Pakistan Journal of Humanities & Social Sciences Research
Volume No. 05, Issue No. 01 (June, 2022)

ISSN (P): 2663-9211 (E): 2663-922X
DOI:https://doi.org/10.37605/pjhssr.v5i1.381

Date of Submission: 5th January, 2022
Date of Acceptance: 19th April, 2022
Date of Publication: June, 2022

CYBER SECURITY THREAT AND PAKISTAN'S PREPAREDNESS: AN ANALYSIS OF NATIONAL CYBER SECURITY POLICY 2021

Sara Ahmad[*]

Abstract

The objective of this research is to evaluate Pakistan's existing national cyber security policy in order to understand its context, effectiveness and readiness to deter cyber security challenges. As the world has become intensively connected and digitized through the internet or information technology, securing cyber space has become the biggest challenge, and has exposed the world to the existence of a novel, global threat. Since the threat to cyber security has no geographical boundaries and is beyond the traditional understanding of security, it is considered to be a paradigm shift in the area of security. The seriousness and enormity attached to cyber threats intrigued us into investigating the status of Pakistan in securing its cyber space and to analyse the National Cyber Security Policy (NCSP) that was developed by the government of Pakistan in 2021 to combat cyber threats from within and outside the country. Cyber security threats and Pakistan's preparedness for them have also been analyzed in this research. This qualitative study intends to employ a qualitative technique for the collection of data, i.e., policy documentary analysis, to investigate the nature of cyber security policy.

Keywords: Cyber, Preparedness, Policy, Threat, Security

[*] Lecturer at Department of Politics and International Relations, Lahore Leads University, Lahore, Pakistan. saraahmad5161@gmail.com

Introduction

The sharing of cyber space has exposed the world to a new kind of threat that exists beyond boundaries. The Internet is a globally connected, borderless network that enables cyber attackers to harm all countries using a computer system that has poor cyber security. Internet communication and technologies are beneficial and bring transformations in different fields such as healthcare, education, business, defence etc. Cyber criminals have realized the potential of the Internet for illegal purposes. The growth of information and communication technologies (ICT) has been unprecedented during the past few decades (Awan & Memon, 2016).

Since the Covid-19 outbreak, digital transformation has become a catalyst and people have relied on the internet more than ever before to mitigate the effect of social distancing. Cyber security has become imperative to safeguard the digital infrastructure and devices connected to the internet (Council of Europe, 2020). Hence, technology has become an essential element of national power, but in recent decades it has increased the national security risk for all states. In the contemporary world, the threat spectrum has been revolutionized, due to the reliance of states on cyber space or digitally connected computer networks (Safdar, 2020). It is estimated that there are over 21 million internet of things, which is likely to double by the end of 2025 (ACS, 2016). With the emerging use of the internet and its easy availability, cyber space is escalating, making it easier for hackers to target infrastructures and services. Due to the over-dependency of the world on the internet and advanced technology, the threat of cyber security being broken through increases enormously and holds the probability of executing serious damage (Syed, Khaver & Yasin, 2019).

According to the Statista Global Survey (2020), 4.66 billion people are regular users of the internet around the world, which is nearly 59 per cent of the global population. Approximately one million more people join the internet daily, and by 2030 it is anticipated that there will be more than 7.5 billion users of the internet (Morgan, 2020). From Pakistan's perspective, due to the undergoing digital transformation of all its services, communication in both the government and the private sector is based on the internet shifting from a conventional infrastructure to a digitized system, and thus being vulnerable to cyber attacks. Pakistan is among the five developing countries where usage of the internet is increasing day by day, with growing frequency (Naiyer, 2020).

According to the World Economic Forum's Global Risk Report (2020), cyber security is placed in the second position in terms of the prospect of manifestation and impacts, just behind natural disasters. The world economic powers of Russia, China and America are also vulnerable to cyber threats, where billions of dollars are at risk when cyber security is not handled properly (Hassan, 2018). It is predicted that globally, cyber crime damaged

$6 trillion in 2021, which is equal to the third largest economy next to the US and China, which increases by 15% every year; in 2025 it will reach $10.5 trillion (Morgan, 2020). A Frost & Sullivan and Microsoft study (2018) demonstrated that due to a cyber security breach, the Asia Pacific economy has lost $1.745 trillion. According to the World Economic Forum's global report (2020), a cyber attack on critical infrastructure was the first highest risk in the year 2020. The number of cyber attacks increased by 300% in the first half of 2019. Half a million attack attempts have been seen in cyber space every minute (ACS, 2016).

The report of the International Institute of Strategic Studies (2021) highlights that the US has been developing its civil sector cyber security policy since the mid-1990s. Initially, the focus of the policy was to counter cyber crimes and prevent losses to the corporate sector. A large number of executive orders were followed, including policy statements, action plans and other decisions. For the last three decades, a sharp concern has been seen to protect the information infrastructure of the country. Similarly, the first cyber security policy in the UK was introduced in 2008, which underlined cyber defence as a high-priority national security issue, while the first National Cyber Security Strategy was shaped in 2009, and updated in 2011 and 2016. These policies focused on cyber security and defence, and clearly illustrated the development of offensive capabilities. China introduced its first cyber security strategy in 2016, reflecting China's intention of becoming a cyber power, having ambitious goals, and relying on indigenous manufacturing internet technologies and having the vision to become a world leader in technologies by 2030. India's first National Cyber Security Policy was released in 2013 by the Ministry of Communications and Information Technology, aiming to protect the citizens, businesses and government from cyber attacks, either by state or non-state actors.

Pakistan is a newly emerging country in the cyber world, and therefore it is significant to understand its contribution and the stage where Pakistan exists in the cyber world. Pakistan also introduced its first National Cyber Security Policy in 2021, which is along the lines of other nations such as the US, Russia, the UK, France and China. They all have an offensive element regarding deterrence, and have linked their cyber policies with national security policies. The objective of this research is to evaluate the existing national cyber security policy of Pakistan to understand its context, effectiveness and readiness to deter cyber security challenges.

Literature Review

Cyberspace is created by human to facilitate communication and to connect the worldwide inter-connected infrastructure. It made possible for more than half of the world's population to interchange the data through a networked system. The emerging threat in cyberspace brought new challenges for societies around the world that have the potential to undermine the security of the people (Hussain, 2022). In the late 1980s the debate on cyber threats originated, and later in the 1990s gained momentum and spread to other countries. The cyber threat was catapulted in the mid-1990s on the political agenda by many countries when national security and industrialized economy rely on a national and international interdependent software system for a reliable and smooth process. In this way, cyber threats became intimidation for the societal values, the economic and well-being of the people. It was further established to carry out cyber attacks by a computer connected to the internet. This new enemy was neither identified nor associated with the particular state. Hacking tools are user friendly and sophisticated and can easily be downloaded. This threat framework links to the critical infrastructure turning the small incidents into high security issues (Cavelty, 2010).

The terms 'internet' and 'cyberspace' tend to use interchangeably, though the internet is one of the components of cyberspace while cyberspace includes far more than the internet (Cavelty, 2015). The internet has converted the world into a "virtual global village" (Yamin, 2014). In its basic sense, 'Cyberspace' means "communication through an electronic medium, for instance, website and email involve the command and control of computers" (Futter, 2016). Over the years various definitions of cyberspace have evolved but a common definition is not available, and the ones that are used are missing some components (Lorents & Ottis, 2010). Lorents and Ottis (2010) proposed a comprehensive definition as, "*cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems*."

Cyberspace is a new entity and no one can imagine life without it. States, groups, individuals, businesses and organizations are the actors in cyberspace that compete to control it. It has led to conflict in cyberspace. Cyber conflict is a confrontation in cyberspace between two or more than two groups or individuals where one group initiates a cyber-attack on another. The nature of cyber conflict depends on the goals of participants such as getting secret information, illegal revenue, and destroy the critical infrastructure of an enemy in a short period (Lorents & Ottis, 2010).

Since the dependence of the country's critical infrastructure on cyberspace has increased, the vulnerabilities that it has created demand the immediate attention of the people at the helm of the affairs as if left unchecked it could undermine the sovereignty of Pakistan (Khan, 2019; Shad, 2017). Cyber crimes and cyber security threats are increasing day by day. Cyber crimes such as harassment, financial fraud, fake profiles, hacking, defamation and blackmailing have sharply increased at social platform in Pakistan from last three years. Cases of harassment are being consider the second highest type of cyber crime in Pakistan. Most frequent use of media for cyber crimes in our country are Facebook, email and WhatsApp (Abbasi, 2021).

However, developing and particularly developed countries are extensively dependent on cyberspace for e-services to make the life of their people convenient but some vulnerabilities or cyber threats also exist (Sharma, 2010), such as a transfer of money from a bank account is vulnerable because the cyber thief does not use a gun for robbery rather use computer code and weak password to drop your bank balance to zero. Similarly, enemy hackers can hack or manipulate militarily sensitive information. The state secrets are stolen and critical public infrastructure is hacked but also affect the individuals because almost every individual use cyberspace or the internet for their communication. These are the unconventional cyber security attacks that cannot be fixed in the traditional or conventional security issues (Harknett & Stever, 2011).

In the cyber security realm, billions of dollars are illegally transferred or stolen, privacies exposed, state secrets acquired and critical public infrastructure hacked (Syed, Khaver & Yasin, 2019). Pakistan is no exception in this case and also face cyber threats and challenges such as hacking, serious and organised cyber crime, cyber terrorism, cyber warfare, (Shad, 2017) computer malware, identity theft, economic data theft, cyber frauds and espionage attempts on critical infrastructures, (Rafiq, 2017) ransom-ware, spyware, social engineering, and even alterations to physical devices, (Syed, Khaver & Yasin, 2019) malware, web application attacks, zero-day attacks, mobile device malware, and malicious insiders and phishing (Awan, Memon, Shah, Awan, 2016) and in the domain of cyber warfare Unregulated Cyber-Space (Cyber Terrorism, Cyber Propaganda, Cyber Harassment, Lack of Awareness of Public), Economic Disruptions (Cyber-Theft, Crypto Currencies, Ransomware), Cyber-Physical Attacks (Data Breaches, Sabotage, Relying on Foreign Equipments) are the cyber threats (Khan, 2019).

Incorrect media framing of cyber security initiatives, the absence of relevant institutions, wide scope security debates, traditional security culture and non-inclusion of the audience are the major challenges to the successful securitisation of cyberspace in Pakistan (Rafiq, 2017). Some e-government services are also facing various challenges like access issues, technical issues, human factors, service delivery issues (Awan, Memon, Shah, & Awan, 2016). Tariq, Aslam, Rashid, and Waqar, (2013) proposed a top-level organizational structure for the establishment of essential cyber security bodies at different tiers, responsible for securing cyberspace of the country such as the National Cyber Security Division will establish in PM Secretariat and responsible to formulating cyber security strategy, policy and legislation, Computer Emergency Response Team under the Ministry of Information Technology, to serve its constituency which comprises of a number of ICT related organizations, under the Ministry of Defence, Computer Emergency Response Team is proposed to deal with cyber threat their analysis and response, National Response Centre on Cyber Crimes is already working but it should enhance its effectiveness. All the scholars are agreed on this point that cyber securitisation remains unrealised and not protected which can undermine the individual and national security of Pakistan. Existing cyber security laws are ineffective and lack of implementation on them (Khan, 2019; Shad, 2017). Hence, Pakistan not only requires realization of cyber threats and consequences of its unchecked usage but also needs appropriate response mechanism to guard against such threats (Tariq, Aslam, Rashid & Waqar, 2013). After reviewing the existing literature on cyber security in Pakistan, it has found that recently introduced cyber security policy demands a comprehensive analysis. This research fill the gap by analyzing all the aspects of cyber security policy.

Method and Procedure

This qualitative study intends to employ a qualitative technique for the collection of data, i.e., policy documentary analysis. Since this study examines the cyber security policy of Pakistan, its data rely on primary and secondary sources. Primary data has been collected from the policy document and reports, while secondary data is taken from newspaper articles and published research papers. Documentary analysis (Bowen, 2009) is used for systematically reviewing or evaluating primary documents, such as government policies and reports, to gain an understanding of the existing policy framework. The kind of documentary analysis method employed in this research is centred on the cyber security policy document, which requires an understanding of the nature and purpose of the policy in order to attempt scrutiny and analysis. As a qualitative research method, a policy document is an easily accessible and cost-effective way to analyse data (Cardno, 2018).

Pakistan's Preparedness: Institutional and Legislative Framework for Cyber Security

Pakistan, however, is not oblivious to this imminent threat and has established different institutional frameworks such as the Pakistan Computer Emergency Response Team (Pak CERT), the Pakistan Information Security Association, and the Computer Emergency Response Team (PISA-CERT). CERTs (Computer Emergency Readiness Team) and CSIRTs (Computer Security Incident Response Team) were created globally in the public and private sectors to respond to cyber threat and for cyber security. These teams handle cyber security within organizations, and they sometimes have national responsibilities. Both respond to cyber security issues, but are technically distinct. CERT is a trademark term and is associated with the threat to intelligence, consisting of experts in information security who detect, protect, prevent and respond to cyber security incidents, while CSIRT is a cross-functional organization that provides legal and technical responses. CERT focuses on any national cyber security threats that impact critical infrastructure, economy, national security and the denial of service attacks

(Tagert, 2010). In addition, the Senate Defense Committee has set up a ‘Pakistan Research Centre’ under the Cyber Security Task Force, to secure its cyber space. In May 2018, Pakistan also launched the first-ever National Centre of Cyber Security (NCCS) at Air University, Islamabad (Shad, 2017). The Federal Investigation Agency (FIA) set up a National Response Centre for Cyber Crime in 2007 to deal with technological abuse in Pakistan, providing the services of computers, videos, mobiles, network forensics and technical training (NR3C, 2007). NR3C works under the PECA 2016, and does not have much capacity to prevent cyber crimes and cyber offenses, while PECA does not cover the strategic aspects of cyber security and is not yet properly implemented (Nabeel, 2018).

The passage of legislation on ‘The Electronic Transaction Ordinance 2002 (ETO, 2002), the Prevention of Electronic Crimes Bill, 2015’, and the draft of the National Cyber Security Policy, 2021, approved by the cabinet, also show commitment and seriousness on the part of the government. Despite all these efforts, it is argued that Pakistan still needs an official cyber security framework and an integrated institutional system, as well as the capacity for the implementation of laws to enforce cyber security measures to international standards.

Public Policy Analysis Framework

Cyber security is an issue of public policy significance. The government decreed to formulate and implement a policy to solve certain problems for its citizens. It is essential to understand the motive behind the policy and the forces that brought it into being, how it has developed and, most importantly, to evaluate the way to achieve its stated objectives in entirety. In the simplest sense, the policy provides guidelines for its practice and ensures capable action. Multiple stakeholders have been involved to formulate the policy document, and analysis has helped to comprehend the nature and sources of the problems. This research uses policy document analysis as a research tool to investigate the nature of cyber security policy (Cardno, 2018).

National Cyber Security Policy (NCSP) 2021: An Analysis

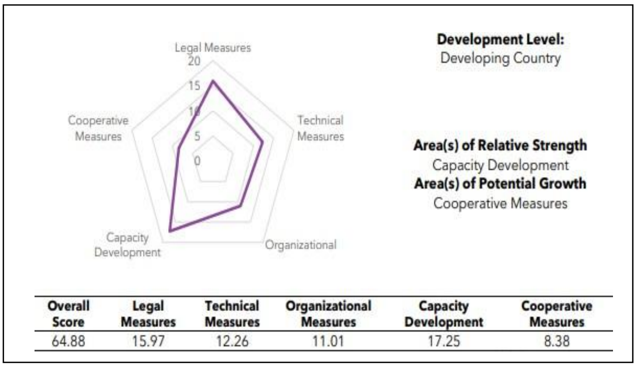
More recently, the government of Pakistan has issued a National Cyber Security Policy (NCSP) 2021. This policy constructed a set of systems or guidelines that help to achieve certain objectives and outcomes, so that the policy reflects ideas, procedures and identifies the rationale objectives. States formulate policies to protect their national interest and sovereignty in the conflicting international system (Knill & Tosun, 2012). In the current digitalized century, where there is a virtual presence in all the components of national security, an additional concern is an emerging cyber security threat to the state. Most of the states are, therefore, working to secure cyber space. In this regard, the first step was the formulation of the ‘National Cyber

Security Policy' that consisted of three pillars: people, data, and information and process. This policy has been designed to cater for these three components. The NCSP highlights the non-traditional threat to Pakistan's sovereignty and Pakistan's readiness in this regard. This research analyses the policy in three categories, as explained by Sapru (2004): context, text and implementation mechanism.

Section One: Context of NCSP

The PTI government initiative 'Digital Pakistan' is a driving force behind the formulation of Pakistan's cyber security policy that was approved by the cabinet on 27th July 2021. But this initiative started in 2018 with the aims to promote and provide digital skills, improvement in digital infrastructure, reliable and accessible internet connectivity, and e-government services to the public. Hence, in the federal budget (2020-21), under the public sector development programme, 6,673 million rupees were allocated for the information technology sector, which was not sufficient. So, Pakistan ranks 107 out of 131 countries in innovation capacity (Global Innovation Index, 2020).

According to the cyber security Global Index Report (2021), Pakistan's current ranking in cyber security is not impressive. Pakistan's overall score is 64.88 out of 100. In organizational and cooperative measures, Pakistan's performance is not satisfactory, while capacity development got the highest score (Figure 1). According to the Microsoft Digital Defense Report 2018-2019, Pakistan is the second most affected country by malware attacks. The monthly malware encounter rate in Pakistan is 18.94. Many cyber security experts are concerned that this malware encounter rate might have increased in the last two years of the coronavirus pandemic. In the last decade, cyber attacks against critical infrastructures in the public, as well as the private sector in Pakistan have resulted in huge financial and informational losses. The PTI government believes that digitalization brought a revolution into the cultural and socio-economic development throughout the world, which is also explained in the introductory section of this policy.



Development Level:
Developing Country

Area(s) of Relative Strength
Capacity Development
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
64.88	15.97	12.26	11.01	17.25	8.38

Source: Global Cybersecurity Index (2021)

Figure 1

Keeping in view the emerging cyber threats, countries are preparing themselves to counter cyber challenges. The internet security company, McAfee (2007), highlighted in its annual report that around 120 countries had developed offensive cyber capabilities. In terms of the commitment to cyber security, the Global Cyber Security Index (2018) identified five areas, i.e., technical, legal, organizational, cooperation, and capacity building, where the countries should take measures with their national cyber security, and divided countries into three groups such as high, medium, and low level, based on their commitment to adopt these measures. The UK, the USA, and France are the most committed countries, while Pakistan is included in those countries that have a medium level of commitment to engage in cyber security initiatives. In the 2017 ITU's Global Cyber Security Index (GCI) list, Singapore, the US and Malaysia are the most staunch primary states, ranking in the top three positions respectively. The GCI list places Pakistan at 66th, which is far behind compared to its neighbouring countries, India and China, which stand at 23 and 32 respectively, and fall into the category of maturing states for showing serious commitment towards securing their cyber space. Overall, the report specifies that these prominent states have shown improvement in adopting lawful actions to check breaches in cyber security, but do not have sufficient capacity to counter cyber attacks (GCI, 2017).

In its survey, the Global Cyber Security Exposure Index (2020) revealed the commitment level of the countries to cyber security in term of cyber crime and cyber attack. At global level, Finland is the least exposed country to cyber crime, followed by Denmark, Luxemburg, Australia and Estonia. The US is also in the top ten least exposed countries, while Pakistan and India are the most vulnerable countries, ranked 76 and 55 respectively out of 108 countries. Afghanistan is the topmost exposed country in the list (Frisby, 2020). These publications highlight the potential areas for improvement that should be part of national plans, as well as being useful for policy makers to help plan and strategize policies for the cyber security of their country.

It is generally believed that the South Asia region is a zone of unresolved conflicts that challenges the stability of the entire region. Both the rival neighbouring countries, India and Pakistan, occasionally indulge in cyber aggression and challenge each other's authority (Safdar, 2020). Pakistan is the most likely target of Indian cyber attack capabilities. The cyber offence policy has consistently been part of India's military doctrines. India's 'Cold Start Doctrine,' or limited war strategy, identifies seven forms of information warfare, including cyber warfare, entailing attacks on computer-based systems of the enemy. Hence, India can potentially launch offensive cyber attacks against Pakistan (Rafiq, 2017). Pakistan cannot ignore this rivalry with India. As highlighted by Qadeer (2020), the threat of Indian cyber attacks against Pakistan becomes serious due to India's growing cyber security alliance with Israel. In the current years, India has increased its efforts to fortify its defensive and offensive cyber warfare know-how, while Pakistan is far behind in cyber security, as revealed by the former CIA contractor, Edward Snowden, in 2013. He stated that Pakistan was amongst the countries which were most targeted for scrutiny by the National Security Agency (NSA), US. Pakistan's Senate Committee on Foreign Affairs also notified the government in June 2017 that Pakistan was the main target of cyber surveillance.

In recent years, numerous data breaches have taken place in Pakistan, which has pointed out the need for the country to rethink its cyber security strategy in the fight against identifying cyber theft. Cyber attacks have targeted infrastructure and services, i.e., in October, 2018, some hackers crossed the threshold, breaching the security system of a Pakistani bank. They hacked into the customers' data, procuring thousands of credit and debit cards. This cyber attack and hacking into the banking security system is a clear indication of the weaknesses in our vigilance against cyber threats (Siddiqui, 2020). Similarly, during 2019, the mobile phones of some high-ranking Pakistani representatives were hacked via technology owned by the Israeli spyware company, NSO Group. The hacking was programmed through WhatsApp with a special type of malware called "Pegasus". The malware could access a phone by making a missed call on a specified WhatsApp number, and could activate the phone's camera and microphone, along with gaining access to messages, emails, contact list, passwords and GPS locations. These incidents alarmed the people responsible for security regarding adversaries at the borders (Qadeer, 2020).

All the above incidents show that Pakistan is on the brink of cyber threats and its confidential data is on high risk that demands protective measures. Recent analyses of the cyber security situation has revealed that it is not satisfactory. Sadly, there is no agency or institute completely covering the country's cyber security, so many organizations are working on cyber security, whether they are civilian, military or academic, but they are working on their own, independently; hence, they require synchronization. Pakistan also lacks ample parameters for defying cyber threats. It is imperative for Pakistani policymakers to categorize any current and future cyber threats and frame a cyber security strategy accordingly, with the help of the IT experts, policymakers and the members of the security agencies who have a deep insight and authority in this field.

Section Two: Text of NCSP

NSCP acknowledged that the existing legislation on cyber security is not sufficiently effective to secure cyberspace. The lack of cyber security experts in Pakistan, the absence of a local ICT industry, the reliance on imported hardware and software, and the absence of national security standards and weak accreditation, have all made Pakistan vulnerable. Hence, the main objective of this policy is to improve the ICT ranking of Pakistan, as well as help to progress its GCI score. Contextually, this policy is a much-needed document that covers the offensive and defensive needs of the country. New governance and an institutional framework are also included in the cyber security policy for a ‘secure cyber ecosystem’, along with security operations centres, computer emergency response teams, and the introduction of implementation and coordination measures at sector, institutional and national levels.

The vision and scope of NCSP have been clearly defined in the second part of the policy document. The vision is to develop a resilient and secure cyber system for national cyber security, and its scope is to secure Pakistan’s cyber space for private and public sectors. The purpose of this policy is to assure the integrity, confidentiality and availability of information systems and the critical infrastructure for socio-economic development, while providing a reliable and resilient cyber space for all. NCSP consists of two parts - cyber offense and cyber security.

The list of objectives that will be achieved under this policy is to: establish the institutional framework; protect the information sharing mechanism and national critical infrastructure; protect the information system of the government; develop public-private partnership; promote a culture of cyber security awareness; enhance the availability of cyber security professionals; ensure legislative and regulatory actions, international cooperation and collaboration; and lastly, ensure the integration of ICT products and services. The government of Pakistan has formed the Cyber Governance Policy Committee for the implementation of cyber security policy 2021. According to NSCP, cyber attack on any institution in Pakistan is considered to be an attack on national sovereignty, and CGPC will monitor the response and retaliatory steps.

There are six significant dimensions of NCSP. The first is deterrence, and the second is the formation of the Cyber-Governance Policy Committee. The third, is to protect the cyber ecosystem, an internal framework which would be established in all public and private institutions, securing the national information system and infrastructure and protecting all the national ICT infrastructures. The fourth is information-sharing mechanisms which will be introduced to protect from cyber attacks at all levels. The fifth is awareness campaigns for citizens, which will be established about cyber threats, and regarding technical and operational assistance with public-private partnerships. The sixth, is training programs which will be arranged for skills development, to produce a skilled workforce.

The indigenization and development of cyber security solutions through R&D programs is an important element discussed in the policy, which needs more attention. Our country’s overdependence on external sources increases the cyber risk and hence, local resources such as man power and technology could resolve this issue. Policymakers did not, however, allocate a specific amount of budget and resources for this purpose.

In the following section, the implementation dynamics of the cyber security policy in Pakistan, along with the challenges and opportunities, are discussed. It has been mentioned in the policy document that its implementation is a major task.

Section Three: Implementation Process of NCSP

The major challenge regarding the policy is its implementation, with an action plan to achieve the objectives. A National Cyber Security Policy is a strategy document that includes timelines, priorities of items to be actioned, and the roles and responsibilities of the organizations responsible for enforcing the policy. Pakistan's weak institutional structure is one of the major hurdles in the implementation of the cyber security policy, with a couple of other imminent challenges, such as anti-state elements and the presence of hostile intelligence networks (Khan & Anwar, 2020). A Cyber Governance Policy Committee has been formed to ensure the proper implementation of the policy, consisting of all the relevant ministries and organizations. Under the said policy, a task has been assigned to the cyber crime wing of FIA to set up the Cyber Patrolling Unit (CPU) to keep a check on internet trends (Shah, 2021).

The government has allocated a 2 billion rupees budget for the placement of a CERT (Computer Emergency Response Team). Besides this, the government is also working on the Data Protection Act and cloud policy, with the collaboration of the international community (The Express Tribune, 2021). The government intended to implement the policy until June 2022 to track, protect, detect and respond to international threats to digital systems of the country. The policy authorizes a central body to remove bureaucratic hurdles, keep a check on the implementation, and carry out capacity building in the changing nature of cyber threats, but there has been no significant advancement (Nasir, 2021).

In addition, Pakistan has not signed the Convention on Cybercrime, also known as the Budapest Convention. Similarly, Pakistan does not have a Mutual Legal Assistant Treaty (MLAT) with the US, where most of the internet companies are based and whose laws they follow. Many legal issues related to social media companies can be resolved if Pakistan pursues MLAT at the policy level. Pakistan has not become a member of the OECD's Model Reporting Rules for Digital Platform, which could enable it to tax the internet companies (Khilji, 2022).

Recommendations

The recommendations for the policymakers are as follows:

1. The government should consider the cyber security issue as a top priority policy agenda, and need to be taken extraordinary action.
2. The government should adopt the preemptive approach, providing a legal framework for cyber policy and reviewing the policies of other countries.

3. The government should establish one authorized agency for the implementation of a cyber security policy.
4. The government of Pakistan must play an effective role as a member of the ITU to sign multilateral agreements to ensure better cooperation in a secure cyber space.
5. The government should provide cyber security training and education that would help in ensuring the protection of the national interests of Pakistan in cyber space.

Conclusion

Over time, cyber space has provided endless opportunities to individuals; however, there are safety and security risks involved for those who participate. The advancement in technology has brought new challenges to the security of all countries across the world. The changes have been occurring since the evolution of the internet, which is a useful platform, but the consequences have motivated the government to manage and prevent cyber incidents. Pakistan also faces multi-dimensional cyber threats that need to be addressed immediately, as developed countries have made policies and introduced strategies to mitigate cyber threats. Pakistan has cyber laws and has recently introduced a Cyber Security Policy, but the need is for its effective implementation. In this regard, the concerned organizations should cooperate and coordinate with each other, focus on the awareness campaign, and educate the masses about cyber threats. Better cooperation would lead to the proper implementation of the policy and improve the cyber security landscape. Pakistan’s cyber security policy has evolved to protect individuals and organizations, as well as society as a whole. Although the policy is quite comprehensive, in order to achieve the desired results, it needs to be put into practice in a timely and effective manner.

References

Abbasi, K. (2021). Cybercrime increases by 83pc in three years. *The News*. Retrieved from https://www.thenews.com.pk/print/884453-cybercrime-increases-by-83pc-in-three-years

ACS. (2016). *Cybersecurity – Threats Challenges Opportunities.* Sydney: Australian Computer Society.

Awan, J.H., Memon, S., Shah, M.H., & Awan, F.H. (2016). Security of Egovernment Services and Challenges in Pakistan. *SAI Computing Conference* (pp. 1082-1085). London: IEEE.

Bowen, G. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal, 9*(2), 27-40.

Cardno, C. (2018). Policy Document Analysis: A Practical Educational Leadership Tool and a Qualitative Research Method. *Educational Administration: Theory and Practice, 24*(4), 623-640.

Cavelty, M.D. (2010). Cyber-threats. In M.D. Cavelty, & Victor Mauer, *The Routledge Handbook of Security Studies* (pp. 180-188). London: Routledge.

Cavelty, M.D. (2015). Cyber secueity. In A. Collins, *Contemporary Security Studies* (4th ed., pp. 400-415). Oxford: Oxford University Press.

Council of Europe. (2020, March 27). *Cybercrime and COVID-19*. Retrieved from Council of Europe portal: https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19

Federal budget. (2020-21). *Federal budget.* finance division. Islamabad: Government of Pakistan.

Frost, & Sullivan. (2018). *Understanding the Cybersecurity Threat Landscape in Asia Pacific: Securing the Modern Enterprise in a Digital World.* Microsoft Asia News Center. Microsoft and Frost & Sullivan. Retrieved from https://news.microsoft.com/apac/2018/05/18/cybersecurity-threats-to-cost-organizations-in-asia-pacific-us1-75-trillion-in-economic-losses/

Futter, A. (2016). Is Trident Safe from Cyber Attack? *European Leadership Network*, 1-7.

Frisby, J. (2020). *global cyber security exposure index.* California: PasswordManagers.co. Retrieved from https://passwordmanagers.co/cybersecurity-exposure-index/#global

Global Innovation Index. (2020). *Global Innovation Index.* SC Johnson college of Business and World intellectual property organization, Who will finance innovation? Retrieved from https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2020.pdf

Harknett, R.J., & Stever, J.A. (2011). The New Policy World of Cybersecurity. *Public Administration Review*, 455-460.

Hassan, R.T. (2018). Cyber security: A non-traditional security threat. *Expert legal review*. Retrieved from http://expertlegalreview.com/cyber-security-non-traditional-security-threat/

Hussain, A. (2022, January 16). Should Pakistan have a cyber army? *The Express Tribune*. Retrieved from https://tribune.com.pk/story/2338876/should-pakistan-have-a-cyber-army

International Institute of Strategic Studies. (2021). *Cyber Capabilities and National Power: A Net Assessment.* London: The International Institute for Strategic Studies.

GCI. (2017). *Global Cybersecurity Index.* Geneva: International Telecommunication Union.

Global cyber security index. (2018). *International Telecommunication Union.* Global cyber security index & cyberwellness profiles. Geneve: ABI research telecommunication development sector. Retrieved from www.itu.int.

Global Cybersecurity Index. (2021). *Global Cybersecurity Index 2020: Measuring commitment to cybersecurity.* Geneva: International Telecommunication Union.

Khan, M.I. (2019). Cyber-warfare: Implications for the national security of Pakistan. *NDU Journal*, 117-132.

Khan, U.P., & Anwar, M.W. (2020). Cybersecurity in Pakistan: Regulations, Gaps and A Way Forward. *Cyberpolitik Journal*, *5*(10), 205-218.

Khilji, U. (2022). Rise in cybercrime. *Dawn*. Retrieved from https://www.dawn.com/news/1668802

Knill, C., & Tosun, J. (2012). *Public Policy: A New Introduction.* London: Palgrave Macmillan.

Nabeel, F. (2018). Need of a Robust Cybersecurity Regime for Pakistan. *Centre for Strategic and Contemporary Research*. Retrieved from https://cscr.pk/explore/themes/defense-security/cybersecurity-pakistan/

McAfee. (2007). One Internet, Many Worlds. *Sage, 2*(1). Retrieved from http://downloadcenter.mcafee.com/products/pdf/sage_2008.pdf

Morgan, S. (2020, November 13). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. *Cybersecurity Ventures*. Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Nasir, J. A. (2021). Cyber security challenges and response. *The Express Tribune*. Retrieved from https://tribune.com.pk/story/2328017/cyber-security-challenges-and-responsel

Naiyer, F. (2020). *Pakistan outlook 2020: Politics, economy & security.* Islamabad: Islamabad policy institute.

NCSP. (2021). Government of Pakistan, Ministry of Information Technology & Telecommunication, *National Cyber Security Policy 2021*, Islamabad.

NR3C. (2007). National Response Center for Cyber Crime. *Federal Investigation Agency*. Retrieved from https://nr3c.gov.pk/about_us.html

Ottis, R., & Lorents, P. (2010). Cyberspace: Definition and Implications. *5th International Conference on Information Warfare and Security* (pp. 267-270). Dayton: Academic Publishing Limited.

Qadeer, M.A. (2020, June 6). The Cyber Threat Facing Pakistan. *The Diplomat*. Retrieved from https://thediplomat.com/2020/06/the-cyber-threat-facing-pakistan/

Rafiq, A. (2017). Challenges of Securitising Cyberspace in Pakistan. *Strategic Studies*, 90-101.

Safdar, A. (2020). The emerging threat of Indian cyber warfare against Pakistan. *Daily times*. Retrieved from https://dailytimes.com.pk/660092/the-emerging-threat-of-indian-cyber-warfare-against-pakistan/

Sapru, R.K. (2004). *Public Policy: Formulation, Implementation and Evaluation.* New Delhi: Sterling Publishers.

Statista Global Survey. (2020). *Value of expenditure towards cyber security in India in 2019 and 2022.* Statista. Retrieved from https://www.statista.com/statistics/1099728/india-expenditure-towards-cyber-security-by-sector/

Shah, S.A. (2021). Cybersecurity through laws in Pakistan. *The Express Tribune*. Retrieved from https://tribune.com.pk/story/2329721/cybersecurity-through-laws-in-pakistan

Sharma, A. (2010). Cyber Wars: A Paradigm Shift from Means to Ends. *Strategic Analysis*, *34*(1), 62-73.

Siddiqui, N. (2020, August 12). Indian cyber attack targeting gadgets of govt officials, military personnel identified: ISPR. *Dawn*. Retrieved from https://www.dawn.com/news/1574034

Syed, R., Khaver, A.A., & Yasin, M. (2019). *Cyber Security: Where Does Pakistan Stand?* Islamabad: Sustainable Development Policy Institute.

Shad, M.R. (2019). Cyber Threat Landscape and Readiness Challenge of Pakistan. *Strategic Studies, 39*(1), 1-19.

Tariq, M., Aslam, B., Rashid, I., & Waqar, A. (2013). Cyber threats and incident response capability - a case study of Pakistan. *2nd National Conference on Information Assurance* (pp. 15-20). IEEE.

Tagert, A.C. (2010). *Cybersecurity Challenges in Developing Nations.* Carnegie Mellon University.

The Express Tribune. (2021, September 17). Cyber Security Policy on the cards. *The Express Tribune*. Retrieved from https://tribune.com.pk/story/2320589/cyber-security-policy-on-the-cards

World Economic Forum. (2020). *The Global Risks Report 2020*. Geneva: World Economic Forum. Retrieved from http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

Rafiq, A. (2017). Increasing cyber threats to Pakistan. *Institute of strategic studies*. Retrieved from https://issi.org.pk/wp-content/uploads/2017/10/IB_Aamna_October_13_2017.pdf

Yamin, T. (2014). *Developing Information-Space Confidence Building Measures (CBMs) between India and Pakistan.* New Mexico: Sandia National Laboratories.