42
India	59.74	40.02	19.72
Pakistan	42.86	32.23	10.63
Sri Lanka	42.86	43.02	-0.16
Nepal	28.57	30.58	-2.01
Bhutan	18.18	36.9	-18.72
Afganistan	11.69	19.5	-7.81

Source: National Cyber Security Index 2022

Table (ii): National Cyber Security Index, Digital Development, and Differences between SAARC Countries

Table (ii) above gives us a picture of the digital capabilities of SAARC countries in managing their digital society. The difference provided in the table indicates that SAARC countries still lag behind in having appropriate capacities for baseline cyber security. The cyber security threat landscape of South Asia is dominated by threats

like data breaches and hacktivism, with recent revelations of cyber espionage by various countries ((Dilipraj, 2015). A closer look at the aspects of cybersecurity of each SAARC member state will also help us understand the cyber security posture of the region.

4.2.1. Afghanistan

A country with a fragile political environment, Afghanistan continuously struggles with nation-building. Since 2003 Afghanistan has been able to kickstart only a few ICT-related projects to speed up internet penetration. Due to limited cyber-awareness that is too eclipsed by political turmoil, Afghanistan lacks e-government services. However, few e-government programs such as National ID cards, E-governance resource centres, and establishing ICT villages have been put forward by the Ministry of Communications and Information Technology (MCIT). With the growing immersion in the cyber environment, Afghanistan framed the "Telecom and ICT Policy" in 2003 along with the "Information and Communication Policy" The drafts of the ICT law and "National Cyber Security Strategy" were submitted to the Parliament for its approval by 2014((ITU, 2014). Before the occupation by the Taliban in 2021, Afghanistan participated in a ten days NATO organized Cyber Defense Training Programme in 2012 to help secure the Afghan Network and Administrative systems ((NATO, 2012). Due to the lack of widespread cyber resources, Afghanistan seems to be at low risk from cyber-attacks, although new threats keep emerging. Hacker groups like the "Afghan Cyber Army (ACA)" have made numerous hacking attacks on various targets, which include both government and private websites and networks in Pakistan, the US and China (Dilipraj, 2015).

4.2.2. Bangladesh

Bangladesh is one of the freshest sovereign states in the South Asian region. Bangladesh is also comparatively forward in modernizing ICT-related development projects. Although Bangladesh is a relatively small country, with an area of 1,47,570 square km, it has already been subject to several cyber-attacks, from its foreign ministry website to its security infrastructure (Islam M. , 2013) as the number of internet users keeps increasing rapidly. Several unfortunate incidents, such as

religious fanaticism and The Gulshan attack in July 2016, can be linked to easy cyber access (Islam M. S., 2021).

In 2014, Bangladesh adopted the “National Cyber Security Strategy”, primarily focusing on the development of cybercrime legislation that is also in line with international and global norms (Ministry of Posts, Telecommmunication and Information Technology, 2014). As part of this strategy, the government, organizations in all sectors, individuals, and international partners are urged to collaborate to mitigate cyber threats (Islam M. S., 2021). Expressing commitment to cooperation in addressing cyber challenges. In 2016 Bangladesh drafted Digital Security Act 2016 to address “the need for cybercrime legislation” ((Jamal E. M, 2016) and is preparing to pass the “Digital Security Bill”. When Bangladesh's central bank was the target of one of the largest digital bank heists to date, the country's cybersecurity policies became internationally visible. Notably, hackers stole US$101 million from Bangladesh Bank's New York Federal Reserve Bank account in February 2016 (The Daily Star, 2016).

From the infrastructural point of view, the Rooppur Nuclear plan is one of the most critical infrastructures that need the utmost protection to avoid any mass disaster. The steps taken by Bangladesh seem to be moving in the right direction in terms of securing cyberspace, and the commitments made by Bangladesh also demonstrate the willingness to cooperate with national and international partners. Bangladesh has also sought cooperation bilaterally. For example, Bangladesh and Russia have agreed to form a joint working group to combat cybersecurity risks by agreeing to establish a “Centre of Excellence in Cyber Security” (Dhaka Tribune, 2018). Bangladesh also signed a Memorandum of understanding (MoU) with India in 2017 with regard to cybersecurity cooperation (India Today, 2017) where a joint committee on cybersecurity would be set.

4.2.3. Bhutan

Bhutan, as a landlocked country which has resisted dramatic modernization processes in the past, is also beginning to adapt its strategies to the changing world with regard to cyberspace. Bhutan started the “Bhutan e-Government Master Plan” in 2014 to roll out nationwide Broadband connection. In 2011 Royal Government of Bhutan opened

the country's first IT park, also known as Thimphu Tech Park, promoting and encouraging a technology-based environment for innovation, learning and collaboration with the aim of attracting reputed IT companies from different parts of the world (Dilipraj, 2015). This Tech Park also houses the Bhutan Innovation and Technology Centre (BITC), aimed to function as a business incubator for new start-ups and a shared technology centre – as a one-stop shop for business ventures in Bhutan for their technical needs and as a data centre for data storage and management for the government and the private sectors (Thimpu Tech Park, 2021).

Bhutan so far appears to be taking slow steps in working towards securing cyberspace. For instance, the country does not have any particular designated agency or intuition that supports in detection, tracking and mitigation of potential cyber-attacks. This institutional void could open gates for all kinds of cyber intrusions without even being detected. There have been several instances of government cite hacking in Bhutan. Moreover, Bhutan's cyber space is infested with all sorts of malware and spyware like Ghost Net, which creates an insecure cyber environment for the country considering how the individual users of the internet are prone to online scams and other social engineering methods of cyber thefts and cybercrimes like the Nigerian 413 scams and phishing due to lack of proper cyber awareness among the general public (Dilipraj, 2015).

Bhutan has, as of yet, not created any concrete legislative mechanism to address the cyber issues. There is no official cyber law, and ICT incidents/crimes are not clearly distinguished from traditional ones, although ICT-related cases are referred to in the Bhutan Information Communication and Media act 2006. Even though there is no comprehensive law or institution to address cyber issues, a separate cyber unit monitored by the attorney general was planned to be set up on August 31, 2014, under the aegis of Prime Minister Tshering Tobgay (Security-Risks.com, 2014). Bhutan also does not seem internationally active in tapping the resources and expertise in order to catch up with the ever-changing nature of cyberspace. Owing to the asymmetrical dependence on India, Bhutan is yet again reliant on Indian support to secure its cyberspace.

4.2.4. India

Compared to other South Asian counterparts, India is much more advance in terms of technology, institutional and policy framework in cyber space. Owing to its massive population, India has the most significant number of internet users, while it is also one of the leading exporters of IT products and services. The ICT sector contributes a considerable share of the Indian economy as there are large numbers of domestic customers. In 2000, the Indian parliament enacted Information Technology Act primarily to regulate online commerce. However, massive growth in information communication technology, as well as cybercriminals, soon challenged the 2000 version of the Information Technology Act, which did not adequately protect data, including sensitive personal data, or address issues concerned to the growth of e-commerce (Basu & Jones, 2003), cyber terrorism (Halder, 2011) and crimes targeting women and children (Halder & Jaishankar, Cyber crimes against women in India: Problems, perspectives and solutions, 2008) Observing the cases of countries such as United Kingdom, United States etc. following the 9/11 attack and how they tailored their cyber security laws and policies (Collin, 1997), India realized that their existing Information technology Act, 200 was not adequate to handle cyber terrorism and cyber warfare incidents such as Mumbai Taj Hotel attack (Halder, 2011).

Even though a new Bill in 2006 was already framed by the parliament to address data security, it was still not sufficient to address criminalities, including cyber terrorism and cyber warfare. Therefore, the Bill was revised, and a new version of the Information Technology Act was implemented in 2008. This act tries to address cyber security aspects comprehensively and therefore is still the primary law that regulates electronic governance, electronic commerce, and cyber security, and cybercrime-related issues are the Information Technology Act, 2000(Amended in 2008) (Halder & Jaishankar, 2021). India has come across incidences of data and information security breaches for critical information infrastructures, even targeting the Central Bureau of Investigation (CBI). Security experts have expressed their concerns about lacunas in cyber security and auditing of the documents and databases by the Government as well as Government-authorized stakeholders (PTI, 2010). It is also noteworthy that while India is the biggest market for social media websites and messaging services like WhatsApp (Pavan, 2016), hence it is essential for India to be

equipped with cyber security laws to provide protection for its citizens on the social level including critical infrastructure information, critical sectors, and personal data to a satisfactory extent (Halder & Jaishankar, 2021).

India introduced National Cyber Security Policy in 2013, prioritizing infrastructure, development, and public-private partnerships, but the policy is still not adequately implemented, resulting in invasions of privacy and human rights abuses (Shairgoji, 2022). Cybercrime in India can take many forms, from viruses to hacking to identity theft to spamming to email bombing to website destruction to cyber defamation. Indian Prime Minister Narendra Modi has claimed that the "Digital India" plan aims to connect every gram Panchayat to broadband internet in order to boost governance so that India can be transformed into a connected knowledge economy. This plan has been approved by the cabinet and is an indicator of how India is serious about Digital transformation.

Institutionally, India has created several organizations, such as the National Center for the Protection of Critical Information Infrastructure and National Technical Research Organizations (NTRO), including CERTs at the national as well as sectoral levels. In terms of capacity building, The Military College of Telecommunications Engineering in Madhya Pradesh now has a cybersecurity lab for officers to learn about signal and data transmission network security (Shairgoji, 2022). Considering the increasing reliance on IT by the Indian military and government agencies, the Indian Ministry of Defense also founded Indian Army’s Cyber Security in 2005 in order to protect networks and conduct cybersecurity audits. India has mainly faced cybersecurity attacks on its critical infrastructures ranging in sectors like energy, finance, defence and telecommunications, posing a serious threat to the country’s economy and public safety. India, however, still lacks a comprehensive national security strategy which incorporates the cybersecurity aspect as has been done by other big nations across the world. India also doesn’t appear to be taking prominent initiatives in creating a collaborative environment with its South Asian neighbours to address emerging cyber-security issues.

4.2.5. Pakistan

Pakistan, a developing country in the Global South, first gained access to the internet in the 1990s, and now Pakistan ranks tenth in the world when it comes to internet users. (Kemph, 2020). The state is moving in the direction of conventional to digital systems, thus making it susceptible to increasing cyber-attacks (Khan, 2021). It is estimated that 20 cyber-related cases are reported daily in Karachi's metropolitan area (Islam, Khan, & Zubair, 2019). Pakistan is also concerned about international interference via cyberspace. For example, a hacking incident occurred in 2019 via WhatsApp when senior Pakistani officials' mobile phones were accessed with 'Pegasus' malware. After reports emerged that Indian intelligence had used the same malware to spy on politicians, lawyers and so on at home, concerns regarding this incident became more widespread. (Khan, 2021). In addition, Pakistan is one of the main targets of US national security surveillance (Qadeer, 2020) and it also faces cyber threats from hostile intelligence networks and anti-state elements that operate from within the country.

Until now, Pakistan doesn't have a comprehensive strategy to address cybersecurity challenges. However, cyber regulations have evolved considerably. "Electronic Transaction Ordinance, 2002" (ETO) was the first document to recognize electronic transactions and cybercrimes. Soon the Electronic Crimes Act followed in 2004 that dealt with "cyber stalking, electronic fraud, cyber war, data damage, electronic forgery, spoofing, cyber terrorism and punishments for cybercrimes" (Iqbal, 2021). Considering the international threats, Pakistan faces extensive surveillance from the United States, and after the alarming revelations made by Edward Snowden on espionage activities conducted by the US through the internet, Pakistan's chairman of the Senate Committee on Defense proposed the 'Seven Points Action Plan' (Senate of Pakistan, 2013). This Action Plan presented strategies to defend sensitive infrastructures of the country, later contributing to the framing of the cybersecurity agenda at a national level. In 2016 Pakistan passed cybersecurity legislation called the "Prevention of Electronic Crimes Act" (Sridharan, 2016) covering issues of cyber terrorism, online glorification of offence, hate speech, electronic fraud, spamming, identity theft, spoofing, and cyber stalking and so on.

Furthermore, the country faces another serious cyber challenge in the form of data theft. In 2017 Punjab Information Technology Board revealed that millions of citizens' data had been compromised, making it one of the biggest data breaches in Pakistan's history (Kalyar, 2019). In building cybersecurity infrastructure, National Response Centre for Cyber Crimes (NRCCC), under the Federal Investigation Agency (the primary law enforcement agency), and Pakistan Information Security Association (PISA), a nongovernmental organization that works alongside the private sector to mitigate commerce-related threats, are two of the main organizations tasked with maintaining cybersecurity (Baker, 2014). Pakistan still has work to do in formulating state-compatible cybersecurity measures rendering the overall posture of the country as weak.

4.2.6. Sri Lanka

The island nation Sri Lanka has a scarred history of civil war between the government and the rebel LTTE (Liberation Tigers of Tamil Ealam) forces. Despite a war-torn history, the country is fairly ahead in the development of the ICT sector, particularly in measures undertaken by the government (Access Now, 2022). In 2002, the government launched the “e-Sri Lanka” project with the mission of developing an ICT roadmap for the country, which further led to the implementation of the Information and Communication Technology Act 2003 (Dilipraj, 2015). This Act was the basis of various cyber initiatives afterwards. As a follow-up for ICTA, Sri Lanka introduced Acts addressing E- identification and E-services. The Computer Crime Act 2007 also established mechanisms for the fight against cybercrimes. Likewise, to provide for the implementation of the National Cyber Security Strategy (2018), Sri Lanka proposed Cyber Security Act in 2019 (Cyber Security Bill, 2018). The Sri Lankan government has invested in ICT capacity building and also encourages the domestic IT-based industry for growth with the vision of export (Businessmirror, 2022). Sri Lanka’s profile as one of the ‘outsourcing’ destinations for IT-related jobs has been moving in a positive trend in recent years (Moorthy, 2022).

However, Sri Lanka, too, is not free from cyber threats. Sri Lanka’s digital society has been subject to malware, phishing, hacking, defacement of both government and other non-government websites, DOS/ DDoS attacks, hate/ threat mail, identity and information thefts, etc., including banking frauds via cyberspace and social

engineering scams (Fernando, 2021). Sri Lanka is also subject to cyber terrorism, where LLTE have hacked the government's information infrastructure several times, also being the world's first terrorist group to attack a country's computer systems in 1998 (Bulathgama, 2021). In order to prevent or deal with these threats, Sri Lanka has put in place several Cyber Crisis Management tools such as "Sri Lanka Computer Emergency Readiness Team | Coordination Centre" (SLCERT | CC). The SLCERT offers services in responsiveness, awareness and consultancy (cite another writer). The SLCERT | CC is also a member of the Asia-Pacific Computer Emergency Response Team (APCERT), which is a collective organization that includes CERTs from different countries in the Asia-Pacific region and works for the cyber security of this region (SLCERT, 2019). In terms of international cooperation, Sri Lanka is the first country in South Asia to accede to Budapest Cybercrime Convention in 2015.

4.2.7. Maldives

Maldives is a country comprising 1,192, and over the past two decades, the island nation has experienced steady socioeconomic growth with some of the highest social, economic and health indicators in the South Asian region (ADB, 2007). As tourism is the primary source of income for the country, the country started making ICT development efforts form 2001 with the vision of providing comprehensive tourism services. Maldives began improving its telecommunication infrastructure, even transitioning from Satellite to a Fiber Cable Network in 2006. The government also initiated a project called "Government Network of Maldives" (GNM), enabling e-government services. Maldives has now become the leading country in the South Asian region with the highest rank on e-government readiness (Shareef, 2010).

A growing number of cybercrimes have been reported in the country with the rise of internet consumption and ICT use, and the country is even more vulnerable as it does not have any cyber laws or a cybersecurity agency up until now (Waheeda F. , 2015). As a result of the lack of an inclusive cybercrime legal framework and the obstacles to collecting evidence, this state presents a challenge to law enforcement (Zalif, 2020). As a result of cybercrime, the Maldives has been facing hindrances since 2009. The crimes have ranged from credit card fraud and phishing, unauthorized access, hacking, chat-abuse and social media blackmail. A large number of Maldivians also fall victim to fake Short Message Services (SMS), phishing, fake lottery and

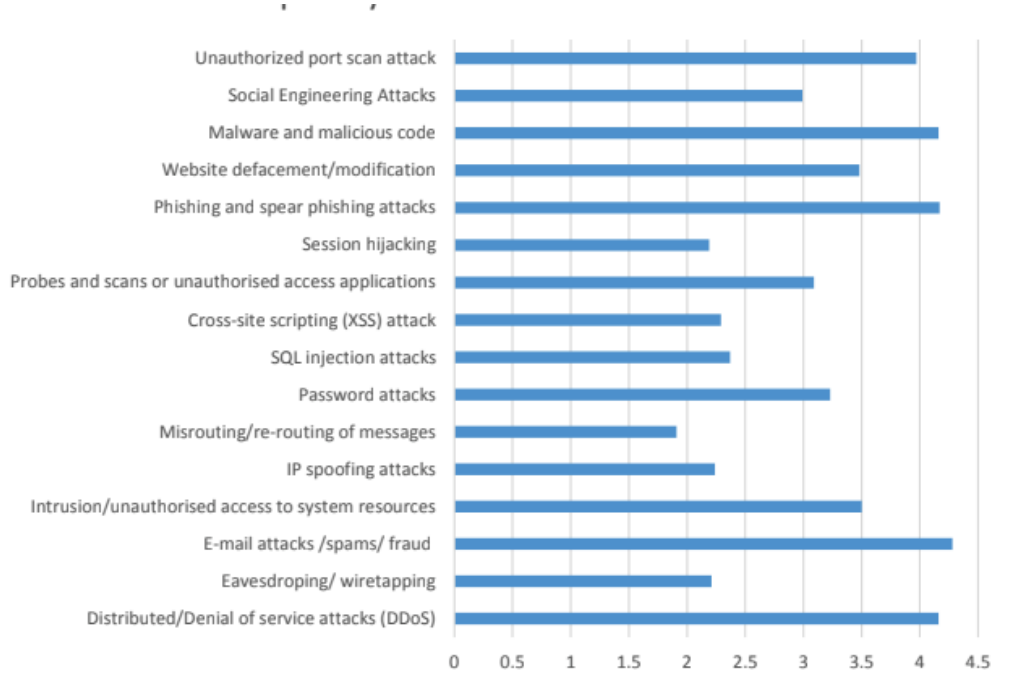
promotions. (Nadira, 2018). Because of their vulnerability and poor security, many E-platforms, including internet banking and government websites, are also often hacked (ITU, 2012).

There are no cyber-security policies in place in the Maldives, nor have they drafted or implemented any laws addressing information and communication technologies to protect their citizens. (Waheeda F. , 2018). For now, The National Centre for Information Technology (NCIT) is responsible for the development and promotion of information technology in the country (Waheeda F. , 2015). Maldives participated and signed the Ministerial Declaration for the ABBMN Forum organized by ITU on Digital Inclusion (ITU, 2010) however is still slow in making progress in developing a cybersecurity framework or devising any legislation in the area (DoNP, 2018).

CHAPTER V
CYBER SECURITY CONCERNS OF NEPAL

Nepal doesn't have a long history of using computers, as it wasn't until the 2000s that access to computers began to be easier for the common population. The internet made it to Nepal only in 2006, and at the time, only 1.1% of the population had access to it. Today, however, the situation has transformed, where the country has 73.8% (National Judicial Academy, 2022) of Internet users. A major driver of internet adoption in Nepal has also been the popularity of social media (Digital Nepal Framework, 2019). The use of telecommunication services and the internet has drastically changed the cyber capabilities of Nepal in a short span of time. However, the transformation doesn't come without risk, especially when cyberspace can also be misused as an extended space to support traditional crimes.

In Nepal, news portals frequently report cyber security breaches. Digitalization has certainly presented security challenges, such as attacks on government websites and anti-government demonstrations organized via the internet (Government of Nepal Ministry of Home Affairs, 2020). The most common attacks have been found in the banking sector. The figure below illustrates different attacks in Nepal's banking sector graphically.



Source: (Maharjan, 2019)

Figure (v): Graphical representation of different attacks in the banking sector of Nepal

With the speeding up of the mandatory process of digitalization, the security threat also increases. Several laws have been formulated by the government of Nepal to legalize certain digital activities, but most of them do not address the emerging cyber threat landscape rendering Nepal the high risk in cyber security owing to slow implementation of laws/policies, lack of appropriate defence system preventing cyber-attacks and low-level cyber security awareness among the people (Acharya & Dahal, 2021). A survey conducted by the Nepal Army, which maintains national security, has shown that armed forces are also unaware of cyber security (Roka, 2017).

5.1. Cyber Attack Incidents in Nepal

The instances of data breaches, data theft and government websites being hacked have become quite common in Nepal due to increasing digital dependence and growing internet access in Nepal, which has invited various cyber-attacks. According to Live Security Threat Map, Nepal is seen as one of the top targeted countries with cyber-attacks with malware like Adware, Phishing and Backdoors (Live Cyber Threat Map, 2022). Table (iii) below gives us a glimpse of the cybercrime status of Nepal, which shows us that the trend of cybercrimes is only increasing. Due to the insufficient scope of the existing laws, many of these cases haven't received appropriate judicial attention (National Judicial Academy, 2022).

Year	Cases Registered	Cases Adjugated	Cases Appealed
2064	-	-	-
2065	-	-	-
2066	-	-	-
2067	2	2	1
2068	6	6	2
2069	8	7	4
2070	7	7	4
2071	38	38	27
2072	24	24	12
2073	36	35	16
2074	24	23	5
2075	61	60	16
2076	46	46	6
2077	52	-	-
2078	20	-	-
Total	325	249	93

Source: Kathmandu district court (National Judicial Academy, 2022)

Table (iii): Data of Cyber Security Cases in Kathmandu

Nature	2067	2068	2069	2070	2071	2072	2073	2074	2075	2076	Total
Defamation	1	2	4	4	18	15	15	14	29	19	121
Blackmailing	1	1	2	2	11	11	9	8	20	15	80
Harassment		2	2	2	14	10	12	17	23	20	102
Unauthorized Access				1	1	1		1	2	2	8
Data leakage			1							1	2
Hacking					1	1	3			1	6
Fraud						2			1	2	5
Against public morality					1						1
Against national Integrity					1						1
Unauthorized Recording					1						1
Data theft			1							1	2
Phishing			1								1

Source: (National Judicial Academy, 2022)

Table (iv): General Nature of Cases in Nepal

As table (iv) above shows us the patterns and trends of cybercrimes in Nepal, it does not show us if any cybercrime was induced via a foreign actor. Apart from internal cases of internal cybercrimes, as shown in the table and some social media-related cybercrimes, Nepal has also faced attacks from foreign actors. For example, a group of Turkish Hackers hacked the Department of Passports in 2017 and defaced their website with threatening notes to reveal the data of the government (My republica, 2017). The same year, one of Nepal's largest breaches of all time occurred when 58 government regime websites were hacked by a Palestinian group called Paradox Cyber Ghost.

Another prominent case is when five Chinese nationals hacked and robbed ATM machines in Kathmandu with cloned debit cards making it one of the biggest heists in Nepal up to date. This incident revealed the realities of Nepal's weak cyber security (The Kathmandu Post, 2019). Cyber Espionage attempts from Chinese actors have also been identified (against Nepal and India security and commercial establishments) as a so-called "advanced persistent threat" group named Suckfly. Having stolen certificates from South Korean firms, Suckfly had been found using them as cover for its cyber-attacks through malware like "Backdoor.Nidiran" (The Times of India, 2019).

Additionally, cyber activities in Nepal from a social media perspective should also need to be considered. For instance, during the border dispute between India and Nepal in the Kalapani Lipulekh area in May 2020, disillusionment was widespread in cyberspace at the grassroots and civilian levels (ICT Frame, 2020). During this time, the tension not only remained in social media but also escalated to a cyber-attack where hackers took down more than 45 Nepali websites, including the website of the Nepal National Library and the official website of the Civil Authority of Nepal (ICT Frame, 2020). In a similar manner, Nepalese hackers leaked the API key of Indian media ABP by tweeting a link to the sites (ICT Frame, 2020).

5.2. Nepal's Initiative for Cyber Security

ICT ramifications have gained prominence throughout politics, economics, and cultures since the new millennium, igniting a paradigm shift towards newer crime in the digital avenues. (Sarkar, 2021). Resulting in a cyber policy regime created by various thematic government bodies. Irrespective of the adequacies to prevent sophisticated cybercrimes, it can be observed how far Nepal has gotten in realizing cyber issues via the table below, which shows 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. This 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 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 a provision relating to electronic records and digital signature, a provision relating to the computer network and network services providers, a provision relating to computer-related crimes and punishments and the 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, 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 of 2053 (1997) has evolved into an active legal instrument to regulate cyber activity. More than ten directives and rules are issued by the Nepal Telecommunication Authority (NTA) on the basis of the Telecommunication Act, 2053 (1997). Chapters 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 By laws 2075 (2018)(MDMS Bylaws)	Bylaws issued by NTA		NTA has framed these MDMS Bylaws for the implementation of an Equipment Identity Register (EIR) system to ensure national and consumer security, to identify genuine mobile handsets and make the fake and non-genuine

			handsets inoperable in Nepal, to enable tracking/blocking of a 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 instructions not to provide service on illegal mobile devices which are not registered in NTA. These Bylaws are important not only 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 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 guideline number 26 that an 'online child abuse complaints system' will be developed and brought into operation. Also, ISPs / MNOs are given instructions to show whether the available content on the Internet is suitable for the age group of children or

			not.
Cyber security By-laws 2077 (2020)	Bylaws issued by NTA	During the lockdown of 2020, NTA issued Cyber Security Bylaw, 2077 (2020), at a time when another cyber-attack was 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 the ICT Infrastructure and Information Systems of Telecommunication Service Providers of Nepal from various malicious attacks and threats and build the 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 the cyber security of Nepal. It directs to examine the risks posed by common technical and

			human errors 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 been 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. The practice has issued binding suggestions to reduce human error in cyber security in offices under the Government of Nepal, and it does not have a legal provision to issue penalties.

Source: (Acharya & Dahal, 2021)

Table (v): Nepal's Cyber Security Initiatives

As seen in the table above, various governmental bodies within the country have begun formulating rules, laws, policies and guidelines to administer cyber activity; however, they are limited in regulation, jurisdiction, and numbers. Through documents like the Digital Nepal framework and Cyber Bylaws, Nepal has indeed articulated a vision for cybersecurity, but by observing the activities so far, it is

struggling to implement these programs due to insufficient resources allocation as well as due to the provision of cybersecurity which could compete with other social values, for example, freedom of assembly, information and freedom of speech. These laws and rules, however, do not have any clear or compatible provisions to deal with cyber activities that cover a wider national security perspective, particularly in the diplomatic context.

5.3. Analyzing Nepal's Cyber Security as a Developing Country

Nepal hasn't had an updated National Security Policy since 2016. The 2016 national security policy launched by the Ministry of Defense states that "functions relating to national security have to be carried out through the defence policy, foreign policy, economic policy, internal security and public information policy having a timely analysis of internal and external circumstances" (National Security Policy 2016, 2016) which is ideally supposed to guide the nation to build suitable security strategies as well as direct defence policy including internal security policy.

The National Security Policy 2016 acknowledges the "rise in international crimes and misuse of modern technology"; however, it does not seem to be any mention of cyber-security in section 1.9, which is about 'Threats and Challenges to National Security'. The document only vaguely mentions creating a "cyber security system for defending and protecting electronic financial structure" in its strategic objective. With the changes that have happened in the world and in Nepal itself, the scope of this document to justify the national priorities of Nepal is already questionable. Reportedly the government already passed a new National Security Policy on March 18, 2018; however, the document has not yet been made public (The Rising Nepal, 2020).

The Digital Nepal Framework (DNF) 2019 is one of the ambitious approaches by the government to support and encourage ICT Nepal is expected to act as a roadmap towards the country's digitalization with the main objective to foster economic growth to participate in the global economy. The DNF, with the aspiration of integrating ICT into Nepal's holistic development, has divided eight developing categories and assigned them 80 digital initiatives in total, envisioning socioeconomic growth. Among these eight categories, the category 'Digital Foundation' is assigned

19 initiatives, and one of the initiatives within them is about building a National Cyber Security Centre. In recognition of the need for comprehensive data security controls, the document proposes the creation of a national cyber security cell tasked with preventing, detecting, defending and recovering from cyber-attacks, although the scope of their operations is not clarified. The economic priorities subdued in the document make it obvious that cyber security is primarily considered from the financial perspective. According to the document, it aims to secure government networks, protect critical infrastructure and assist citizens and businesses in securing their own systems.

With the launch of Apps like the Nagarik App, the Nepal National Single Window (NNSW) system and the electronic National ID card, the momentum of digitalizing public services has already begun in Nepal. The records and data of Nepalese citizens, either stored in some server or cloud, demand adequate security more than ever. In the latest budget announcement, about 0.48% out of the total budget of 1.472 trillion has been allocated for the development of the ICT sector with the main focus on cybersecurity, national payment gateway, and mobile pp for farmers, e-learning, broadband expansion, Digital Nepal Framework etc. (Youtech Nepal, 2020). Recently the Ministry of Communications and information Technology (MoCIT) also announced an investment of NPR 22 billion for The Digital Nepal Framework project, where NPR 17 billion is invested by The World Bank and NPR 5 billion is received by the Ministry as a business loan (Nepali Telecom, 2022). We are yet to see how much of the fund will be utilized in to fortify the cyber security of the whole nation as the scope of investment wasn't finalized at the time of this study.

5.4. ICT as a Critical Infrastructure in Nepal

Nepal is finally on the verge of graduating as a middle-income country (United Nations, 2021). A World Bank report says that to meet the expectation of being a middle-income country, Nepal needs to prioritise closing the infrastructure gap as Nepalese citizens have, for too long, hasn't received reliable and adequate access to infrastructure services (World Bank, 2019). ICT infrastructures are only beginning to spread in Nepal. It wasn't until 1995 that optical fibre was introduced in Nepal, facilitating the launch of the internet. In the beginning, the internet was scarcely used by the government and some big companies; however, owing to the initiation of

private sectors, Internet Service Provider businesses started emerging, and today internet has already become an essential part of the socioeconomic environment in Nepal. Currently, the internet penetration in Nepal is 63% ((The Kathmandu Post, 2018); however, the internet usage data is only 38% (World Bank (a), 2020).

Institutionally, the promotion of Information Technology began in 2002 at the government level with the establishment of the National Information Technology Center (NITC). Shortly after, NITC established a network within government agencies with financial support from the World Bank. The project helped connect all the central government agencies through optical fibre resulting in the mainstream usage of computers in government services. The IT development in Nepal is guided by the e-Government Master Plan (e-GMP) developed by Korean Information Technology Promotion Agency (KIPA) in 2006, covering the sectors like e-Health, e-Education, e-Agriculture etc. (Sharma, 2016). Many components of this plan haven't been satisfactorily implemented due to political hurdles, although the e-GMP Government Integrated Data Center (GIDC) was established in 2009 as a standard data centre with the support of the Korean Government. GIDC is responsible for providing services like data storage, sharing computing resources, email/internet and website hosting to all the government ministries and departments, making it the high-grade data centre at a national level (NITC, n.d.). It is clear that all the critical data of Nepal is in one place, which raises the stake for the threat.

5.5. Digital Divide in Nepal

There's no denying the connection between Digital Divide and cybersecurity. The digital divide is usually described by scholars as a lack of access to ICTs and the inability to use them, which contributes to a great economic as well as a political disadvantage (Ayanso & Lertwachara, 2010). Even though cyber warfare does relatively little damage to them, developing countries are more vulnerable to cyber-attacks. Digital disadvantaged nations have weak cyber security, and this insecurity could further weaken a nation's international geopolitical standing (Gamreklidze, 2014). Disrupted communication and services due to cyber insecurity as a result of the Digital Divide could erode the cyber power of a state, ultimately diminishing the global standing of that state (Manjikian M. M., 2010).'

Nepal, including many developing countries, faced a serious disadvantage during the Covid-19 pandemic when access to education was majorly disrupted due to a lack of necessary digital infrastructure throughout the nation (Pudasaini, 2022). Owing to the connection between the digital divide and poverty, we could argue that Nepal is a 'digitally marginalized' country, with some internet access and limited digital literacy of only 31% (Baniya, 2021). More than 23% of the Nepalese population is still under the poverty line, and 66% of the population is work force which is engaged in agriculture. This also explains the slow adoption of digital infrastructure from the context of less demand-driven digital penetration. Cultural and language factor has also equally contributed to the digital divide in Nepal. There are about 123 different languages spoken within the country; about 44% use the national language Nepali, and only about 2- 10% of them can understand English. This linguistic diversity also acts as a barrier to digital proliferation.

Language	**Population%**
Nepali	44.6
Maithili	11.7
Bhojpuri	6
Tharu	5.8
Tamang	5.1
Newar	3.2
Bajjika	3
Magar	3
Doteli	3
Urdu	2.6
Other	18

Source: (Nepal in Data, 2018)

Table (vi): Languages Spoken in Nepal

So far, Nepal hasn't given enough space to the inequality of digital capacity in national discourse; however, several NGO initiatives have already noticed the digital divide and have started working towards it.

5.6. Digital Sovereignty

Recently, the term “sovereignty” has been used more frequently when discussing topics of “digital”, “data”, and “technology” since data, including electronic computing techniques, have increasingly become the information commodity in today’s digital world (Toupin, 2019). The concept of digital sovereignty has also become a topic of discussion for state actors. As seen in chapter 4, countries like Russia have already assigned great importance to information security, and China is also quiet vocal in terms of maintaining digital sovereignty. A form of cyber-alliance also has been observed between these two countries with regard to “internet sovereignty” in global discourse (Budnitsky & Jia, 2018). We can accept that the idea of sovereignty could easily be compromised by any global pandemic or disaster. Similarly, the global spread of telecommunication infrastructures and, with it, the internet has also contributed to brushing blur lines to the idea of sovereignty. While the practice of state sovereignty has kept enduring through several political instruments, such as international or bilateral treaties, the make-up of contemporary international relations is still new to the concept of digital sovereignty, especially when the governance or regulation of the internet transcends the national borders. The state actors’ argument in terms of digital sovereignty significantly revolves around the topic of data control or regulating the flow of data because the socioeconomic stakes of data protection are not only limited to the technical periphery but have also become a matter of political priority.

Data protection is a big part of digital sovereignty. It has become increasingly common for personal data to be processed on the Internet instead of in the country of origin of the data subject, and the fragmented legal framework that exists is no longer viable. (Albrecht, 2016). Regions like the EU recognize data protection as a fundamental right. The Snowden revelation was a big wake-up call for nations and individuals to see data as a critical asset. The mass surveillance programme called Pegasus Project, led by US National Security Agency, was ethically questionable on many levels. The mere ability of “cyber rich” countries to encroach the cyberspace of nations and individuals with the usages of highly sophisticated Spyware without the individual or the nation even noticing shows us the asymmetry in possessing cyber capabilities. National-level legislation and the development of domestically developed

technology have been used by many governments to safeguard state and citizen data (Toupin, 2019). The former Brazilian president Rousseff introduced a plan aimed at freeing the Brazilian Internet of the influence of the United States and its tech giants, a move that has been described as an attempt at asserting digital sovereignty (Armijo, 2014). In recent years, after the evidence of former President Merkel's email and phone surveillance by the United States, Germany has built "national emails, new undersea cables and localized data storage as a counter strategy" (Maurer & Morgus, 2015). In Canada, the Canadian Network Sovereignty has also been called for improving infrastructures so as to "diminish data routing through the United States", acknowledging the threat to national sovereignty "when an otherwise internationally independent state has its rights and powers of internal regulation and control violated by the encroachment of a foreign body" (Clement, 2013).

Nepal isn't spared from sly mass surveillance as well as data theft. The Wikileaks published in 2010 about China-Nepal correspondence is a good example of where the confidential document that was leaked could have compromised the diplomatic relation with its neighbouring countries (Ankita Mukhopadhyay, 2020). It has also been reported that state-sponsored hackers exploited the territorial disputes in 2020 between Nepal, India and China to target government and military organizations across South Asia, including the Nepalese Army and the Ministry of Defense and Foreign Affairs. (Center for Strategic and International Studies , 2022). With the speeding up of e-government services, Nepal has implemented a structure called GEA (Government Enterprise Architecture and Interoperability Framework) to standardize the electronic government work so as to arrange information and services in such a structure in which information and services can be accessed from the collective government system (Department of Information Technology, 2019). Many electronic data are stored in cloud-based storage, which is facilitated from foreign servers, as Nepal does not have its own satellite server. This increases the vulnerability of data breaches when Nepal's data are transferred between servers located in neighbouring countries (Acharya G. , 2022). Despite the resource limitations, the GEA framework does provide guidelines for securing data flow, encryption, data centre localization national routing of internet traffic for the protection of national backbone communications infrastructures (Nepal GEA 2.0, 2019).

5.7. Capacity Building for Nepal

There is undeniable economic benefit in the ICT sector, and many developing countries are already on the verge of yielding opportunities for their ICT industry which is why the countries should not take cybersecurity lightly. Owing to the digital divide developing countries with poor technical security standards are prone to acquire unsecured or even flawed products from the market, which poses an even bigger risk to the cybersecurity dimension of the country. In developing countries, poor cybersecurity is also attributed to a lack of skills and knowledge - for example, basic awareness of cyber threats and 'digital hygiene' (Kshetri, 2010). For instance, the lack of digital education causes people to ignore simple security measures like updating software and operating systems. The ICT sector has been contributing NPR 77.16 billion to the Gross Domestic Product of Nepal, accounting for 2.22 percent of the total GDP of the country (Central Bureau of Statistics, 2021).

The insufficient human, as well as technological resources, have limited the country from unleashing its full potential. In Nepal, 90% of schools lack digital connectivity and ICT equipment. However, Nepal is preparing to entail digital technologies into the nationwide education system as per the Digital Nepal Framework. Many computer and cyber security courses, including some tailored courses, are available in education institutes and universities of Nepal but certain digital limitations, such as good internet quality and access to ICT devices, act as a barrier for the grassroots population to access such education. “Brain drains “is also one of the reasons for the lack of adequate IT professionals in Nepal. Nepal produces around 15000-16000 IT graduates every year, and more than half of them go for job opportunities overseas (The HRM, 2022). The investment in Research and Development to promote innovations, as well as usage of ICT services, is also negligible in Nepal.

5.8. International Cooperation by Nepal for Cyber Security

Small and developing countries usually experience undermined diplomacy owing to their relatively weak position in the international political sphere. Factors such as professional competency and resources also greatly affect the representation of developing countries in the arena of international decision-making and negotiations.

Similarly, there hasn't been much effective participation from developing countries with regard to digital policy debates (Hanna, 2017).

Table (vii) below provides estimates of regional financial losses due to cybercrime:

Region	Income level	No. of countries	Region GDP (US$, trillions)	Cybercrime cost (US$, billions)	Cybercrime loss (% GDP)
East Asia & Pacific		**36**	**22.5**	**120 to 200**	**0.53 to 0.89%**
thereof	High income	12			
	Developing	24			
Europe & Central Asia		**55**	**20.3**	**160 to 180**	**0.79 to 0.89%**
thereof	High income	35			
	Developing	20			
Latin America & Caribbean		**38**	**5.3**	**15 to 30**	**0.28 to 0.57%**
thereof	High income	13			
	Developing	25			
Middle East & North Africa		**21**	**3.1**	**2 to 5**	**0.06 to 0.16%**
thereof	High income	8			
	Developing	13			
North America		**3**	**20.2**	**140 to 175**	**0.69 to 0.87%**
thereof	High income	3			
South Asia		**8**	**2.9**	**7 to 15**	**0.24 to 0.52%**
thereof	Developing	8			
Sub-Saharan Africa		**48**	**1.5**	**1 to 3**	**0.07 to 0.20%**
thereof	High income	1			
	Developing	47			
Total		209			

Source: (Świątkowska, 2020)

Table (vii): Cyber Crime Cost and Cyber Crime Loss

Even though the table shows that the developing countries lose comparatively much less than developed countries, the economic consequences, however, could be much more severe for the developing countries as skillset shortages, untrustworthy strategic and legal systems, and the growing strength of organized criminal groups – to name a few – significantly impede economic conditions and the relative position of

developing countries in the international arena (Świątkowska, 2020). There are two parallel and competing interstate platforms created to discuss cyber issues. One is the Group of Governmental experts which was first created by the United States and supported by the "like-minded" states (UN GGE, 2021). And the second was created by Russia, which called for an Open-Ended Working Group (OEWG). While China, India Indonesia from the global south represents both platforms (UN Open- Ended Working Group, 2020) , Nepal isn't a member in any of them.

As per the Report on Nepal's Foreign Affairs (2019-2020), during the 74th session of the United Nations General Assembly, the then Foreign Minister Pradeep Kumar Gyawali, in his statement, mentioned that the absence of order in cyberspace endangered international peace and stability acknowledging that cybercrime is also one of the pressing global issues. But no calls for enhanced consultations, coordination and collaboration were made (Ministry of Foreign Affairs, 2020). The report faintly mentions that the delegation of Nepal made contributions on the topic of digital technology, among other topics such as peacekeeping, climate action, poverty and inequality, rights of women and girls and the role of youth; but does not provide any elaboration on the particularities of those contributions.

Nepal, as a developing country, is bound to continue its digital journey, subsequently finding its own priorities and trajectories. Yet, approaches with regard to building cybersecurity may not be efficient without coordinated efforts both with internal actors as well as international actors. Nepal, as a developing country, should seek support from advance states for developmental assistance, which includes digital aspects with cybersecurity as an embedded element. For example, the country could make efforts to overcome skill shortages and seek support for best practice transfers, technological aid and other initiatives to empower the nation against dealing with cyber threats.

5.9. Cyber Defense

The necessity of cyber-defense has clearly increased with the increase in cybercrimes and cyber-attacks. The growing dependence on cyber control over critical infrastructures also makes space for more vulnerabilities. The attacks on cyberspace can be of a very low cost while they can wreak great havoc due to features like

selectiveness and no limit of boundaries or borders. When it comes to cyber defence, only considering internet protection, information and data protection and software &system protection are not enough. From a national security perspective, the cyber defence has to be considered from the architecture, policy and strategic levels and only then at the operational level ((Libicki M. , 2009). Normally military is responsible for designing nationwide security strategies. However, due to the overtly multidisciplinary nature of cyberspace, significant non-military initiatives can also be found.

Nepal has done very little in terms of national cyber defence. Nepal Military does not have a cyber-defence unit; not there is evidence of cyber operations exercises. On a domestic level, The Cyber Bureau established under the Nepal Police Headquarters deals with cybercrimes and other cyber challenges to security and intelligence (Cyber Bureau, n.d.). Although due to the unclear demarcation regarding the authority, the international scope of the investigative abilities of the Bureau is, at best vague.

- **CERT Nepal**

  National Computer Emergency Response Team has been established by the government to respond to computer and network security incidents, report vulnerabilities, and encourage effective ICT security practices across Nepal. The teams are made of expert groups who are responsible for handling incidents related to computer security and aware people in the area of cyber security in Nepal (Nepal CERT, 2019). The role of CERT in shaping the cybersecurity posture of the nation could be very useful in dealing with changing nature and modes of cyber-attack as this is the organization that is comprised of both technical as well as political intellectuals of Nepal. However, only relying on Internet safety practices and working with regional CERTs does not provide a holistic defence against cyber incidents. Up until now, Nepal has had no formal assessment of cyber threats, and there are no reliable national mechanisms to anticipate cyber intrusions. Many developed countries have created an alliance to tackle cyber challenges. It is high time for Nepal to put forth strong calls for an allied cyber defence network on both regional and international forums.

CHAPTER VII
FINDINGS AND CONCLUSION

Cybersecurity is not the responsibility of the tech sector or private sector anymore. A multistakeholder approach is a given when it comes to dealing with cybersecurity challenges. As the ICT infrastructures permeate the whole world, effectively finding solutions for cyber threats in developing countries is not only the responsibility of the governments but also of private sectors, civil society and global leaders. The scope of cybersecurity is multidimensional in nature which requires pragmatic strategies. Cybersecurity in itself is also a matter of global stake; therefore, the discussion related to cybersecurity should also connect to global issues.

7.1. Findings

Many nations have been focusing on raising awareness of the issues surrounding the governance of cyberspace during the past few years. Directly related to the question of who wants to govern the Internet is the one who controls it. Many different groups, including users, communication companies, ISPs, and governments, sought to dominate the Internet as soon as it was made available for commercial use. Of all of these groups, the government's involvement was the one that drew the most criticism, but it is the government that has been able to exercise the most influence. Cyberspace has some defining characteristics that pose a number of legal issues for our current laws. These qualities include its disregard for territorial distinctions, the enormous volume of traffic it can handle almost instantly, its openness to participation, the potential for member anonymity in the virtual community, and its seeming economic effectiveness. As a result, the researcher draws the following conclusions for this dissertation:

- Because hackers still target Nepalese government websites, Nepalese citizens and the government are unable to recognize the severity of the country's cyber security issues. However, as the country's citizens and government delve deeper into cyberspace, the situation is changing (online payment and banking, e-governance, smart license, nationality card, embossed number plate etc.).

- The Digital Nepal Framework aims to integrate ICT into Nepal's development and includes a category on building a National Cyber Security Centre
- About 8 laws and policies has been created by various thematic government bodies. However, these laws and rules do not cover a wider national security perspective, particularly in the diplomatic context.
- The Electronic Transactions Act of 2006 and other Nepalese laws do not adequately handle the country's cyber security challenges or adhere to the Convention on Cybercrime's criteria (Budapest Convention on Cybercrime).
- The momentum of digitalizing public services in Nepal, including through the Nagarik App and the Nepal National Single Window system, has increased the need for data security
- Because it has no boundaries, cyberspace allows for anonymous behaviour. Hackers and other criminals take advantage of these features to commit crimes online.
- For any cyber security risk Nepal is currently experiencing or could experience in the near future, and the IT infrastructure and resources available are insufficient.
- The safety and security to be free from online harassment and persecution based on one's own political, ethical, or gender identity, as well as for her or his private professional, educational or health data without her or his consent, are all aspects of human rights in cyberspace.
- In many nations, both democratic and non-democratic, concerns about national security have long been used to justify broad surveillance measures, with more and more citizen data being collected and easily accessed by state authorities. This compromises privacy as the IT industry develops. It is also perceptible in Nepal.
- Lack of technology, human resources, and adequate funding to maintain it are the fundamental and key issues for all poor countries, including Nepal, in relation to cyber security.

- Developing countries, including Nepal, are more vulnerable to cyber-attacks and can have their international standing diminished by disrupted communication and services due to cyber insecurity
- Nepal is a digitally marginalized country with limited digital literacy and internet access, and cultural and language factors, including linguistic diversity, contribute to the digital divide.
- Nepal's Digital Nepal Framework includes initiatives to improve cybersecurity, but it is unclear how much funding will be allocated to this area.
- In Nepal, the ICT sector has contributed to the GDP and digital technologies are being incorporated into the education system, but there are still issues with access to education and a lack of IT professionals. Investment in research and development and the use of ICT services is also low in Nepal.
- There are two platforms for discussing cyber issues at the international level, one supported by the US and "like-minded" states, and one supported by Russia. Nepal is not a member of either platform and has not made specific calls for enhanced consultation and collaboration on cybersecurity.
- Nepal has done little in terms of national cyber defense. Nepal Military does not have a cyber-defense unit; nor there is evidence of cyber operations exercises. Nepal has National Computer Emergency Response Team (N-CERT) but is not sufficient to provide a holistic defence against all kinds of cyber attacks.
- Nepal has faced cyber-attacks from foreign actors, as a result of growing digital dependence and internet access. Nepal has also faced data theft and mass surveillance, including state-sponsored hackers exploiting territorial disputes to target government and military organizations.

7.2. Conclusion

Many developing countries lack sufficient resources to attain infrastructure and maintain them. Form the case study of Nepal, we can find that despite the growing awareness, the county has been able to allocate a very limited budget for the development of ICT sectors and, in particular, cybersecurity issues. This will significantly limit the country's ability to implement the frameworks and ICT development plans that have been proposed. This also affects building cyber capacity and creating professionals who can overcome the technological complexities and work towards building secure cyberspace. It is essential to have adequate institutional support and clear legal instrument which can enact necessary decisions in framing secure cyberspace. In the case of Nepal, the country has proposed ambitious cyber bills and introduced Cyber bylaws, but the scope of those documents is too broad and is less clear in matters of regulation, cyberspace governance and in punishing crimes. The Digital Nepal Framework, even though it proposes plans for economic development via digitalization, however, does not reinforce strategies that directly target cybersecurity.

The lack of understanding and recognition of cybersecurity as a national security challenge will lag the country behind in setting up a holistic plan. The awareness of government leaders affects the quality of reforms and support in the matter of cybersecurity. The foreign policy of Nepal and the National Security Policy has no clauses dedicated to cybersecurity. These documents are important in stating a consistent narrative to make sense of the digital position Nepal holds or intends to hold.

Nepal views cybersecurity primarily from a financial context and associates very little or nothing with the challenges of cybersecurity from a strategic standpoint. The increasing dependence of their essential systems on online networks certainly increases the vulnerability to cyber offensives for developing countries like Nepal, and up until now, Nepal is far from adequately identifying cyber threats specific to its national security orientation. After several catalyzing cyber incidents, Nepal has made several policy responses, and institutionally, a separate Department of Information Technology has been created, which is tasked with all the responsibilities for administering cyber-related activities. However, Nepal is still at the nascent stage of

cybersecurity development. Instead of allowing a defining incident to question the cybersecurity of the country on a national level, the country can take advantage of this nascent state of cybersecurity development in shaping mechanisms that are more niece to the country's needs and learning from others' failures.

Developing countries now account for the vast majority of internet users. Although advanced nations have more at stake in cyberspace than developing nations do, the latter are increasingly being drawn into its domain. Thus, they, too, are vulnerable to attacks from what are, in general, the larger and more sophisticated cohorts of hackers from the first world. Considering national vulnerabilities, if we are to distinguish nations which have undergone major cyber-attacks of cyber breaches to either military or civilian sectors with potentially devastating economic, social and political consequences; Nepal, as a developing country, may have undergone somewhat less significant breaches- with effects being felt mostly locally or within the limited sector but the rational for integration of cybersecurity policy in foreign policy does not emerge from present concerns, rather for the future with the inevitable digital transformation it is prepared to acquire by increasing connectivity and penetration rates, as well as increasing digital reliance through e-commerce and e-government.

What Nepal most lacks, besides a variety of economic and technological issues, are cybersecurity plans, policies, and a legal and regulatory framework. ETA, 2006 is neither focused on cyber security nor current in addressing the current problem of cybercrime and cybersecurity. In order to handle the problem and challenges of cybersecurity, Nepal urgently requires new cyber legislation and a distinct cybersecurity policy.

REFERENCES

Aaviksoo, J. (2010). Cyberattacks Against Estonia Raised Awareness of Cyberthreats. Defense Against Terrorism Review, 3(2), 13-22.

Access Now. (2022). POLICY BRIEF: Nine steps to protect our data and privacy in Sri Lanka.

Acharya, G. (2022, June 16). Tech Sovereignty: A Quest for Nepal. Retrieved September 2022, from My Republica: https://myrepublica.nagariknetwork.com/news/tech-sovereignty-a-quest-for-nepal/

Acharya, S., & Dahal, S. (2021). Security Threats and Legalities with Digitalization in Nepal. Research Nepal, 1-15.

Adamson, L. (2020). International Law and International Cyber Norms. In Governing Cyberspace: Behavior, Power and Diplomacy (pp. 19-43). London: Rowman & Littlefield.

ADB. (2007). Country Partnership Strategy-Maldives 2007-2011. Asian Development Bank.

Albrecht, J. P. (2016). Regaining Control and Sovereignty in the Digital Age. In C. Springer, In Enforcing Privacy (pp. 473-488).

Aljazeera. (2020, December 20). Julian Assange: What you need to know about the WikiLeaks founder. Retrieved from https://www.aljazeera.com/news/2020/12/20/julian-assange

Ankita Mukhopadhyay. (2020, March 9). Nepal's delicate balancing act between China and India. Retrieved September 2022, from The Kathmandu Post: https://www.dw.com/en/nepals-delicate-balancing-act-between-china-and-india/a-52693835

Armijo, S. R. (2014). Brazilian leadership and the global Internet. Retrieved from AULA Blog: https://aulablog.net/tag/digital-sovereignty/

Austin, G. (2016). Mapping and Evaluating China's Cyber Power. Lau China Institute Policy Paper Series, King's College London.

Ayanso, A., & Lertwachara, D. C. (2010). The digital divide: Global and regional ICT leaders and followers. Information Technology for Development, 4(16), 304-319.

Baker, E. (2014). A Model for the Impact of Cybersecurity Infrastructure on Economic Department of Defence. . Retrieved from Dictionary of Military and Associated Terms: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

Baniya, S. (2021). Bringing digital literacy to Nepal: exhibit showcases student work in international service. Retrieved September 2022, from Virginia Tech: https://lib.vt.edu/magazine/spring-2021/creativity-innovation/nepal.html#:~:text=Research%20showed%20that%20the%20digital,cybercrime%20because%20of%20the%20pandemic.

Basu, S., & Jones, R. (2003). E-commerce and the law: a review of India's Information Technology Act, 2000. Contemporary South Asia, 1(12), 7-24.

Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmid, J., & Weiss, J. (2012). Cyber security policy guidebook. John Wiley & Sons.

BBC. (2019). Ransomware hits Johannesburg electricity supply. Retrieved from Available at: https:// www.bbc.com/news/technology-49125853

Becker, C., & Nanni, N. T. (2022, July 19). The Standardisation of Lawful Interception Technologies in the 3GPP: Interrogating 5G and Surveillance Amid Us-China Competition. Retrieved 2022, from Interrogating 5g and Surveillance Amid Us-China Competition: https://deliverypdf.ssrn.com/delivery.php?ID=860065085009094103092097100003111073058016039023044067109085006111072004078005090025025031037030005038045126026006087102023002114023070069004116122120025068026096120067028060026087099005086117069077068103022093

Beer, J. (2018). “WannaCry” ransomware attack losses could reach $4 billion. Retrieved from CBS News: https://www.cbsnews.com/news/wannacry-ransomware- attacks-wannacry-virus-losses/

Begum, A. A. (2018). Cyber Security in South Asia: Validating Danger as Security. FORUM-ASIA's working paper on SDGs and Human Rights.

Ben, D., Hasan, S., Pal, J., Vallentin, M., Panjwani, S., & Brewer, P. G. (2011). Computing security in the developing world: A case for multidisciplinary research. Proceedings of the 5th ACM workshop on Networked systems for developing regions , (pp. 39-44).

Bennett, C. (2015, May 8). China Wants Cyber 'Sovereignty' in the latest National Security LAw. Retrieved from The Hill: http://thehill.com/policy/ cybersecurity/241420-china-wants-cyber-sovereignty-in-latest-national-security-law

Bloomberg. (2016, November 7). China Adopts Cybersecurity Law Despite Foreign Opposition. Retrieved from https://www.bloomberg.com/news/articles/2016-11-07/china-passes-cybersecurity-law-despite-strong-foreign-opposition

Brenner, J., & Lindsay, J. R. (n.d.). Correspondence: Debating the Chinese Cyber Threat. International Security, 1(40), 191-195.

Broeders, D., & Van Den Berg, B. (2020). Governing Cyberspace: Behavior, Power and Diplomacy. Rowman & Littlefield Publishers.

Budnitsky, S., & Jia, L. (2018). Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. European Journal of Cultural Studies, 1-19.

Bulathgama, T. (2021). Cyber Terrorism an Emerging Threat to Sri Lanka's National Security. Retrieved from Institute of National Studies: http://www.insssl.lk/ index.php?id=300

Businessmirror. (2022, July 27). Sri Lanka supplements synergies in ICT sector. Retrieved from https://businessmirror.com.ph/2022/07/27/sri-lanka-supplements synergies-in-ict-sector/

Center for Strategic and International Studies . (2022). Significant Cyber Incidents Since 2006. Retrieved from CSIS: https://csis-website-prod.s3.amazonaws.com/s3fs-public/220906_Significant_Cyber_ Incidents.pdf?OSKTnneXKCxI_Qx1Y7An4JGjm6DiTB0_

Central Bureau of Statistics. (2021). CBS- GDP 2021.

Chang, A. (2014). Warring State China's Cybersecurity Strategy.

Chen, Y. C., & Romanuik, T. T.-T. (2021). Serving the People: China's cybersecurity policy and its implications. In S. N. Eds Romaniuk, & a. M. Manjikian, Routledge Companion to Global Cyber Security Strategy (pp. 284-296). Routledge.

Chouchri, N., Madnick, S., & Ferwada, J. (96-121). Institutions for Cyber Security: International Responses and Global Imperatives. Information Technology for Development, 2013.

Choucri, N. (2012). Cyberpolitics in International Relations. MIT Press.

Choucri, N. (2019). International relations in the cyber age: The co-evolution dilemma. MIT Press.

Clement, J. O. (2013). Internet Surveillance and Boomerang Routing: A Call for Canadian Network Sovereignty. Rochester, NY: Social Science Research Network.

Collin, B. C. (1997). The future of cyberterrorism: Where the physical and virtual worlds converge. Crime and Justice International, 2(13), 15-18.

Corn, G. P., & Taylor, R. (2017, August 22). Sovereignty in the Age of Cyber. Retrieved 2022, from Cambridge University Press: https://www.cambridge.org/core/journals/american-journal-of-international-law/article/sovereignty-in-the-age-of-cyber/02314DFCFE00BC901C95FA6036F8CC70

Costello, J. (2016). The Strategic Support Force: China's Information Warefare Service. China Brief, 3(16), 15.

Creemers, R. (2020). China's Conception of Cyber Sovereignty. In Governing cyberspace: Behavior, power and diplomacy (pp. 107-145).

Cyber Bureau. (n.d.). Retrieved September 2022, from https://old.nepalpolice.gov.np/index.php/cyber-bureau#

Cyber Security Bill. (2018). Cyber Security Bill. Government of Sri Lanka.

Cyberspace Administration of China. (2016, December 27). Guojia wanglu kongjian anquan zhanlue" ("National Cyberspace Security Strategy. Retrieved from www.cac.gov.cn/2016-12/27/c_1120195926.html

Daskal, J. (2015). The un-territoriality of data. Yale Law Journal, 326-398.

Department of Information Technology. (2019). GEA. Retrieved from https://doit.gov.np/en/spage/gea

Dévai, D. (2019). The US Response to the 2016 Russian Election Meddling and the Evolving National Strategic Thought in Cyberspace (Part 2). Academic and Applied Research in Military and Public Management Science, 18(1), 59-77.

DeVore, M. R., & Lee, S. (n.d.). APT (advanced persistent threat) s and influence: Cyber weapons and the changing calculus of conflict. The Journal of EastAsian Affiars, 39-64.

Dhaka Tribune. (2018, March 15). Dhaka, Moscow Agree to Form Joint Working Group to Ensure Cyber Security. Retrieved from www.dhakatribune.com/technology/2018/03/15/dhaka-moscow-agree-form- joint-working-group-ensure-cyber-security

Dilipraj, E. (2015). South Asian Cyber Security Environment: An Analytical Perspective. Asian Defence Review 2012-2015, pp. 161-190.

Diplo. (2021). 2021: The emergence of digital foreign policy. Retrieved December 2021, from Diplomacy Education: https://www.diplomacy.edu/blog/the-emergence-of-digital-foreign-policy/

DoNP. (2018). Seventh National Development Plan 2006 -2010. Retrieved from Department of National Planning (Maldives): http://www.planning.gov.mn/ en/images /stories/ndp/seventh_ndp.pdf

Etribune. (2011). 36 government sites hacked by „Indian Cyber Army. The express Tribune.

Europol. (2018). IOCTA 2018. Retrieved from https://www.europol.europa.eu/ activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

Fernando, R. (2021). The Evolution of Cyber-Attacks in Sri Lanka. Retrieved from Millennium IT: https://www.mitesp.com/blog/the-evolution-of-cyber-attacks-in-sri-lanka/

Fourkas, V. (2004). What is 'Cyberspace'? WACC.

Fruhlinger, J. (2018, December 20). What is ransomware? 4 steps to prevent these file-locking attacks. Retrieved September 2022, from What is ransomware? 4 steps to prevent these file-locking attacks.

Gamreklidze, E. (2014). Cyber security in developing countries, a digital divide issue,. The Journal of International Communication, 2(20), 200-2017.

General Assembly, UN. (2018a). Developments in the Field of Information and Telecommunications in the context of International Security. A/RES/73/27.

General Assembly, UN. (2018b). Countering the Use of Information and Communications Technologies for Criminal Purposes. Edited by 3rd committee of United Nations.

Gilli, A. G. (2018). Why China has not caught up yet: military-technological superiority and the limits of imitation, reverse engineering, and cyber espionage. International Security, 3(43), 141-189.

Giri, S. (2019). Cyber Crime, Cyber threat, Cyber Security Strategies and Cyber Law in Nepal. Retrieved from https://www.academia.edu/40449593/Cyber_ Crime_Cyber_ threat_Cyber_Security_Strategies_and_Cyber_Law_in_Nepal

Global Commission on the Stability of Cyberspace. (2018, May). CALL TO PROTECT THE ELECTORAL INFRASTRUCTURE. Retrieved from https://cyberstability.org/wp-content/uploads/2018/05/GCSC-Call-to-Protect-Electoral-Infrastructure.pdf

Google Inc. (2021). Government Detailed Removal Request. Google. Inc.

Government of Nepal Ministry of Home Affairs. (2020). Press Release.

Government of Nepal. (2019). Digital Nepal Framework. Retrieved from https://mocit.gov.np/application/resources/admin/uploads/source/EConsultation/EN%20Digital%20Nepal%20Framework%20V8.4%2015%20July%20%202019.pdf

Grigsby, A. (2017). The end of cber norms. Survival, 59(6), 109-122.

Halder, D. (2011). Information Technology Act and cyber terrorism: A critical review. In Cyber Crime and Digital Disorder (pp. 75-90). Available at SSRN 1964261.

Halder, D., & Jaishankar, K. (2008). Cyber crimes against women in India: Problems, perspectives and solutions. TMC Academic Journal, 3(1), 48-62.

Halder, D., & Jaishankar, K. (2021). Cyber Governance and Data Protection in India: A critical legal analysis. In Routledge Companion to Global Cyber-Security Strategy (pp. 339-348). London: Routledge.

Hall, R. B., & Biersteker, T. J. (2002). The emergence of private authority in global governance. Cambridge University Press, 85. Retrieved from https://www.researchgate.net/profile/Thomas-Biersteker/publication/236219118_The_Emergence_of_Private_Authority_in_Global_Governance/links/5fd1e4ca92851c00f8626d17/The-Emergence-of-Private-Authority-in-Global-Governance.pdf

Hanna, N. K. (2017). How can developing countries make the most of the digital revolution? Retrieved June 2020, from World Bank Blogs:

https://blogs.worldbank.org/digital-development/how-can-developing-countries-make-most-digital-revolution

Hern, A. (2017, Dec 30). WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017. Retrieved from The Gurdian News Website: https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware

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

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

ICT4Peace Foundation. (2018). ICT4Peace published Commentary on Voluntary Non-Binding Norms of Responsible State Behaviour in Cyberspace. Retrieved from ICT For Peace Foundation: https://ict4peace.org/activities/ict4peace-sponsored-first-global-commentary-on-norms-of-responsible-state-behaviour-in-cyberspace/

India Today. (2017, July 12). Cabinet Informed about India, Bangladesh Cyber Security Pact. Retrieved from www.indiatoday.in/pti-feed/story/cabinet-informed-about-india-bangladesh-cyber-security-pact-996683- 2017-07-12

Iqbal, Z. (2021). Cyber Threats to Pakistan's Digital Landscape. Retrieved from https://sdpi.org/spdiweb/publications/files/SDC-Anthilogy-2020.pdf

Islam, M. (2013, June 2). Cyber Security: It Merits Serious Attention. Retrieved from The Financial Express: www.thefinancialexpress-bd.com/old/index.php?ref=MjBfMDZfMDJfMTNfMV8yN18xNzEzNjg

Islam, M. S. (2021). CYBERSECURITY A national priority for Bangladesh. In Routledge Companion to Global Cyber-Security Strategy (pp. 349-355).

Islam, z., Khan, M., & Zubair, M. (2019). Cybercrime and Pakistan. Global Politics Review, 2(4).

ITU. (2009). Making an IMPACT on global cybersecurity. Retrieved from https://www.itu.int/net/itunews/issues/2009/08/22.aspx

ITU. (2010). Regional Forum on Digital Inclusion includes the countries: Afganistan, Bangladesh, Bhutan, Maldives and Nepal (ABBMN). Retrieved from https://www.ict.gov.ir/fa/news/4959/ITU-Regional-Forum-on-Digital-Inclusion-boosts-regional-cooperation-Ministers-of-Afghanistan-Bangladesh-Bhutan-Maldives-and-Nepal-commit-to-increased-regional-cooperation

ITU. (2012). Readiness Assessment for Establishing a National CIRT (Afghanistan, Bangladesh, Bhutan, Maldives and Nepal), ITU/IMPACT.

ITU. (2014). Cyber Wellness Profile- Afganistan. Retrieved from https://nanopdf.com/download/cyberwellness-profile-afghanistan_pdf

ITU. (2018, December 7). ITU releases 2018 global and regional ICT estimates. Retrieved from Available at: https://www.itu.int/en/mediacentre/Pages/2018-PR40.aspx

Jamal E. M, M. M. (2016, October 29). Digital Security Act, 2016. Retrieved from The Daily Star: www.thedailystar.net/opinion/interviews/how-does-it-affect-freedom-expression-and-the-right-dis sent-1305826

Johnson, D., & Post, D. (1996). Law and Borders: The rise of law in cyberspace. Stanford law review, 1367-1402.

Kalyar, J. (2019, December 22). Cyber Insecurity. Retrieved from The News: http://www/thenews.com.pk/tns/detail/586618-cyber-insecurity

Kello, L. (2019). The virtual weapon and international order. Yale University Press.

Kemph, S. (2020). Digital 2020. DataReportal- Global Digital Insights. https://dataportal.com/reports/digital-2020-pakistan.

Khan, U. P. (2021). Cybersecurity in Pakistan: Regulations, Gaps and way Forward. Cyberpolitik Journal, 206-2018.

Klimburg, A. (2018). The darkening web: The war for cyberspace. Penguin.

Klimburg, A., & Faesen, L. (2020). A Balance of Power in Cyberspace. In Governing Cyberspace: Behavior,Powe and Diplomacy (pp. 145-171). London: Rowman & Littlefield.

Koong, K., & Yunis, M. (2015). A Conceptual Model for the Development of a National Cybersecurity Index: An Integrated Framework.

Kowalewski, A. (2017). China's Evolving Cybersecurity. Georgetown Security Studies Review.

Kshetri, N. (2010). Diffusion and Effects of Cyber-Crime in Developing Economies. Third World Quarterly, 31(7), pp. 1057-1079.

Kumar, R. (2018). Security threats to E-business among SAARC Nations – A Preliminary Study. International Journal of Engineering Research in Computer Science and Engineering (IJERCSE), 5(4), 5-7.

Kurowska, X. (2020). What does Russia Want in Cyber Dilomacy. In Governing Cyberspace: Behavior, Power, and Diplomacy (pp. 85-106). London: Rowman and Littlefield.

Lewis, D. P. (2021, July 20). Pegasus Project: Edward Snowden Calls For a Global Moratorium on Spyware Trade. Retrieved from The Wire: https://thewire.in/world/pegasus-project-edward-snowden-spyware-trade

Libicki, M. (2009). Cyberdetterrence and Cyberwar. Rand Corporation.

Libicki, M. C. (2007). National Security and Information Warfare. Cambridge.

Live Cyber Threat Map. (2022, Sep 1). Retrieved Sep 1, 2022, from https://threatmap.checkpoint.com

Maharjan, R. (2019). Framework for Minimizing Cyber Security Issues in Banking Sector of Nepal. LBEF Research Journal of Science, Technology and Management, 1(1), 82-98.

Manjikian, M. (2020). Cyber Politics and Policies. Washingto DC: CQ press.

Manjikian, M. (2021). The United States : A declining hegemon in Cyberspace? In N. S. Romaniuk, & M. (. Manjikian, Routledge Companion to Global Cyber-Security Strategy (pp. 463-472). Routledge.

Manjikian, M. M. (2010). From global village to virtual battlespace: The colonizing of the Internet and the extension of Realpolitik. International Studies Quarterly, 381-401.

Maurer, T., & Morgus, I. S. (2015). Technological sovereignty: missing the point? 7th international conference on Cyber conflict: Architectures in cyberspace (CyCon), (pp. 53-68).

Ministry of Defense. (2016). National Security Policy. Retrieved from mop.gov.np: http://mod.gov.np//public/files/231574029-National%20Security%20Policy,%202016.pdf

Ministry of Foreign Affairs. (2020). Report on Nepal's Foreign Affairs (2019-2020). Retrieved from https://mofa.gov.np/wp-content/uploads/2020/12/Report-on-Nepals-Foreign-Affairs_MOFA_2019-2020.pdf

Ministry of Posts, Telecommmunication and Information Technology. (2014). National Cyber Security Strategy. Retrieved from Government of Bangladesh: www.dpp.gov.bd/upload_file/gazettes/10041_41196. pdf

MOCIT. (2019). 2019 Digital Nepal Framework: Unlocking Nepal's Growth Potential. Retrieved from https://mocit.gov.np/application/resources/admin/uploads/source/EConsultation/EN%20Digital%20Nepal%20Framework%20V8.4%2015%20July%20%202019.pdf

Moorthy, S. (2022, April 07). Sri Lanka crisis unlikely to have significant impact on IT operations, say experts. Retrieved from Money Control:

https://www.moneycontrol.com/news/business/sri-lanka-crisis-unlikely-to-have-significant-impact-on-it-operations-say-experts-8325741.html

My republica. (2017, July 24). Nepal vulnerable to cyber attacks. Retrieved from https://myrepublica.nagariknetwork.com/mycity/news/nepal-vulnerable-to-cyber-attacks

Nadira, F. (2018). Makara heelathun faisa hoadumuge massalathah raiiyithun mihaarah vure bodah heyluntherive samalukan dheynjehey. [The Public should be more aware and cautious of cases of acquiring money through fraud and deception]. Retrieved from http://www.policelife.mv/page/132679

Nakashima, E. (2019). The U.S is urging a o vote on a Russian-led U.N Resolution calling for a Global Cybercrime Treaty. Retrieved from The Washington Post: https://www.washingtonpost.com/national-security/the -us-is-urging-a-no-vote-on-a-russian-led-un-resolution-calling-for-a-global-cybercrime-treaty/2019/11/16/ b4895e76-075e-11es-818c-fcc65139e8c2_story.html?wpisrc=ni_cybersecurity202 &wpmm=1

National Judicial Academy. (2022). A Study on Cyber Crime Cases in Nepal: Challenges and Recommendations 2022. Kathmandu: National Judicial Academy.

National People's Congress. (2015, July 7). National Security Law of the People's Republic of China. Retrieved from www.npc.gov.cn/npc/xinwen/2015-07/07/content_1941161.htm

National Security Policy 2016. (2016). Retrieved May 2020, from https://kms.pri.gov.np/dams/pages/download_progress.php?ref=2105&size=&ext=pdf&k=e763966226

NATO. (2012, June 01). Cyber Defence Training for Afghan Professionals. Retrieved from https://www.nato.int/cps/en/natolive/news_88116.htm?selectedLocale=en

Nepal CERT. (2019). About Nepal CERT. Retrieved september 2022, from Nepal CERT: https://www.nepalcert.org.np/

Nepal GEA 2.0. (2019, September). Nepal GEA 2.0 Security Architecture,Final September 2019. Retrieved September 2022, from https://doit.gov.np/ckfinder/userfiles/files/Guidelines/Nepal%20GEA%202_0%20Security%20Architecture.pdf

Nepal in Data. (2018, May 13). Retrieved from MAJOR LANGUAGES SPOKEN AS MOTHER TONGUE IN NEPAL: https://nepalindata.com/insight/major-languages-spoken-as-mother-tongue-in-nepal/

Nepali Telecom. (2022, May 4). Digital Nepal Framework Gets 22 Billion Investment. Retrieved from https://www.nepalitelecom.com/2022/05/digital-nepal-framework-gets-22-billion-investment.html

NITC. (n.d.). Government Integreted Data Center. Retrieved September 2022, from National Information Center: https://nitc.gov.np/

Nocetti, J. (2015). Contest and Conquest: Russia and global internet governance. International Affairs, 1(91), 111-130.

NTA. (2020). Cyber Security Byelaw, 2077 (2020). Retrieved from https://www.nepalkhoj.com/wp-content/uploads/2020/08/Cyber-Security-Bylaw-2077-2020.pdf

Nye, J. (2014). The regime complex for managing global cyber activities. USA: Belfer Center for science and International Affairs. John F. Kennedy School of Government, Harverd University.

Obar, A. C. (2015). Canadian internet “boomerang” traffic and mass NSA surveillance: Responding to privacy and network sovereignty challenges. In Law, privacy and surveillance in Canada in the post-Snowden era (pp. 13-44).

Ohlin, J. D. (2018). Election Interference: The Real Harm and the only Solution. Cornell Law School Research Paper, 1-26.

Pavan, K. (2016). An Empirical Study of the Effects of Demonetization in India in the Year 2016 and Analyzing Shifting Trends in Marketing/Purchasing to the

Alternative Options. Journal of Engineering and Information Technology, 3(6), 2394-8124.

Pingman, L. (2019). Russia's Vision of Cyberspace: A Danger to Regime Security, Public Safety and Societal Norms and Cohesion. Journal of Cyber Policy, 4(1), 22-34.

PTI. (2010). CBI Website Hacked by 'Pakistani Cyber Army. Retrieved from Times of India: http://timesofindia.indiatimes.com/articleshow/7038524.cms?utm_source= contentofinterest&utm_medium=text&utm_campaign=cppst

Pudasaini, S. (2022, January 11). Addressing Nepal's digital divide. Retrieved september 2022, from nepalitimes: https://www.nepalitimes.com/opinion/addressing-nepals-digital-divide/

Qadeer, A. (2020). The Cyber Threat Facing Pakistan. Retrieved from https://thediplomat.com/2020/06/thecyber-threat-pakistan/

Raud, M. (2016). China and Cyber: Attitudes, Strategies, Organisation. Tallinn, Estonia: NATO CCDCOE.

Rayome, A. D. (2017, July 6). UN report: 50% of countries have no cybersecurity strategy in place. TechRepublic.

Riotta, C. (2019, October 9). Russia Used Social Media to Support Trump in 2016 at Direction at Kremlin, Senate Intelligence Report Says. Retrieved from Independent: www.independent.co.uk/news/world/americas/us-politics/trump-russia-2016-intelligence-report-read-kremlin-facebook-a9148036.html

Roka, C. B. (2017). CYBERCRIME AND SECURITY IN NEPAL: THE NEED FOR TWO-FACTOR AUTHENTICATION IN SOCIAL MEDIA. Crossing the Border: International Journal of Interdisciplinary Studies, 5(2), 31-36.

Rollins, J. W. (2015, October 16). U.S.–China Cyber Agreement. Retrieved 2022, from https://sgp.fas.org/crs/row/IN10376.pdf

Romaniuk, S. N., & Manjikian, M. (2021). Routledge companion to global cyber-security strategy. Routledge.

Sarkar, S. (2021, September). Indo-Nepal Cyber Diplomacy and Regime Formation. Political Reflection, 7(3), pp. 23-30.

Schia, N. (2017, December 11). The cyber frontier and digital pitfalls in the Global South. Third World Quarterly, 39(5).

SCIO. (2010, June 8). The Internet in China (White Paper). Retrieved from http://www.chinadaily.com.con/china/2010-06/08/content_9950198.htm

Security-Risks.com. (2014, August 31). A Cyber Unit to Specialise in Cyber Crime. Retrieved from http:// www.security-risks.com/security-issues-south-asia/iw-cyber-security/bhutan-cyber-unit-to- specialise-in-cyber-crime-3388.html

Segal, A. (2018). When China Rules the Web: Technology in Service of the State. Foreign Aff., 10.

Senate of Pakistan. (2013). Report of the Senate Committee on Defence and Defence Production. Retrieved from https://www.senate.gov.pk/uploads/documents/ 1378101374_113.pdf

Shackelford, S. J. (2010). 'Estonia three years later: A progress report on combating cyber attacks', Journal of Internet Law. INTERNET L, 8(13), 22-22.

Shaik, A., Seifert, J., Borgaonkar, R., & Niemi, N. A. (2016). Practical Attacks against Privacy and Availability in 4G/LTE Mobile Communication Systems. In Proceedings of the 23nd Annual Network and Distributed System Security Symposium (NDSS 2016).

Shairgoji, A. A. (2022). Emerging Cyber Security India's Concern and Threats. Journal of Technology Innovations and Energy.

Shareef, M. (2010). Electronic Governance in the Maldives: Status, Issues and Plans .

Sharikov, P. (2020). Alternative Approaches to Information- Age Dilemmas Drive US and Russian Arguments about Interference in Domestic Political Affairs. U.Maryland: Center for International & Security Studies.

Sharikov, P., & Stepanova, N. (2019). Russia's approaches to information policy. Sovremennaya Evropa 2, 73-83.

Sharma, A. (2016). Information Communication Technology Development in Nepal. JRSD, 101-141.

SLCERT. (2019). About us. Retrieved from SLCERT: http://www.slcert.gov.lk/aboutUs.php.

Smith , B. (2018, Apr 17). 34 companies stand up for cybersecurity with a tech accord. Retrieved from Microsoft on the Issues: https://blogs.microsoft.com/on-the-issues/2018/04/17/34-companies-stand-up-for-cybersecurity-with-a-tech-accord/

Smith, B. (2017, Feb 14). The need for a Digital Geneva Convention. Retrieved from Microsoft on the Issues: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

Sridharan, V. (2016, August 11). Pakistan passes 'draconian' cybercrime law threatening civil liberties. . Retrieved from International Business Times: https://www.ibtimes.co.uk/pakistan-passes-draconian-cybercrime-law-threatning-civil-liberties-1575530#

Stadnik, I. (2021). The Russian approach to cyber- sovereignty. In Routledge Companion to Global Cyber-Security Strategy (pp. 153-164). Routledge.

Suman, D. (2021). Security Threat Analysis and Prevention towards Attack Strategies. In Cyber Defense Mechanisms. CRC Press.

Świątkowska, D. J. (2020). Tackling cybercrime to unleash developing countries' digital potential. Pathways for Prosperity Commission.

The Daily Star. (2016, March 15). $101m Heist: Atiur Quits as Governor of Bangladesh Bank. Retrieved from www. thedailystar.net/business/101m-heist-bb-governor-ready-quit-791542

The HRM. (2022, July 31). Human Resources Crunch Engulfs Nepali IT Sector. Retrieved September 2022, from https://www.thehrmnepal.com/report/human-resources-crunch-engulfs-nepali-it-sector/

The Kathmandu Post. (2018, January 20). Nepal added over 250 internet users per hour. Retrieved September 2022, from https://kathmandupost.com/money/ 2018/01/20/nepal-added-over-250-internet-users-per-hour

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

The Rising Nepal. (2020, Jan 06). National Security Policy Updated As Per Political Context. Retrieved from https://old.risingnepaldaily.com/interview/national-security-policy-updated-as-per-political-context

The State Council of the People's Republic of China. (2014, August 25). Ministry of Public Security. Retrieved from english.www.gov.cn/state_council/ 2014/09/09/ content_281474986284154.html

The Times of India. (2019). Red alerts issued on cyber threat from China. Retrieved from http://timesofindia.indiatimes.com/india/Red-alert-issued-on-cyber-threats-from- China/articleshow/52720087.cms

Thimpu Tech Park. (2021). About Us. Retrieved from Thimpu Tech Park: http://www.thimphutechpark.com/about

Tikk, E., Kardi Kaska, & Liss Vihul. (2010). International Cyber Incidents Legal Considerations. Tallin: NATO CCD COE, (pp. 14-35).

Toupin, S. C. (2019). What does the notion of “sovereignty” mean when referring to the digital? New media & Society, 1-16.

Tsagourias, N. (2020). Electroal Cyber Interference, Self- Determination, and the Principle of Non- intervention in Cyberspace. In Governing Cyberspace: Behavior, power and Diplomacy (pp. 45-63). Rowman & Littlefield.

U.S senate. (2014, July 15). “Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks.”. Retrieved from Committee on the Judiciary, Subcommittee on Crime and Terrorism.: www.judiciary.senate.gov/meetings/taking-down-botnets_public-and-private-efforts- to-disrupt-and-dismantle-cybercriminal-networks

UN GGE. (2021). Group of Governmental Experts. Retrieved from United Nations Office for Diarmament Affairs: https://www.un.org/disarmament/group-of-governmental-experts/

UN Open- Ended Working Group. (2020). Open- Ended Working Group. Retrieved from UN Open- Ended Working Group: https://www.un.org/disarmament/open-ended-working-group/

UNGA. (1999). Developments in the field of Information and Telecommunications in the context of Internationsl Security. A/RES/53/70.

United Nations. (2021). Nepal after LDC Graduation: New avenues for exports. Retrieved September 2022, from https://www.un.org/ohrlls/content/nepal-after-ldc-graduation-new-avenues-exports#:~:text=Nepal's%20Road%20to%20Graduation ,by%20the%20end%20of%202026.

Verizon. (2018). Data Breach Investigations Report.

Waheeda, F. (2015). Legislating for Cybercrimes in the Maldives: Challenges and Prospects. Maldives National University, 415-438.

Waheeda, F. (2018). Prosecuting Modern Identity theft: A Comparative Analysis. Contemporary and Emerging Issues in Syariah and Law. Uinversiti Sains Islam Malaysia (USIM) Press.

Weber, A. K. (2018). What can Russia teach us about change? Status-seeking as a catalyst for transformation in international politics. International Studies Review, 20(2), 2092-300.

World Bank (a). (2020). Individuals using the Internet (% of population) - Nepal. Retrieved September 2022, from https://data.worldbank.org/indicator/ IT.NET.USER .ZS?locations=NP

World Bank. (2019). NEPAL INFRASTRUCTURE SECTOR ASSESSMENT. World Bank Group.

World Bank. (2019). World Bank Country and Lending Groups. Retrieved from Available at: https:// datahelpdesk.worldbank.org/knowledgebase/articles/ 906519

Yannakogeorgos, P. A. (2012). Internet governance and national security. Strategic Studies Quarterly, 102-125.

Youtech Nepal. (2020, June 1). Nepal Budget 2077/78 on ICT Sector; what to expect? Retrieved September 2022, from https://youtechnepal.com/nepal-budget-on-ict-sector/

Zalif, Z. (2020, November 5). Enhancing response cpacity of law enforcement agencies is pivotal to protect human rights. Retrieved from Raajje: https://raajje.mv/89987

Zapoeozhets, O., & Syvak, O. (2020). I the Line of Russian Ukraine, Hybrid Warfare, and Cybersecurity Defense Aggression. In Routledge Companion to Global Cyber-Security Strategies (pp. 185-190). Routledge.

Zeng, J. (2017). Does Europe Matter? the Role of Europe in Chinese Narratives of ‘One Belt, One Road’ and 'new type of great power relations'. JCMS: Journal of Common Market Studies, 1162-1176.

Zhou, Z. (2015, December). China's Draft Cybersecurity Law. Retrieved from China Breif: https://jamestown.org/program/chinas-draft-cybersecurity-law/ [Original source: https://studycrumb.com/alphabetizer]