ISSUE BRIEF

INSTITUTE OF STRATEGIC STUDIES ISLAMABAD
Web: www.issi.org.pk
Phone: +92-920-4423, 24
Fax: +92-920-4658

INCREASING CYBER THREATS TO PAKISTAN

By
Aamna Rafiq
Research Associate

Edited by
Najam Rafique

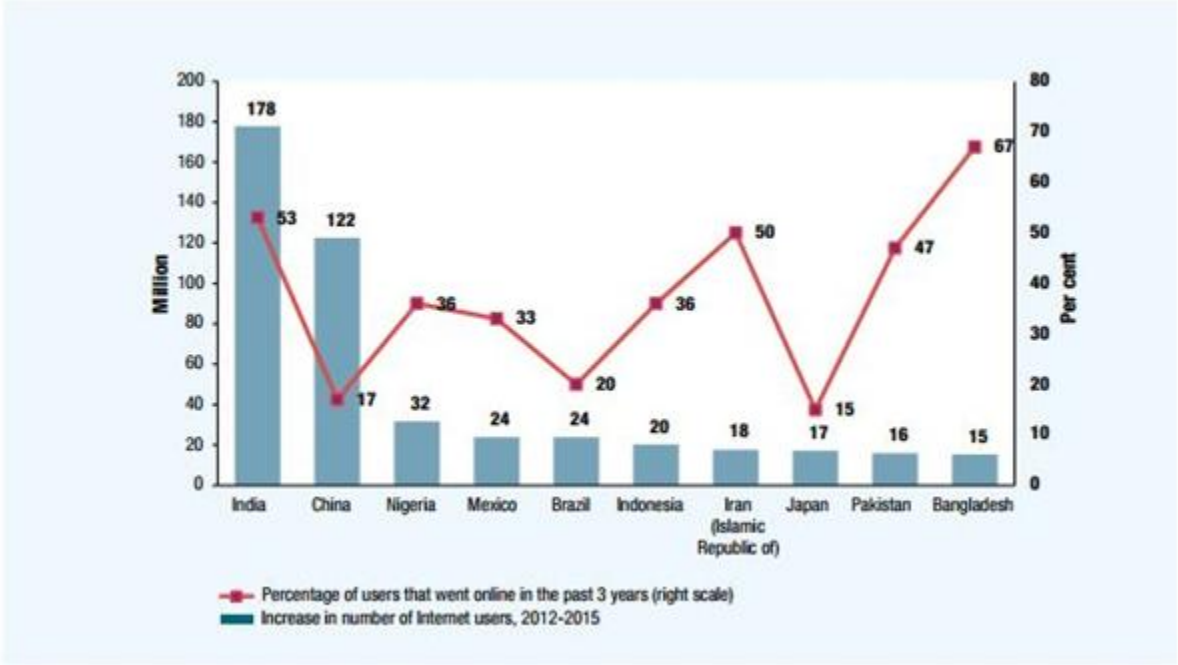
October 13, 2017

The United Nations ranked Pakistan 9th globally for its flourishing digital economy. Arrival of 3G and 4G technologies has revolutionized connectivity in Pakistan and internet penetration has increased from 3% to 15%. Over the course of three years (2012 – 2015), 16 million Pakistanis went online for the first time[1], and the number is expected to reach 17 million by 2020.[2] Undoubtedly, the development of cyberspace is creating more productive, innovative and efficient businesses and lives, but there are also serious cyber threats generated by this digitalization. Pakistan needs to be aptly prepared not only for the management of such an enormous and rapid transformation, but also to counter these threats.

1 "Information Economy Report 2017: Digitalization, Trade and Development," *United Nations Conference on Trade and Development (UNCTAD)*, October 02, 2017, http://unctad.org/en/PublicationsLibrary/ier2017_en.pdf.

2 Maheen Kanwal, "Pakistan will have 17 million new mobile subscribers by 2020, GSMA Report," *Techjuice*, April 17, 2017, https://www.techjuice.pk/gsma-mobile-economy-2017-report-pakistan-mobile/.

Figure 1: Top 10 Economies by number of people that went online for the first time (2012 - 2015)



Source: *United Nations Conference on Trade and Development (UNCTAD)*

For Pakistan, cyberspace is turning out as a domain where threats of crime, war, conflict and crisis are played out in an exceptional manner and vary vis-à-vis kind, character, power and occurrence. Pakistan has been declared as the top target of cyber espionage and malware attacks globally by the Microsoft.[3] In Pakistan, such an attack by India - Operation Hangover - was identified in 2013 against its private industries, security and political institutions which lasted for three years.[4] Earlier this year, the Cabinet Division of Pakistan issued an advisory alert against a possible hacking attack on smart phones through Whatsapp video call by Indian intelligence agencies.[5] Another organized and systematic state-sponsored cyber espionage campaign against the security institutions of Pakistan was identified in May 2017.[6]

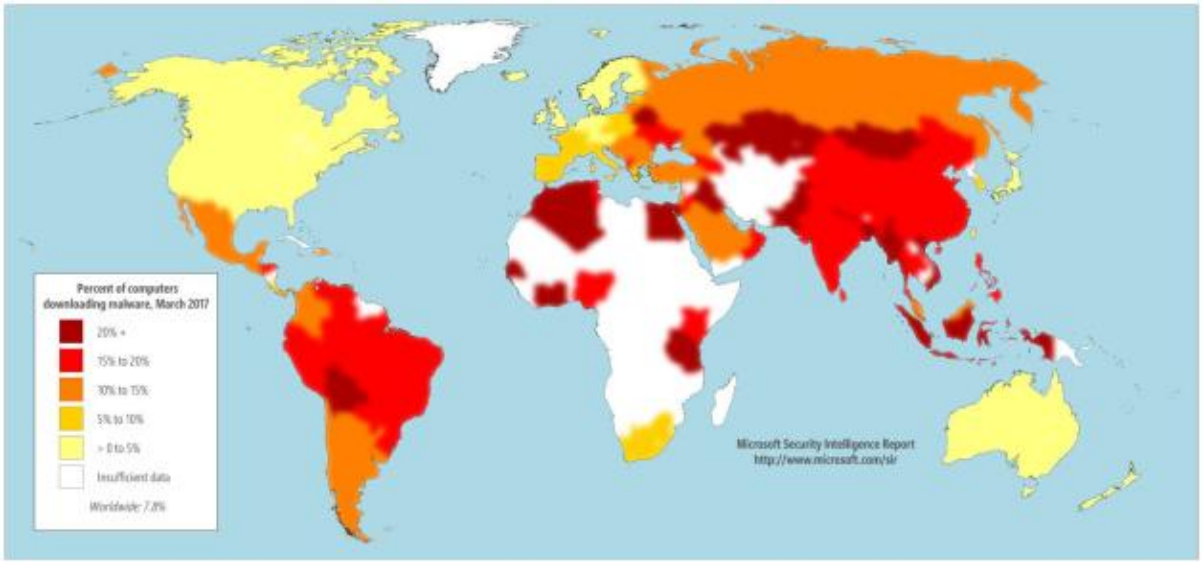
[3] "Microsoft Security Intelligence Report (Volume 21)," December 14, 2016, https://www.microsoft.com/en-sa/security/Intelligence-report ; Inamullah Khattak, "Pakistan top target for foreign espionage, Senate committee told," *Dawn*, January 19, 2017, https://www.dawn.com/news/1309413/pakistan-top-target-for-foreign-espionage-senate-committee-told.

[4] Phil Muncaster, "India attacked Norwegian telco to get at Pakistan, China – report," *The Register*, May 21, 2013, https://www.theregister.co.uk/2013/05/21/hangover_india_apt_discovered/

[5] Ahmed Ahmadani, "Advisory alert issued against cyber espionage by Indian spy agencies," *Pakistan Today*, January 3, 2017, https://www.pakistantoday.com.pk/2017/01/03/advisory-alert-issued-against-cyber-espionage-by-indian-spy-agencies/.

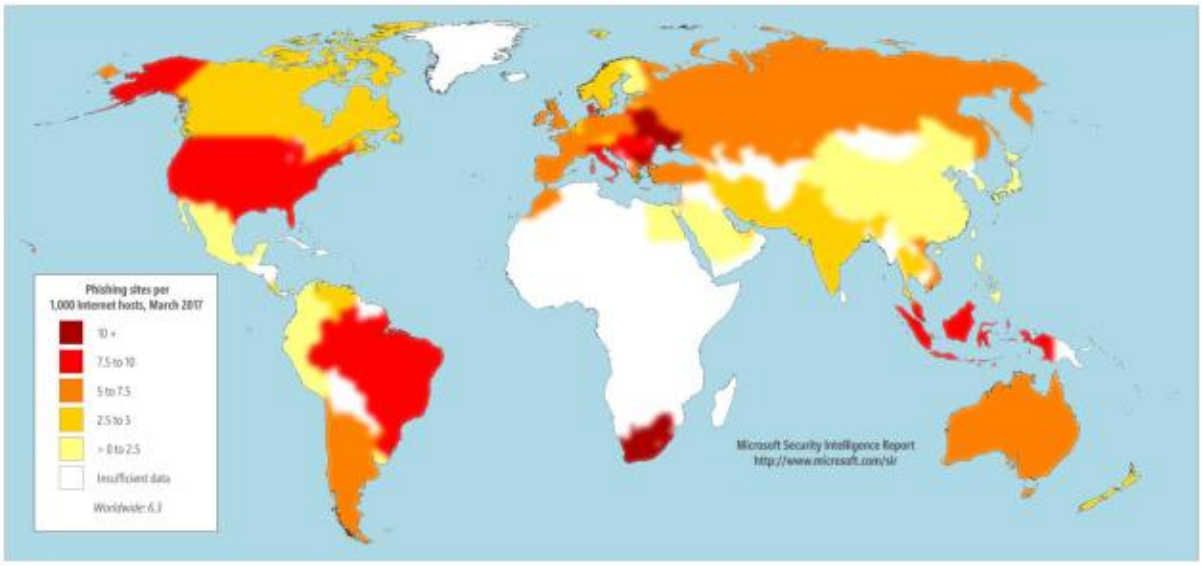
[6] Rahul Bhatia, "Exclusive: India and Pakistan hit by spy malware - cybersecurity firm," *Reuters*, August 28, 2017, https://www.reuters.com/article/us-india-cyber-threat/exclusive-india-and-pakistan-hit-by-spy-malware-cybersecurity-firm-idUSKCN1B80Y2 .

Figure 2: Encounter Rates by Country/Region, 2017



Source: *Microsoft Security Intelligence Report, 2017*

Figure 3: Phishing sites per 1,000 Internet hosts for locations around the world 2017



Source: *Microsoft Security Intelligence Report, 2017*

Globally, Pakistan has one of the highest concentrations of malware hosting sites (15 - 20 malware hosting sites per 1,000 hosts) and low concentrations of phishing sites in the world (2.5 – 5.0 phishing sites per 1,000 Internet hosts). A phishing site tries to steal confidential information by pretending as a legitimate site. A 27.48% malware encounter rate was recorded for Pakistan in the first quarter of 2017 which is the second highest worldwide.[7] The unusually common malwares directed towards Pakistan are Win32/Nuqel, Win32/Ippedo and Win32/Tupym. All of them are

[7] "Microsoft Security Intelligence Report (January – March 2017, Volume 22)," Microsoft, last modified August 17, 2017, https://www.microsoft.com/en-sa/security/Intelligence-report.

worms which are placed at the severe end of the malware threat spectrum. These self-replicating worms spread through messengers e.g. MSN/Yahoo, emails, shared network folders and removable devices. They are specialized in obstructing the normal processing of the system e.g. disables Windows utilities, changes system settings, deletes registry data and restore points, modifies web browser settings, automatic ad-clicking, downloading additional files, restarting or shutting down the system and install backdoor Trojans, key loggers, and viruses. They also have the capability to steal vital information from the system e.g. geographical location, usernames and passwords without any digital signature.[8]

In military domain, serious threats are originating from arch rival India about which there is limited academic research and alertness in Pakistan. India integrated "Information Warfare" with conventional, sub-conventional, nuclear, chemical and biological warfare in its "Cold Start Doctrine." This doctrine outlines seven types of Information Warfare: *Command and Control Warfare; Intelligence Based Warfare; Electronic Warfare; Cyber Warfare; Economic Information Warfare; Network Centric Warfare; and Psychological Warfare*.[9] India is also taking extensive measures to expand its cyber capabilities. During the year 2016-17, India signed 17 bilateral agreements and MOU`s to upgrade its cyber security infrastructure at national, regional and international level with countries like United Kingdom, United States, Israel, France, Australia, Bangladesh, Indonesia, Malaysia, Mauritius, Qatar, Portugal, Singapore and United Arab Emirates.[10] The former Indian Naval Chief Admiral Suresh Mehta categorically hinted at this intension in his statement:

> "*The Indian armed forces are increasingly investing in networked operations, both singly and in a joint fashion. We cannot afford to be vulnerable to cyberattacks. Information technology is our country`s known strength and it would be in our interest to leverage this strength in developing a formidable 'offensive' and 'defensive' cyber warfare capability."*[11]

---

[8] " Win32/Nuqel," Windows Defender Security Intelligence, Microsoft, last modified September 15, 2017, https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32%2FNuqel; "Worm: W32/Ippedo," F-Secure Corporation, last modified September 15, 2017, https://www.f-secure.com/v-descs/worm_w32_ippedo.shtml; "Win32/Tupym," Windows Defender Security Intelligence, Microsoft, last modified September 15, 2017, https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32%2FTupym.

[9] Government of India, Integrated Defence Staff, *Indian Army Doctrine 2004*, last modified October 4, 2004, http://ids.nic.in/indian%20army%20doctrine/indianarmydoctrine_1.doc

[10] "Mapping of India's Cyber Security-Related Bilateral Agreements," The Center for Internet and Society, https://cis-india.org/internet-governance/blog/india-cyber-security-bilateral-agreements-map-dec-2016.

[11] Safiya Salman, "Pak-India Cyber Warfare," *The Frontier Post*, last modified April 29, 2014, http://thefrontierpost.com/article/71262/PYF%E2%80%99s-concluding-day-tested-participants%E2%80%99-determination/

Pakistan needs to increase its capability to tackle these threats. In Global Cybersecurity Index (GCI) 2017, Pakistan is ranked 67th among 193 states with regard to cyber preparedness.[12] In terms of cyber preparedness, the Index divided states into three categories: *leading states; maturing states and initiating states*. Pakistan is among the group of "maturing states" that are developing multifaceted commitments, engaged in limited cybersecurity programs and committed to take new initiatives.[13] In recent years, Pakistan took radical measures to develop comprehensive, cross-sectoral and multi-stakeholder national cybersecurity framework and the biggest achievement in this respect is the enactment of country`s first ever cybersecurity law titled "Prevention of Electronic Crime Act, 2016."[14] It provides protection against online child abuse, electronic fraud, identity theft, cyber stalking, cyber terrorism and unauthorized access and transmission of critical infrastructure information system or data. Furthermore, Digital Pakistan Policy 2017, has also been drafted by the Ministry of Information Technology.[15] As a part of long-term plan under China-Pakistan Economic Corridor (CPEC), Pakistan is also preparing for the overhaul of its communication framework e.g. digital TV for all, safe cities project, Pakistan-China optic fiber cable connectivity project, and new submarine landing station at Gwadar for internet traffic flow.[16]

Figure 4: Pakistan's Cybersecurity Performance

Source: *International Telecommunication Union (ITU)*

To improve its ranking as a digital economy, Pakistan must work to improve its capabilities in the areas like designing cybersecurity good practices and incentive mechanisms, public-private partnership in research and development, public awareness campaigns and professional training courses. Furthermore, an exclusive public institution should be established to recommend, develop, coordinate and regulate the use of information and communication technologies by

12 "Global Cybersecurity Index (GCI) 2017," International Telecommunication Union, last modified October 05, 2017, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

13 Ibid.

14 Government of Pakistan, *Prevention of Electronic Crimes Act, 2016* , last modified August 19, 2016, http://www.na.gov.pk/uploads/documents/1472635250_246.pdf

15 Government of Pakistan, Ministry of Information Technology, *Digital Pakistan Policy, 2017*, last modified August 8, 2017, http://moit.gov.pk/policies/DPP-2017v5.pdf.

16 Qurat-ul-Ain Siddiqui and Jahanzaib Haque, "Exclusive: The CPEC plan for Pakistan's digital future," *Dawn*, October 03, 2017, https://www.dawn.com/news/1361176.

organizations and professionals. In defence sector, a specialized cyber command must be established which will modernize the cyberdefence of Pakistan to achieve the strategic cyber deterrence. Cyber threats will grow exponentially in the years to come and it is imperative to focus and invest on achieving full spectrum cyber capabilities for a secure digital future.