Question#1 2k21/IT/96

cyber security implementation in pakistan and other countries?

Ans: n a virtually connected world, digital gadgets
and associated services have become a fundamental part of human life. Such devices and
services are increasingly exploited by state and nonstate actors for cyber-related and cyber-enabled
crimes, which fall in the realm of cyber security.
Countries are increasingly adopting new technologies across various business spheres, and
Pakistan is no exception. With the world becoming
more and more interconnected through Information Technology (IT), cyber security threats
are multiplying and posing a fuzzy future for a

digitalized world. Since the global penetration of internet users has increased exponentially (5 billion internet users forming 63.1% of the world population, out of those, 40.7 billion are social media users who make up 59% of the world population).1 In recent years, there have been millions of cyber-attacks targeting infrastructure and services; therefore, effective cyber security is a need of the day. In the emerging cyber age, it is important to understand the impact of cyber security, data sovereignty and privacy of users linked to the sovereignty of a country. Thus, Pakistan faces cyber security challenges in critical infrastructure, governance and institutional framework. According to Global Cyber Security Index (GCI), Pakistan is lagging in technical and organizational measures, posing an imminent threat to its national security.

2 The cyber security landscape of Pakistan presents a looming picture in terms of the promotion of data gorernance and protection, virtual privacy, capacity building, national and global cooperation, and special emphasis on setting up the adoption of a risk-based approach. Most importantly, issues such as the lack of gorernance framework, ineffective implementation mechanism, excessive reliance on external resources and inadequate human resources are creating difficulties in maintaining a cyber security posture. According to a survey, Pakistan is rated 79th worldwide for cyber security capabilities. 3 In this way, Pakistan's growing reliance on Information and Communication Technologies (ICT) has increased vulnerabilities in diverse fields of security and the arena of global cyber-crimes.

Pakistan announced its first Cyber Security Policy in 2021. The draft policy requires extraordinary measures to address critical cyber issues causing challenges to Pakistan's national security. This policy objectifies a governance and institutional framework for the secure functioning of public and private organizations in compliance. Cyber Security Policy 2021 comprises 17 distinct policy deliverables, 16 of which are directly linked to cyber security. These policy deliverables present a spectrum of e-governance, technology, human resource and, particularly, cyber awareness. In a nutshell, cyber security governance is being run under exclusive national cyber security frameworks, as seen in the best practices worldwide. For the protection of cyber frontiers of a country, frameworks are arranged in an institutionalized manner. In

such systems, chief information security officers directly report to chief executive/ risk officers assigned for risk management who have dedicated security budget and performance evaluations of cyber security measures, which are entirely independent of the ICT domain, across the globe.4
I