DATE: __/__/____

Q The ascending potency of hybrid warfare being foisted on Pakistan, adding to its security woes.

Ans. **INTRODUCTION:**

States all over the world became reluctant to engage in a massive conflict, owing to the fact that conventional war - with increased lethality, technological advancement and nuclear threat - have become a cost prohibitive option. There has been an increase trend of subjugating the enemy through hybrid warfare.

Hybrid Warfare

- Kinetic
  - Terrorism
- Non-Kinetic
  - 5th generation war
  - Proxy war
  - Cyber attack

There are different tools used by which the tactical, political and military objectives in hybrid warfare acheived. Mostly by cyber attacks, which includes digital security breach and data theft.

Pakistan - already in shackles of multiple economic and political crisis - have been a victim of cyber attacks over the past years. The National Telecommunication and Information Security Board, recently

warned the authorities of a cyber attack by hostile elements on 14th August 2023 for disruption of services and defacement to tarnish Pakistan's image globally." Luckily that did not happen, but the advisory exposed vulnerability of Pakistan's government led websites in front of non-state actors.

=> **Increased Potency of Cyber Attacks in Pakistan:**

over the past years, Pakistan has faced multiple events of digital security breach and data theft. The digitalisation of various departments - mainly to benefit from technological advancement - has ironically exposed it of possible cyber attacks.

i) **CyberSecurity breach at NIFT:**

On July, 2023 Cyber attackers managed to breach the security of the cheque clearing institution; National Institutional Facilitation Technologies. The data of 67.5 million customers was put at high risk, and putting the national security on the verge of compromise.

) **Cyber attack on National Bank of Pakistan's servers:**

On October 2021, National bank of Pakistan came under attack for

DATE : __/__/____

the purpose of data theft. After such a blunt attack on state owned institution, the data of customers somehow remained safe, only ..... affecting some of its branches.

iii) Federal Board of Revenue under hackers attack:

On August 2021, hackers managed to break the hyper-V software by microsoft, and managed to bring down all the websites operated by tax machinery. FBR, however, managed to restore the system, but also got exposed in terms of weak cyber security, as hackers managed to exploit the weakest link; hyper-V software.

) India's Cyberattack on military departments:

"According to report of International institute of security studies, India's cyber capabilities are more focused on Pakistan, due to the ongoing tensions between the two countries."

In 2021, India organised a ... spying ware operation against ... high military officials of Pakistan using Pegasus spyware. The aim of such attack was to gather sensitive information and use it against Pakistan.

DATE: __/__/____

=> **Pakistan's Approach Towards Cyber Security:**

In recent years, Pakistan have taken several necessary steps to enhance its security in the cyber domain.

i) Pakistan launched its first-ever and much needed Cyber Security Policy in 2021.

ii) Pakistan also adapted Prevention of Electronic Crime Act, 2016. which covers variety of cyber security matters.

iii) Two private Cyber Emergency Response Centres are also active.

iv) Pakistan has also established National Centre of Cyber Security, which promotes research in cybersecurity fields.

v) Think Tanks of Pakistan also organize various seminars and conferences to highlight further steps and initiatives to be taken for cyber security.

vi) Above all, Pakistan has cooperated with China to enhance protection against common cyber threats. In 2019, first joint exercise was held to improve the ability to respond against these cyber attacks. China also provides Pakistan all the necessary aids regarding capacity building, information sharing and technical assistance.

=> Conclusion:

Pakistan rightly has strong defense strategies against conventional form of terrorism. However, a substantial amount of work needs to be done to improve cyber security of the country. Laws and regulations regarding cyber-security policies must be effectively implemented. Moreover, cooperation with strategic partners must be enhanced to deal with such non-state actors with iron hands.