Original Article (JSPGA) Publishing Date: 31th December 2021

Journal of Strategic Policy and Global Affairs

Vol: 02, Issue: 01(2021) DOI: https://doi.org/10.58669/jspga.v02.i01.01

# Cyber Security and Policy Making: An Analysis of Pakistan

Muhammad Ismail*, Naheem Gul**

* MPhil Scholar, Department of Political Science, Federal Urdu University, Karachi

** MPhil Scholar, Department of Media and Communication Studies, International Islamic University, Islamabad

**Abstract:** The knowledge and technology era is currently in full swing. Political entities are constantly evolving, with advancements ranging from electronic utilities payment processing to modern infrastructure, the use of machine learning, advanced communication systems, and technological combat. Distances have shrunk the advancement of technology, but its use has also given rise to fresh dangers and anxieties. Cybercrimes, including stealing, criminal conspiracy, financial crimes, data breaches, matters of national security acquisition, and even dangers to essential systems, have evolved into modern-day forms of cyber warfare. These risks affect both wealthy and emerging nations, creating a national security problem. Pakistan is a nuclear-capable emerging nation that is particularly exposed to these dangers. It is more difficult for the government and lawmakers to control Pakistan's digital world because of its vast variety of internet users and poorly informed technology literacy. Nowadays, Pakistan has experienced significant cyber-attacks on vital governmental portals, and attackers have effectively breached the cyberspace of crucial infrastructure. Lawmakers in Pakistan have developed legal actions that don't fully and comprehensively address the concerns to keep this from happening. What is the status of Pakistan's policy alternatives to address significant cybersecurity challenges is the real cause of discussion. However, this study concentrates on the approach of cybersecurity framework in Pakistan. This paper highlights both primary and secondary sources as part of their qualitative research approach. Finally, a few suggestions for strengthening the nation's cyber security measures are also made.

**Keywords:** Cyber Security, Policy Making, Pakistan, Technology

## Introduction

Cybersecurity is the application of all technologies, processes, and controls to protect networks and data from cyber-attacks. Information and Communication Technologies (ICT) have turned the world into a global village during the last two decades. This growth has provided low-cost access to the digital world across the globe. However, this unprecedented growth also led to some negative trends in cyberspace, and the phenomenon of cyber security emerged.

Cyberterrorism emerged as a new threat to the security of the countries. The US government body, the FBI, describes "cyber terrorism" as a "preplanned, politically inspired invasion on statistics, software, database, and records that causes extremism towards non-combatant victims by sub-national level parties or secret operatives."Cyber-terrorism involves using pc and/or related technologies to cause loss or injury to compel a target community and change the policies of the intended state or somehow change its actions (Sheldon, 2021).

Cyberterrorism is the fourth operational domain of terrorism after land, sea, and air. There are social, political, religious, or ideological goals behind an attempt at cyber terrorism activity. Usually, there are political goals behind the state-sponsored cyber terrorist activity. The journey that started from the invention of computer viruses has now reached Denial of services attacks, phishing, advanced persistent threat, and other cyber terrorism activities.

Cyberterrorism is a new challenge for Pakistan in the war against terrorism. A nuclear country with geo-political importance is at risk of victimization by cyber terrorism. Terrorist outfits are now adopting this new domain of terrorism, and rival countries are also challenging the cyber security of Pakistan. The "Indian Chronicles" exposed by EU Disinfo Lab exposed how Pakistan is being targeted on the cyber front. Pakistan needs to devise a cyber security policy keeping in view the changing trends in the cyber world (Machado et al.,2020).

### Analysis of Cyber Security Status of Pakistan

### Cyber Security Ranking of Pakistan

Pakistan ranked 79th out of 182 countries on the global cybersecurity index (GCI). In contrast, India ranked 10th, Bangladesh ranked 53rd, and Iran ranked 54th on the GCI index 2020 (International Telecommunication Union, 2020). This index checks the preparedness of the countries to defend against cyber terrorism. It means cybersecurity is not on the priority list of Pakistan, which is a matter of concern when the world is shifting to the digital economy and digital workspace. Pakistan Stock Exchange, mobile banking, and other government and treasury departments are at risk of cyber attacks.

## SWOT Analysis

| **Strengths** | **Weaknesses** |
|---|---|
| ● World's best intelligence agencies.<br>● The strict legal framework to address cybercrimes.<br>● Increasing digital workforce. | ● Lack of coordination between law enforcement agencies.<br>● Lack of research and development for indigenous cyber security solutions.<br>● Weaker defense against cyber-attacks in the past |
| **Opportunities** | **Threats** |
| ● Centre of world politics can arrange cyber drills for learning cyber security<br>● Formation of Cyber army.<br>● Sharing burden with public-private partnership. | ● Losing the war on the cyber front.<br>● Sensitive information leaks like in the past.<br>● Deterioration of law and order. |

## Review of Pakistan's Cyber Security Landscape

To ensure the online safety of the citizens of Pakistan, many federal and provincial bodies are working according to the laws defined by the Government of Pakistan. Pakistan Telecommunication Reorganisation act (1996), Electronic Transaction Ordinance (2002), Investigation of Fair Trial Act (IFTA 2013), and Prevention of Electronic Crime Act (PECA 2016) cover the aspects related to cyber security.

| **Name of Country** | **Overall Score** | **Legal Measures** | **Technical Measures** | **Organizational Measures** | **Capacity Development** | **Cooperative Measures** |
|---|---|---|---|---|---|---|
| **Afghanistan** | 5.20 | 0.40 | 1.46 | 3.35 | 0 | 0 |
| **Bangladesh** | 81.27 | 14.86 | 16.77 | 16.39 | 17.03 | 16.22 |
| **China** | 92.53 | 20 | 17.94 | 16.63 | 19.04 | 18.91 |
| **India** | 97.49 | 20 | 19.08 | 18.41 | 20 | 20 |
| **Indonesia** | 94.88 | 18.48 | 19.08 | 17.84 | 19.48 | 20 |
| **Iran** | 81.06 | 16.48 | 14.63 | 16.82 | 17.80 | 15.33 |
| **Pakistan** | 64.88 | 15.97 | 12.26 | 11.01 | 17.25 | 8.38 |

Among all of these, PECA is the most effective action that covers all the aspects of information and cyber security, but there is a need to amend this act and to increase the efficiency of Law enforcement agencies to cope with new challenges of the cyber world. Data is an asset of the country in the digital world, and our digital assets are still at risk. Even the National Database Authority (NADRA) is vulnerable to cyber-attacks. Currently, Pakistan is fighting these challenges according to National Cyber Security Policy 2021. Every cyber security policy is reviewed after three years depending upon the emerging cyber threat. But, future cyber security policy review will be a game of months or even days if we want to maintain the digital safety of the citizens of Pakistan (MINISTRY OF INFORMATION TECHNOLOGY & TELECOMMUNICATION, 2021).

## Cyber Security Challenges in Pakistan

Pakistan has a weaker cyber defense, and therefore, it is exposed to cyber terrorism. According to the Microsoft Malware infection index, Pakistan is at the top of the list of high-risk countries in the Asia Pacific region. For example, Pakistan was using Crypto AG for secret communications. A report exposed that the CIA secretly owned Crypto AG and had access to intercept communication ( Adeel & Shan, 2021).

A few years back, Indian cyber terrorists hacked 36 government websites in Pakistan, including NADRA, Pakistan Navy, and NAB sites. Another research revealed that American National Security Agency (NSA) is constantly spying on Pakistan, with 13.5 billion pieces of emails, fax, and other intercepted communications. It makes Pakistan the second-highest observed country by NSA after Iran.

Pakistan lacks a centralized digital policy for cyber security, and the country's digital assets are uncoordinated. Existing legislation doesn't provide adequate legal protection for the digital assets of Pakistan. Inadequate resources and a digital workforce are not enough to fight the war against cyberterrorism.

### GCI Index 2020: Asia Pacific Countries Profile

| Sr. No | Pakistan | Neighboring Countries |
|---|---|---|
| 1 | Regarding legal measures, Pakistan is far away from neighboring countries like India, China, and Iran. Limited resources and the capacity of affiliate departments are the leading cause of its low ranking of Pakistan on the GCI index in terms of legal measures. | India and China score 20 out of 20 on the GCI index regarding legal measures. Enhanced capacity of affiliate departments, data exchange agreements, and efficient working of the judicial system make these countries a safe place against cyber terrorism attacks |
| 2 | Pakistan lacks digital infrastructure and a cyber security workforce due to a lack of Research and Development, education, and training, which makes its ranking low in capacity development of the GCI Index. | India and China have almost full capacity development scores, making them more preprepared against cyber terrorism. |

### Detailed Overview of Asia Pacific Countries Measures Future Outlook of Cyber Security

### The Role of Artificial Intelligence

Artificial Intelligence is being used both by cyber terrorists and defenders. It is difficult to foresee the future of cybersecurity as the market is continuously changing in response to changing cybercriminal activities. But the global race to develop AI technology predicts that the future lies in the field of Artificial intelligence.

Global spending on Artificial intelligence was $ 37.5 billion in 2019, which is expected to reach $97.7 billion in 2023. It means heavy investment is needed to create an attacker-defender balance.

The first generation of AI tools helped perform tasks requiring human intelligence, i.e., decision-making, speech recognition, facial recognition, etc. The second generation of AI encouraged malicious use, and now not only individuals but also the states are fighting on the cyber front ( Durbin, 2021).

It still needs to be made clear that there will be some AI attackers-defenders balance in the future. The defenders need continuous investment, research, and development to mitigate the risk. Any security compromise will be the digital death of a country.

There are some lessons for Pakistan to foresee the future outlook of cybersecurity and build defensive capacity. We have the world's best army and the air force. But there is a need for a cyber army to combat cyber terrorism in the digital world. A country struggling on the economic front has to bear the expenses of tackling cyber terrorism. The government of Pakistan will need to build defensive capacity by finding affordable access to existing defensive technologies in the market.

### Cyber Warfare Threats Will be the Focus

The future wars will be state-run cyber warfare. It started in 2010 when a worm (Stuxnet) was implanted in Iranian Uranium Centrifuge machines. This combined operation of America and Iran caused a massive loss for Iran. In 2017 Sandworm group, a Russian Cyber military unit attacked America and Europe; in 2022, it attacked Ukraine.

Small economies in the world are shifting to this domain of warfare, avoiding traditional conflicts as they cost huge investments and human lives. Pakistan has been a victim of state-run cyber warfare in the past, and threats are still there. It demands additional security layers to sensitive government sites and systems, e.g., Airport management networks (Rasool, 2015).

### Cloud Computing and the Future of Cyber Security

Due to increased dependency on cloud computing after the advent of remote work, the world is now adopting Software as a service. Cloud storage allows you to store and access data from anywhere. According to World Economic Forum, cloud computing investment is expected to increase from $141 billion in 2021 to $ 178 billion in 2022 (Sahu, 2022).

No doubt, public cloud software has made our work easy, but at the same time, it is a big security challenge as well. Cyber security is a shared responsibility between individuals and service providers in the public cloud. Cyber terrorists launch DoS attacks and inject codes to break into a cloud server.

### Protecting Digital Identity Will be an Uphill Task

Digital Identity is an emerging phenomenon in the post-pandemic era. The future of digital identity can be a single ID to navigate the whole world. This ID can be used in credit cards and as a tool for every online service. But, protecting digital identity will be an uphill task due to identity theft and deep fake technologies. Poorly secured digital IDs will be vulnerable to cyber-terrorist attacks.

### Decreasing International Cooperation

The decreasing trend of information sharing will likely continue in the future. The UK left European Union in 2019, and since then UK has been no more part of EU cyber security bodies. State-sponsored cyber terrorism is rising due to increased political interference in the cyber world. US and UK election campaigns, the UK Brexit campaign, and Indian chronicles are examples of state-sponsored cyber security threats.

### Deep Fake and Cyber Security

Deep Fake technology uses AI techniques to temper audio-visual content for bad purposes like spreading misinformation and manipulating opponents. Deep fake increases the threat of phishing attacks and can also be used in evidence tempering to benefit the courts. Deep faking is also damaging political relations between countries. The term deep fake is now word of mouth in the politics of Pakistan, and this technology will be a challenge for cyber security if we don't find a solution.

### Data Breaches

Data breaches are going where in the near future, which means basic cyber security hygiene is needed. Search engines and social media platforms are accused of the data breach. Artificial intelligence and machine learning can predict about you based on the data gathered from cyber-terrorist attacks. Stolen data from these platforms ends on Dark Web.

## Policy Recommendations

### Active Defense Policy

Pakistan should work with Internet Service Providers (ISPs) to block or restrict access to Malware sites through Domain Name System (DNS) blocking. Pakistan can promote best cyber security practices with the help of internet governance organizations e.g., The Internet Corporation for Assigned Names and Numbers (ICANN). Similarly, with the help of international law enforcers, Pakistan can save citizens from unprotected international digital infrastructure.

### Foundation of Independent Cybersecurity Body

Pakistan lacks an independent body that can tackle every cyber security issue single-handedly. The cyber security infrastructure of Pakistan works in pieces. For example, the National Response Center for Cybercrime works under FIA and not as an independent body. A National Cyber Command Authority (NCCA) Should be formed with a mandate to tackle all legal and technical aspects of cyber attacks. Provincial cyber emergency response centers should work in collaboration with NCCA. Recently KP government has founded the KP emergency response center that can set an example for other provinces of the country.

### Protection of Government's Information Infrastructure

Government should establish national data centers to co-locate federal and provincial servers. Government should allocate a sufficient budget for cyber security. All technical government systems should be vulnerability management, and patch management of all the bugs should be performed after regular intervals. Staff vetting and clearance should also be practiced across all governmental departments.

### Raise Cyber Security Awareness

Raising cyber security awareness among the masses should be the government's top priority. For effective measures, there should be a people-centric approach, not a technology-centric one. People should adopt security measures devised by the national security policy of Pakistan.

At the organizational level, such cybersecurity lapses are due to employee negligence. Research revealed that 62 % of data breaches are due to the employee's negligence. Organizations should train individuals about common phishing and other techniques to fight cyber attacks at the individual level ( Adeel & Shan, 2021).

### Participation in Cyber Drills

Cyber drills is just like joint army training in which one country learns from the experiences of another country and vice versa. Such drills can be arranged at the organizational and country levels. In 2020, Estonia arranged cyber drills for NATO member countries to form an active defense against cyber terrorism through regional collaboration. Pakistan arranges joint army exercises every year to enhance the capabilities of the Pakistan Army, Airforce, and Navy. Pakistan is the center of world politics and can arrange cyber drills to enhance its capability against cyber terrorism ( Adeel & Shan, 2021).

### Information Security Assurance Framework

Pakistan should introduce the concept of "Cyber Security by Design" concept. There is a need to build national cyber security forensic setup to avoid advanced AI-based attacks. Constant cyber security audits can help to assess whether our cyber security mechanism complies with the world's best cyber security practices like ISO 2001, ISMS certification, and vulnerability assessment (MINISTRY OF INFORMATION TECHNOLOGY & TELECOMMUNICATION, 2021).

### Cyber security Infrastructure and Capacity Building

Establishing a Center of Excellence to educate and train human resources in cyber security can help improve the GCI ranking of Pakistan. We should encourage research and development in the cyber security field, and the government should increase the budget for research and development for indigenous solutions to cyber security threats. Cybersecurity should be a compulsory subject in the curriculum of Law and Engineering students. Special cybercrime courts are the need of the hour to tackle cyber terrorism.

### Research and Development

Research and development in the field of cyber security should start to meet short-term and long-term goals, and it should address all aspects of cyber security, including testing and maintenance, etc. The government should facilitate R & D in both public and private sectors to gain cost-effective local solutions for cyber security challenges.

### Global Cooperation and Collaboration

Pakistan should join global partners like International Multilateral Partnership Against Cyber Threats (IMPACT) in the war against cyber terrorism. The Ministry of IT & Telecom can represent Pakistan's point of view at international forums. The Ministry of foreign affairs, law, and interior ministry can help as per requirement. Pakistan should set the ground for trusted information sharing about cyber terrorism locally and globally (Rasool, 2015).

### Improving Cyber Security Via Cyber Range Concept

Improving cybersecurity through the cyber range concept can help improve Pakistan's cyber security posture in the upcoming years. The government should regularly arrange cyber security awareness sessions and training to educate professionals and the general public through standard

methodologies such as cyber ranges. Cyber ranges are virtual environments that have all the tools necessary to check the cyber security capabilities of an individual, organization, or country. Government and intelligence agencies worldwide use cyber ranges to enhance security and performance.
( Adeel & Shan, 2021)

## Conclusion

Cybersecurity is the technique of preventing harmful assaults on pcs, databases, digital phones, telecommunication technologies, networking, and communications. IT safety and online data protection are some names for it. The word can be categorized into a few typical subgroups and is used in a multitude of settings, including corporate and smartphone coding.

Likewise, cyberterrorism is any planned, ideologically biased operation over software applications, programs, and facts that makes violent threats or actually causes violent acts is common. The phrase is also broadened to cover any operation that causes anxiety or intimidation among the sample population. Attackers frequently accomplish it by destroying or impairing the country's infrastructure.

Cyberterrorism emerged as a new threat to the stability of the world. Not only are individuals involved in cyber-terrorism, but it has also become state-sponsored. While attackers and defenders use AI for attacking and defense purposes, defenders must be on the stronger front to avoid digital death.

Cybersecurity is not on Pakistan's priority list, as evidenced by the Global cyber security index. The future outlook of the cyber world demands the creation of a cyber army to tackle the emerging challenges of the digital world.

In Pakistan, the new organizational and governmental structure, and strategy will give origin to a secure cyber environment in the nation. Moreover, it will provide administrative, sectoral, and federal backing for technology emergency services and a threat detection hub.

Just like Pakistan has defensive strategies against conventional forms of terrorism, the cyber front also demands a cyber defense policy keeping in view the changing trends in the cyber world.

## Recommendations

- Avoid using secret communication software designed by any other country.
- Pakistan should not let go of state-sponsored cyber-attacks like the Indian chronicles exposed by the EU Disinfo lab.
- Encouragement of Research and development to provide indigenous solutions to cyber security challenges.
- Be an active participant in regional and international bodies fighting against cyber terrorism.
- Foundation of a single cybersecurity body for all legal and technical actions.

**Action Plan**

| **Sr. No.** | **Actions** | **Responsible agencies/departments** | **Key Performance Indicators (KPIs)** | **Timeline** |
|---|---|---|---|---|
| 1 | Enhanced Collaboration between Federal and provincial Cybersecurity Operation Centers. | All the Federal and provincial agencies. | ● Formation of National Cyber Command Authority.<br>● Enhanced technical and operational information sharing between provincial and federal bodies | 4 to 6 months. |
| 2 | Joint engagement and information sharing with the private sector on cybersecurity | Law enforcement agencies and private cyber security departments | ● Standardize cyber security information sharing protocols<br>● Joint briefings of LEAs with private sector | 6 to 8 months |
| 3 | Continued efforts on public awareness | DGPR and PID | ● Public awareness campaigns on websites and social media<br>● Providing clear and trustworthy information to citizens about how to manage threats. | 4 months |

## References

Adeel, A., & Shan, R. u. (2021). Global Cyber Terrorism: Pakistan’s Cyber Security in Perspective. PAKISTAN JOURNAL OF TERRORISM RESEARCH, 1-23. Retrieved from https://nacta.gov.pk/wp-content/uploads/2021/09/Global-Cyber-Terrorism.pdf

Durbin, S. (2021). Artificial Intelligence: The Future Of Cybersecurity? Forbes. Retrieved from https://www.forbes.com/sites/forbesbusinesscouncil/2021/09/23/artificial-intelligence-the-future-of-cybersecurity/?sh=13f71940454c

Naseer, R., & Amin, M. (2018). Cyber-Threats to Strategic Networks: Challenges for Pakistan’s Security. 2018: Research Journal of South Asian Studies. Retrieved from http://pu.edu.pk/images/journal/csas/PDF/2_v33_1_18.pdf

International Telecommunication Union. (2020). Global Cybersecurity Index. ITUPublications. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Machad et al., (2020). Indian Chronicles: deep dive into a 15-year operation targeting the EU and UN to serve Indian interests. Brussels: EU Disinfo Lab. Retrieved from https://www.disinfo.eu/publications/indian-chronicles-deep-dive-into-a-15-year-operation-targeting-the-eu-and-un-to-serve-indian-interests/

**How to Citation:** Ismail, M., & Gul, N. (2021). Cyber Security and Policy Making: An Analysis of Pakistan. *Journal of Strategic Policy and Global Affairs*, *02*(01), 1–7. https://doi.org/10.58669/jspga.v02.i01.01

MINISTRY OF INFORMATION TECHNOLOGY & TELECOMMUNICATION. (2021). NATIONAL CYBER SECURITY POLICY 2021. MoITT. Retrieved from https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Consultation%20Draft(1).pdf

Rasool, S. (2015). Cyber Security Threat in Pakistan: Causes Challenges and way forward. Elixir International Journal, 1-7. Retrieved from https://www.elixirpublishers.com/articles/1451374135_89%20(2015)%2037237-37243.pdf

Sahu, A. (2022). Why the cloud is the new rainmaker for cybersecurity. World Economic \Forum. Retrieved from https://www.weforum.org/agenda/2022/07/cloud-computing-cybersecurity/

Sheldon, R. (2021). *What is cyberterrorism?* TechTarget. https://www.techtarget.com/searchsecurity/definition/cyberterrorism