Is Pakistan's cyber security strong enough to protect the country?

With the growth and spread of connected digital technologies, cyber threats have become an inescapable reality. According to the World Economic Global Risk Report 2019, massive data fraud and theft were ranked the number four global risk in terms of likelihood, with cyber-attacks at number five.

The same report published in 2020, listed cyber-attacks on critical infrastructures as the fifth top risk. This elucidates the growing potential of the cyber realm where governments, political groups, non-state actors, and corporations can engage in espionage, warfare, and terrorism using this domain.

According to multiple governments as well as privately documented reports, there is an ever-growing threat of cyber-based attacks on crucial infrastructure systems.

Critical infrastructure systems, being the lifeline of the modern world, hold paramount importance for both national and economic security as their reliable and secure operation is crucial for the smooth working of a state. Recognizing it as a global and national security concern, all modern states undertook emergency measures to consolidate their cybersecurity.

The cyber-attack on K-Electric

The cyber-attack on K-Electric, Pakistan's largest power supply company that took place in late 2020 reinitiated the long-drawn debate on the enactment of an appropriate cybersecurity legislation and governance framework, but to no avail. Cyberspace legislation and governance remain a neglected area in Pakistan.

The ransomware attack launched by Net walker put at risk the data of 2.5 million consumers of the company whose names, addresses, CNIC, and NTN numbers were dumped on the dark web as K-Electric failed to pay the ransom amount of $7 million.

Although K-Electric officials have claimed that the attack has not been harmful and their data remains safe, the consequences of any such future attack can be further catastrophic as Pakistan neither has an effective redressal mechanism to monitor cyber infiltrations nor data protection laws that strengthen digital privacy in the country.

The cyber-attack on K-Electric and numerous other such incidents show weaknesses in Pakistan's preparedness against cyber threats. According to the Global Security Index 2018, Pakistan was ranked 94 out of a total of 193 countries in terms of cyber preparedness.

The situation has worsened since then and can be attributed to a lack of commitment in legal, technical, organizational, capacity building areas as well as a dearth of interagency/sector cooperation in the cybersecurity domain.

What Pakistan's cyber laws lack

Different computer and internet-related laws have been enacted by the government to govern and regulate cyberspace in Pakistan.

The key ones include "National IT Policy and Action Plan of 2000", "Electronic Transaction Ordinance 2002", "Electronic Crime Ordinance 2004", "Pakistan Electronic Crime Ordinance 2007", "Prevention of Electronic Crimes Act (PECA) 2016", "Data Protection Bill 2018", and the most recent being "Citizen Protection (Against Online Harm) Rules 2020".

Even though all these legislations were aimed at addressing internet and computer-related crimes to some extent, none however adequately understands the growing sophistication of cyber-attacks.

While penalizing cybercrimes through effective national legislation is a step in the right direction, Pakistan's cybercrime laws are just one determinant of a good and secure cybersecurity system.

Unfortunately, Pakistan lags in fulfilling some of the major credentials of a good cybersecurity system. According to International Telecommunication Union (ITU), a national cybersecurity strategy is an essential first step in addressing cyber-security challenges.

Apart from the "Prevention of Electronic Crimes Act 2016", there is no security agency that lays down a national cybersecurity strategy and framework in Pakistan. There is also a lack of coherence in criminal law procedures and the policies to address cybersecurity incidents.

Moreover, there is a dearth of intelligence sharing as well as cooperation frameworks amongst the national institutions which ultimately hampers national cybersecurity efforts. Pakistan also lacks a proactive Computer Emergency Response Team (CERT) at the national level to detect and respond to cyber-threats/attacks in real-time.

Capacity-building in the domain of cybersecurity is another essential component for a robust cyber-security structure, and efforts in this regard are still at a very nascent stage.

A much-needed collaboration

Foregoing suggests Pakistan is extremely vulnerable to cyber-attacks and lacks an appropriate response mechanism.

Pakistan, therefore, needs to address its policy shortcomings vis-à-vis cybersecurity and its preparedness, considering the evolving threats to national security, which have further heightened during the COVID-19 pandemic. Any delay to ramp-up infrastructure related to cyber-security may prove costly.

The need to neutralize any possible cyber incursion is essential and cyber security laws in Pakistan must be made responsive to cope with the emerging cyber threat environment. A "National Cyber Security

Agency" should be formed to ensure collaboration between the government, military, and intelligence stakeholders. A body should be formed to conduct a cyber risk assessment of critical infrastructures and establish protection levels.

Most importantly, there is a dire need to revamp the current digital legislations, particularly PECA from a broader lens of catering for problems relating to cyberspace.

Any indifference, procrastination, or delay in acquiring robust and dynamic cyber defense will be at Pakistan's own peril.

Amna Tauhidi and Aneeqa Safdar are researchers at the Centre for Aerospace & Security Studies (CASS), Pakistan. The article was first published in Global Village Space (GVS). They can be reached at cass.thinkers@gmail.com