Institute of Regional Studies

Cyber Crime and Cyber Security Issues
Executive Summary

As the world is becoming more and more digitized and the economy is going more interdependent, cyber space tends to be the only medium through which our progress would unfold. The Covid-19 pandemic has furthered this transformation. In the digitalized world, nature of threats to a state has also been digitalized as the state institutions are becoming more vulnerable to cyberattacks. To counter this emerging menace, countries are increasing their scrutiny of cyber laws and policies. Past major cyber breaches in the region and around showed the importance of cybersecurity and also one can assess its importance from the remarks of Hillary Clinton "As president, I will make it clear that the United States will treat cyberattacks just like any other attack, we will be ready with serious political, economic and military responses".

Situation in Pakistan is graver as the country with the 76.38 million users has become the 10th largest internet user in the world, however, severely lagging in dealing with cyberattacks. On its part, Pakistan has adopted Prevention of Electronic Crimes Act passed in 2016, which proposes punishments for cyber offenders. Pakistan has only one responsible department for cyber laws implementation and cybercrime investigation named as National Response Center for Cybercrime (NR3C). NR3C records and investigates the cyber cases but is not able to counter live cyber-attacks i.e. hacking, ransomware etc. Although, over the years, Pakistan has done its share of legislation and progress regarding cyber space, yet those mechanisms and legislations have not adequately addressed the issue. Further there is a need for legislation, policymaking, coordinated efforts and collective responsibility when it comes to securing Pakistan's cyber space. In order to counter these weaknesses all commercial and government organizations must have their Security Operation Center(SOC) along with National Cyber Emergency Response Unit which will be responsible for sharing/coordination, cyber drilling, threat assessment and awareness.