**Emerging Cyber warfare threats to Pakistan**

[Basma Khalil](https://dailytimes.com.pk/writer/basma-khalil/)

February 16, 2020

“The potential for the next Pearl Harbor could very well be a cyber-attack.” Leon Panetta

In the modern era, war has been revolutionized due to rapid advancements in technology. As a result, cyber security along with its pros and cons is contributing increasingly to modern warfare. Pakistan, however, is still in the developmental phase of cyber security. Although Pakistan has passed its first law related to cyber-crimes, in the form of the 2016 Prevention of Electronic Crime Act, the overall legislation related to cyber security is still vague and not as strong to deal with the dynamic and broad-ranging nature of threats that emanate from the realms of cyber security.

In recent years, the government has taken some initiatives in order to build capacity amongst the general public such as through PAK-CERT, Presidential Initiative for Artificial Intelligence & Computing (PIAIC), Skills for all Hunarmand Pakistan, Kamyab Jawan, and National Vocational & Technical Training (NAVTTC).Yet, as has been the case for quite some time, most of these initiatives are aimed simply at spreading greater awareness to help lay the foundations for a more robust cyber security architecture. Amidst such developments, the question that arises for Pakistani policymakers is thus where their country currently stands in the cyber domain and how cyber warfare is posing threats to its national security.

In this era of innovation and connectivity even major powers such as the U.S, Russia, China, Israel and the United Kingdom remain vulnerable to an evolving spectrum of cyber threats. Across the world, states are now increasingly dependent on cyber technology which has greatly increased their chances of vulnerability. The most known example is 2015 Stuxnet virus, whereby a devastating cyber-attack on Iranian nuclear facilities wreaked havoc such as at the Nantaz Nuclear facility, significantly rolling back the Iranian nuclear program. Similarly, the WannaCry outbreak in 2017 caused mass disruption by shutting down vital computing systems in more than 80 NHS organizations in England alone. This resulted in almost 20,000 cancelled appointments, 600 GP surgeries having to return to pen and paper, and five hospitals simply diverting ambulances, unable to handle any more emergency cases. Widely attributed as being state sponsored, the attack set another devastating precedent testifying to the wide-ranging vulnerabilities that exist even in some of the world’s most advanced countries.

Pakistan’s cyber space too is insecure for many reasons because Pakistan is dependent on others for technology. According to leading global cyber security firms such as Symantec, Pakistan is among the ten most targeted countries in the world. Main targets include Pakistan’s nuclear and other critical installations, with publicly revealed assaults on an assortment of media houses, as well as the communications networks, of key government departments including, transport and, basic utilities. Such threats for instance were further confirmed by the Snowden documents released between 2013-2014 that had showed how the NSA was keeping an eye on Pakistan’s civilian and military leaders, utilizing a malware called SECONDATE.

Recently in the year 2019, Rising Security Research Institute has captured the attack launched by the internationally renowned Advanced Persistent Threat (APT) organization “Rattlesnake” through the Rising Threat Intelligence System. This time, the organization had targeted the Pakistani Navy via Target collision hijacking method. Specifically targeting the Pakistan Naval Public Relations Bureau, the attempt was aimed at stealing vital information from secure military networks while planting misleading documents masquerading as official statements from the Pakistan Navy regarding its regional neighbors such as China and India. Based on such threats, Pakistan must be readily prepared for any kind of cyber espionage and take steps towards establishing a strong national cyber policy to protect its civilian and military infrastructure.

There is still immense space to develop advanced tools and research technologies to protect Pakistan’s cyberspace, sensitive data, and local economy from cyber-attacks while restricting illegal penetrations in it

Therefore, at this stage it is imperative that Pakistan seriously focus on the development of a robust cyber war apparatus. This would especially help mitigate the numerous threats being posed to its banking system, as well as major government networks such as its ministry of Foreign Affairs as well as other military networks that have been previously targeted such as in the case shown above. As such Pakistan can take a number of initial steps by developing strategies to prevent malwares and denial of service (DOS) attacks to reduce such threats at least to a certain level.

Yet, Pakistan has still not developed a cohesive Cyber Command or any National Cyber Policy to deal with the regional cyber threats being posed to Pakistan. Even though Pakistan has recently developed a cyber-security auditing and evaluation lab, it is still in its formative stages. There is still immense space to develop advanced tools and research technologies to protect Pakistan’s cyberspace, sensitive data, and local economy from cyber-attacks while restricting illegal penetrations in it. Especially such as the initiative taken by the newly setup National Centre for Cyber Security which aims increase the number of indigenously trained cyber security professionals within the public sector.

Keeping to this trajectory Pakistan should emphasize more on indigenously developing its own cyber security industry so that in the near future it could benefit both its civilian and military infrastructure in the long run. Hence, while Pakistan may be limited in its ability to wage a strong offensive campaign within the realm of cyber warfare at the moment, such steps would go a long way in helping lay the foundations to build something greater on.

*The writer is working as Research Affiliate at Strategic Vision Institute Islamabad, a non-partisan based out of Islamabad.*