Cyber Threat Landscape and Readiness Challenge of Pakistan

Muhammad Riaz Shad*

Abstract

Today, vital social infrastructures — electricity, finance, water, transportation, health and food — are increasingly dependent on the Information and Communication Technology (ICT) networks for functioning, distribution and interconnectedness. This dependence results in both opportunities and vulnerabilities, which can be exploited by a variety of actors ranging from individuals to organisations and governments. This indicates that information revolution, experienced by the contemporary world, is both a boon and bane. To a large extent, it is a bane because the ICT has an 'enabling function' for disruption, crime and state-level aggression. The ICT dependence may become more prone to vulnerabilities in the times of social unrest, political tensions and other appalling events. At present, Pakistan experiences a fast growing application of the ICT in different sectors but seriously lacks in cyber readiness. In addition, the country confronts a hostile security environment internally as well as externally. These factors expose it to various cyber threats. Drawing on the securitisation theory, this paper attempts to examine the cyber threat landscape of Pakistan and focuses on the cyber threats that the country faces across the spectrum — hacking, serious and organised cybercrime, cyberterrorism and cyberwarfare. This is followed by an evaluation of Pakistan's cyber readiness profile in the light of the five-pillar criteria laid down by the UN specialised agency the International Telecommunication Union (ITU), namely legal, technical, organisational, capacity building and international cooperation.

Keywords: ICT, Cyber Threats, Cyber Readiness, Pakistan, Hacking, Cybercrime, Cyberterrorism, Cyberwarfare, Securitisation.

* *The author is Assistant Professor at Department of International Relations, National University of Modern Languages (NUML), Islamabad.*

Introduction

Since the mid-1990s, the Information and Communication Technologies (ICTs), particularly internet, have increasingly become a key part of the social life. The fast-growing internet technologies are transforming the efficiencies of various spheres of human life — business, work, governance, security and politics. However, along with bringing advantages, the ICTs tend to pose cyber threats to individual and national security. Cyber threats vary in terms of degree of severity ranging from hacking, espionage and information warfare to cybercrime, cyberterrorism and cyberwarfare. In terms of motivation, they may be related to politics, security, economics, ethnicities or cultures.

As the ICTs serve both productive and destructive objectives, states ideally adopt protection mechanisms to minimise cyber vulnerability and maximise cyber productivity. These mechanisms, entailing both administrative and technical measures to secure the ICT-dependent infrastructures are termed as cybersecurity. Since the ICTs meet socio-political objectives, they are increasingly seen as a social institution rather than mere technologies. In this sense, they constitute an important social determinant of national power, which is called cyber power. Cyber power is defined as "the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power."[1] This means that the ICTs are instrumental in realising efficient governance, better law and order, higher economic growth and military advantage. However, it is important to highlight that a state's cyber power depends on cybersecurity readiness — preparedness level against cyber threats — otherwise it transforms into cyber vulnerability. In this context, the present paper argues that Pakistan faces wide-ranging cyber threats while it increasingly makes use of internet technologies but it seriously lacks in cyber readiness.

This paper draws on the Securitisation Theory developed by the Copenhagen School with the distinct contribution of Barry Buzan and Ole Waever. The theory evolved in the context of including societal and ecological 'referent objects' in the post-Cold War security agenda.

[1] Daniel T Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, eds. F D Kramer, S Starr and I K Wentz (Washington D.C.: National Defence University Press, 2009), 38.

Securitisation involves "the process of presenting an issue in security terms, in other words as an existential threat."[2] Across a broad spectrum, an issue may be defined as 'non-politicised' (not part of political agenda), 'politicised' (part of political agenda) or 'securitised' (a matter of urgency that needs extraordinary measures).[3] In the same vein, it is the discursive process of securitisation which constructs an issue as an existential threat and, therefore, justifies a prompt response. Lene Hansen and Helen Nissenbaum identify three modalities for the securitisation of the cyber sector: hyper securitisation and everyday security practices and technification.[4] The hyper securitisation discourse emphasises 'multi-dimensional cyber disaster scenarios in view of the inter-connected societal, financial and military effects of prospective cyber warfare and, therefore, calls for 'excessive countermeasures.'[5] The discourse of everyday security practices involves mobilisation of 'normal individuals' to secure their compliance in cybersecurity and earn political legitimacy for hyper securitisation.[6] Technification, the third discourse on cyber securitisation, highlights the role of computer and information scientists in cybersecurity on account of the technical expertise required to understand cyber-attacks and protection.[7]

In the light of Securitisation Theory, this study argues that Pakistan's growing reliance on the ICTs risks vulnerability to cyber threats, particularly in the context of inter-state and intra-state conflict as well as increasing cybercrimes worldwide. More importantly, its vulnerability to cyber threats exacerbates because it does not have appropriate cybersecurity arrangements in place. Although cybersecurity, the issue remains the part of the political agenda, is not a key priority in the policy discourse, manifesting a lacklustre approach to cyber readiness. The country has adopted significant cybersecurity laws but does not yet have a national cybersecurity policy and lacks an integrated institutional system and capacity for implementation of those laws. Finally, cyber securitisation remains unrealised in Pakistan as the policy discourse, which presents a cyber threat

[2] Barry Buzan and Lene Hansen, *The Evolution of International Security Studies* (Cambridge, New York: Cambridge University Press, 2009), 214.
[3] Ibid.
[4] Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cybersecurity and the Copenhagen School," *International Studies Quarterly* (2009): 1163-1168.
[5] Ibid., 1164.
[6] Ibid., 1165.
[7] Ibid., 1166-67.

as an existential threat requiring extraordinary measures which are missing. This means that Pakistan has so far not undertaken the above-mentioned three discourses of cyberspace securitisation — extraordinary measures under hyper securitisation, mobilisation of common individuals for cyber awareness and role of cybersecurity experts under technification.

Essentials of Cyber Landscape

While the technical details of cyber threats are beyond the scope of this paper, understanding of essential concepts is important to analyse cyber issue within the socio-political construct. These concepts include cyber and cyberspace, cyber threat and cyber-attack, critical infrastructure, and cybersecurity.

According to Andrew Futter, "cyber" is a contested term carrying different meanings for different people — and should not be taken as 'merely' interchangeable with the internet.[8] Conceptually, cyber has two characteristics: electronic medium as its components and online communication as its capability.[9] Thus, in this basic sense, cyber means communication through an electronic medium, for instance, website and email. In a broader sense, cyber involves the "command and control of computers."[10] "Cyberspace," together with the characteristics of cyber, incorporates the characteristics of space, namely people or users and places for their communications.[11] Altogether, cyberspace is defined as "a time-dependent set of interconnected information systems and the human users that interact with these systems."[12] Cyberspace includes not only the internet, although most sizeable and visible area but also (online/offline) telecommunications networks, (online/offline) computer systems and embedded processors as well as controllers.[13]

[8] Andrew Futter, "Is Trident Safe from Cyber Attack?," *European Leadership Network* (2016): 1, https://www.europeanleadershipnetwork.org/wp-content/uploads/2017/10/Is-Trident-safe-from-cyber-attack-1.pdf
[9] Binxing Fang, *Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace* (Beijing: Springer, 2018), 3.
[10] Futter, "Is Trident Safe."
[11] Fang, *Cyberspace Sovereignty*.
[12] Ibid.
[13] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford University Press, 2014), 9.

"Cyber threat" is a possible "action that may result in unauthorised access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, or availability of an information system or information that is stored on, processed by, or transiting an information system."[14] The cyber threat may take two forms — cyber-attack and cyber exploitation. "Cyber-attack" is a cyber-operation to "alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programmes resident in or transiting these systems or networks."[15] Cyber exploitation involves confidential information covertly obtained through cyberspace. Depending on the kind of actor and motivation, cyber threats can be divided into various types — cybercrime, cyberterrorism, cyberwar and cyberespionage. In technical terms, these cyber threats can take place in a number of forms — account takeover, imposter fraud, denial of services, computer network attack, computer network operations, remote shutdown and sabotage.

Serious cyber-attacks target critical infrastructures of an organisation or even a state. Here, infrastructure refers to "a framework of interdependent networks and systems, generally interlinked at many different levels, including industries, institutions and distribution capabilities that provide a flow of products or services."[16] Five broad sectors can be identified as critical infrastructures, particularly in modern developed countries: information and communication, banking and finance, energy, transportation networks and human services.[17] Among these, information and communication infrastructures are directly vulnerable to cyber-attacks. Since other critical infrastructures are interconnected through information and communication networks, they are also vulnerable to cyber risks.

"Cybersecurity," also termed as information technology security refers to the technologies, processes and practices "to prevent, detect and recover from damage to confidentiality, integrity and availability of information in

[14] Pauline C Reich and Eduardo Gelbstein, *Law, Policy and Technology: Cyberterrorism, Information Warfare and Internet Immobilisation* (Hershey, USA: 2012), 228.
[15] Alison L Russel, *Cyber Blockades* (Washington, DC: Georgetown University Press, 2014), 8.
[16] Edward Halpin et al., eds. *Cyberwar, Netwar and the Revolution in Military Affairs* (Hampshire & New York: Palgrave Macmillan, 2006), 35.
[17] Ibid.

cyberspace."[18] This general definition indicates that cybersecurity involves not only technical but also political and legislative measures.

Pakistan's Cyber Threat Landscape

The cyber threat landscape of a state or an organisation is shaped by the degree of vulnerability of its ICT dependent infrastructures. This vulnerability is related to both technical and social factors. A state that lacks effective cybersecurity arrangements and faces a hostile socio-political environment — resulting from its involvement in internal/external conflict — risks relatively more cyber threats including cyberwar. In this context, Pakistan's cyber threat landscape is shaped by the country's increasing reliance on the internet for governance and service delivery and its vulnerability to cyber threats due to poor cybersecurity preparedness as well as the hostile socio-political environment it faces domestically and regionally.

Pakistan's Growing Reliance on ICTs

In the last two decades, the growing use of the ICTs, particularly the Internet, has led to the rise of e-commerce and e-government. As the countries worldwide rapidly develop a reliance on the ICTs, their dependency on cyberspace increases more than ever. More than four billion people across the world (55.1 per cent) use the internet as of June 2018, compared to only 16 million users (0.4 per cent) by December 1995.[19] This demands an ever-increasing responsibility of a state to secure its virtual boundaries in addition to physical boundaries. This is especially true for Pakistan as it experiences fast growing e-government, e-commerce and e-business in a security environment which potentially poses serious cyber threats due to volatile regional conflict, extremism and terrorism. Since independence, Pakistan has been confronting challenges to physical security, now it also needs to address the threats to information security in pursuance of securing its increasing use of the ICTs.

According to the Pakistan Telecommunication Authority's (PTA) February 2019 statistics, 65 million people in Pakistan have internet access,

[18] Jennifer L Bayuk et al., *Cybersecurity: Policy Guidebook* (Hoboken, New Jersey: John Wiley & Sons, 2012), 3.
[19] "Internet Growth Statistics," https://www.internetworldstats.com/emarketing.htm

accounting for more than 31 per cent internet penetration rate in the country.[20] The UN Conference on Trade and Development, in Information Economy Report 2017, ranked Pakistan among top 10 booming digital/internet economies in the world.[21] The report revealed that around 16 per cent Pakistanis got internet access in a period of just three years (2012-2015), increasing penetration rate from 3 per cent to 15 per cent. This exponential increase in internet access is mainly the outcome of the introduction of 3G/4G technologies in Pakistan in recent years. Currently, out of a total of 65 million broadband subscribers, 63 million access internet through 3G and 4G smartphones.[22]

Pakistan falls among those developing countries where both public and private organisations are increasingly deploying online administrative and service systems. In this regard, the National Database and Registration Authority (NADRA) is the most important and sensitive public organisation as it centrally holds national Identity Documents (ID) database of the Pakistani citizens. The NADRA shares online information of citizens with banks, Election Commission of Pakistan, immigration and passports department, mobile networks and security departments.

For modernisation and better efficiency, a number of Pakistan's public corporations are growingly providing e-services in economic, social and security sectors. In Pakistan, E-Government Directorate was established in 2002 under the IT Ministry which was renamed as National Information Technology Board after the merger with Pakistan Computer Bureau in 2014. Consequently, the economic sector of the country routinely experiences a number of ICT-based services, including Automatic Teller Machines (ATMs), internet banking, online payments and online stock exchanges. Some social sectors, such as educational institutions, hospitals and police departments (Khyber Pakhtunkhwa), also deliver e-government services. Furthermore, digitalisation of military assets and nuclear arsenals is the hallmark of their modernisation in the 21st century and Pakistan is no exception in this regard.

[20] "Telecom Indicators," *Pakistan Telecommunication Authority*, https://www.pta.gov.pk/en/telecom-indicators
[21] Amin Ahmed, "Pakistan Among Top 10 Economies in Terms of its Internet Users," *Dawn*, October 4, 2017, https://www.dawn.com/news/1361586
[22] "Telecom Indicators."

Pakistan's Vulnerability to Cyber Threats

In the age of digital technology, cyberspace is becoming the weapon of crime, terrorism and conflict, complementing and, at times, replacing the traditional instruments of crime. This virtual reality of today's world poses a great challenge to national security as it offers opportunities to malicious actors to attack the critical infrastructures. Accordingly, Pakistan's growing dependency on cyberspace, notwithstanding its necessity and advantages, creates vulnerabilities for the country's national security, particularly because it lacks reliable cybersecurity systems. According to the 2017 annual report of the Global Cybersecurity Index (GCI), Pakistan ranked 67th out of 193 countries in terms of commitment to cybersecurity.[23] According to the report, this poor ranking owes to the country's insufficient measures — legal, technical, organisational, capacity building and cooperation — to upgrade cybersecurity.

Pakistan's poor cybersecurity arrangements are evident from a few examples. In March 2013, *Guardian* revealed through Snowden's leaks that after Iran, Pakistan was the second most targeted country for surveillance by the US National Security Agency (NSA).[24] Later, *Intercept,* citing the same source, reported that the UK's intelligence agency Government Communications Headquarters (GCHQ) hacked into Pakistan's central communications infrastructure to access commonly used websites.[25] The Microsoft declared that Pakistan received the highest number of malware attacks in the second half of 2015, while Pakistan's Senate Committee on Foreign Affairs later found out that the country was among the top countries under the foreign espionage.[26]

With regard to cybersecurity, this poor state of affairs not only shows the degree of Pakistan's vulnerability to cyber threats but also exposes the

[23] "Global Cybersecurity Index 2017," 55, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

[24] John Cassidy, "Why Edward Snowden is a Hero," *New Yorker,* June 10, 2013, https://www.newyorker.com/news/john-cassidy/why-edward-snowden-is-a-hero

[25] "British E-spy Agency Hacked Network Routers to Access Almost any Internet User in Pakistan," *Express Tribune,* June 24, 2015, https://tribune.com.pk/story/908732/british-e-spy-agency-hacked-network-routers-to-access-almost-any-internet-user-in-pakistan/

[26] Aamna Rafiq, "Increasing Cyber Threats to Pakistan," Institute of Strategic Studies Islamabad, Issue Brief (2017): 2.

lack of readiness — in terms of legislation, policy and implementation — to counter the threats. Coupled with the external and internal security challenges, Pakistan's lack of preparedness in cybersecurity make it a likely target of various cyber threats which can broadly be divided into four types:

i. Hacking
ii. Serious and organised cybercrime
iii. Cyberterrorism
iv. Cyberwarfare

Hacking

Hacking — illegal access to computer systems for destruction, disruption or any illicit activity — is the first and most common cyber threats. The types of hackers vary with respect to their motivation and expertise. The hackers might commit the act of hacking for mere fun, petty theft and revenge or they may be motivated by some ideological or political campaign either at the national or international level. In terms of their motivations, the hackers may be seen as those who hack for themselves or activism, or those who are doing it for criminal purposes, or those who are sponsored by the states. Since hacking is a disorganised activity and has low-level consequences, it is far less threatening than other serious cyber threats. Still, it is considered as a consequential threat not only because it may seriously perturb the affected but also because it may lead to more profound cyber threats such as serious cybercrime and cyberwarfare.

While the above-mentioned hackers' activities have relevance to Pakistan, the Indian hackers apparently acting under the sponsorship and direction of the Indian state, pose a serious challenge. Since 1998, the Indians have been hacking the Pakistani government and security agencies' websites mostly with the Denial-of-Service (DoS) attacks. According to the reports, 1600 Pakistani websites were targeted by the Indian hackers between 1999 and 2008.[27] The phenomenon has become more frequent and organised since the formation of the Indian Cyber Army (ICA) comprising software professionals in August 2010. The group hacked about 36 Pakistani websites, including those of NADRA, National Accountability

[27] Ahyousha Khan, "Cyber Securitisation: Need of the Hour for Pakistan," *South Asia Journal* 24 (2017), http://southasiajournal.net/cyber-securitization-need-of-the-hour-for-pakistan/

Bureau (NAB), Pakistan Navy and ministries of finance, foreign affairs and education.[28] In 2013, a Norwegian cybersecurity firm reported that the Indian hackers had been conducting an espionage 'operation hangover' against Pakistan since 2010.[29] The firm disclosed that the hackers targeted senior managers of the corporate and government institutions.

India-Pakistan cyber-attacks usually occur in the context of important events, such as Independence Day and in a tit-for-tat move. For instance, retaliating to the ICA's attack on Pakistan's 40 websites, including that of the State Bank of Pakistan, the Pakistani hackers defaced India's 270 websites, including that of the Central Bureau of Investigation (CBI).[30] More recently, the Indian hackers targeted 30 government websites in Pakistan as a reaction to the latter's announcement of a death sentence for an Indian spy, Kulbhushan Jadhav. The Pakistani hackers launched a counter-attack which was then retaliated by the Indians.[31] These examples are a manifestation of not only the existing nature but also the future trend of cyber threat between Pakistan and India. At present, hacking of the Pakistani websites by the Indians does not pose a serious threat but the frequency of attacks indicates that it is more than just a nuisance. More seriously, the frequent exchange of hacking between the Indians and Pakistanis may lead the two sides to engage in serious and sophisticated cyber-attacks, resulting in cyberwarfare.

Serious and Organised Cybercrimes

With increasing digitalisation of financial and commercial activity, the organised and skilled criminals are accordingly tempted to cybercrime. The black market networks, for instance, Dark Market, are engaged in a variety of cyber crimes such as theft, buying and selling of personal data from bank accounts, credit cards, identity numbers and passwords as well as the trade of botnets. With "the migration of real-world organised crime to cyberspace,"

[28] Muhammad Shabbir, "Cybersecurity in Pakistan: Emerging Threats and Preventive Measures," *ISSRA Paper* vi (2013): 30.
[29] Khan, "Cyber Securitisation."
[30] Iftikhar Alam, Pakistan-India Cyber-War Begins," *Nation*, December 5, 2010, https://nation.com.pk/05-Dec-2010/pakistanindia-cyber-war-begins
[31] Arpan Rai, "Tit for tat Hack attack! Pakistan Black Hats Hit Back after Indian Cyber Strike to Avenge Naval Officer's Death Penalty," *Mail Online India*, April 26, 2017, http://www.dailymail.co.uk/indiahome/indianews/article-4445606/Pakistan-black-hats-hit-Indian-cyber-strike.html

world economy significantly suffers. According to a 2014 report of the Centre for Strategic and International Studies (CSIS), cybercrime costs the world economy around US$445 billion per annum.[32] While cybercriminals can operate transnationally without being detected, authorities across the world have yet to agree to cooperate with one another.

With the increasing trend in e-banking and e-government, cybercrime is on rise in Pakistan. The country meets the cases of cybercrime on a daily basis, which may range from account hacking to dangerous attempts like unauthorised and illegal cash withdrawal or fund transfer. Federal Investigation Agency's (FIA) cybercrime wing, the National Response Centre for Cyber Crimes (NR3C), registered 2019 complaints in 2017, which can be divided into three main categories: 1592 (76 per cent) pertaining to harassment, defamation and blackmailing via social media; 307 (14 per cent) regarding financial fraud; 116 (5 per cent) related to threatening calls and 186 about email hacking.[33] It is important to underline that a number of cases remain unreported due to the lack of awareness about cyber laws or trust in the law enforcement agencies.

Given the aforementioned list, the banking sector seems to be more prone to vulnerability to serious cybercrimes. In late 2017, a serious cybercrime targeted the ATM facilities of Habib Bank Limited (HBL) through skimming devices, resulting in an unauthorised intrusion into 579 accounts and loss of Rs.10 million.[34] The bank also received cyber-attacks in 2015 and 2016. It is important to underscore the two means of cybercrime that are particularly on rise in these days — computer hacking and phishing/email scams. Through these means, cybercriminals get into a computer network and steal personal/confidential data which enables them to commit fraudulent activities.

[32] "Cybercrime Costs Global Economy US$445 Billion a Year: Report," *Reuters*, June 9, 2014, http://www.reuters.com/article/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609

[33] "FIA Launches Cyber Crime Reporting Website," *Pakistan Today*, January 9, 2018, https://www.pakistantoday.com.pk/2018/01/09/fia-launches-cyber-crime-reporting-website/

[34] Salman Siddiqui, "Beware ─ Hackers are going after ATMs in Pakistan," *Express Tribune*, December 3, 2017, https://tribune.com.pk/story/1574702/2-beware-hackers-going-atms-pakistan/

Cyberterrorism

Cyberspace is becoming an important meeting place for ideologically and politically motivated terrorists, particularly because this offers them a convenient space to pursue their local and transnational agendas. They can use cyberspace for a number of activities: communication, propaganda, indoctrination, radicalisation, recruitment and training. Moreover, they can exploit the ungoverned cyberspace for disrupting the websites and networks of their enemies, stealing money and coordinating attacks in the physical world. The use of cyberspace for terrorist agenda is lucrative and convenient because it offers anonymity; it is cheap and it provides transnational virtual reach.

In the post-9/11 period, Pakistan suffered the worst form of politico-religious extremism and terrorism, particularly at the hands of Tehreek-i-Taliban Pakistan (TTP) and sectarian outfits. This is coupled with ethnic separatism and violence. While the terrorist organisations in Pakistan have mostly launched physical attacks to play havoc in the country, they have utilised cyberspace to brainwash/recruit members as well as spread their narrative.

Following the *Zarb-e-Azb* military operation against various militant groups in FATA, particularly North Waziristan, the terrorist hideouts and safe havens have been demolished. Consequently, the physical space has widely squeezed for terrorist groups to carry out their operations. This can potentially push them to exploit the cyberspace to realise their nefarious aims. To this end, two factors are notably important. First, the terrorist organisations like TTP, Islamic State and al-Qaeda, have the resources and capacity for adaptability to virtual warfare. Second, known for a strong aversion to Pakistan, TTP allegedly has a backing of the security agencies which are hostile to Pakistan. This indicates that the group, with foreign support, can potentially make use of cyberspace for vindictive activities vis-à-vis Pakistan. In such a scenario, the terrorists can attack critical infrastructures in lieu of their previous attacks on physical infrastructures and can indulge in cybercrime for stealing money.

Cyberwarfare

Cyberwarfare refers to the state-sponsored cyber-attack which is usually well-funded, organised and conducted by highly skilled personnel. Usually, the states have political, security and strategic motivations behind such cyber-attacks. A new form of warfare has come of age in which cyberspace is being strategically used to facilitate the conventional military attacks. This kind of 'cyber-enabled physical attack' first disrupts critical infrastructures to facilitate a physical attack on a military target. For instance, in 2007, Israel shut down Syria's air defence capabilities using a cyber-attack and launched an air strike on a nuclear reactor in the country, without being detected.[35] Similarly, in 2008, Russia allegedly made strategic use of cyberspace in the midst of its conflict with Georgia over South Ossetia.[36]

In its 2007 annual report, McAfee, the internet security company, stated that around 120 countries had been developing offensive cyber capabilities — manipulation, denial, disruption, degradation, or destruction of computer and information systems. India, along with others particularly the US, China, Russia, Israel, North Korea and Iran, is certainly a notable country in this list. Given an enduring rivalry between the two neighbours, Pakistan is the most likely target of the Indian cyberwarfare capabilities. The cyber offence policy has consistently been part of India's military doctrines. India's 'Cold Start Doctrine' or limited war strategy identifies seven forms of information warfare, including cyberwarfare entailing attacks on computer-based systems of the enemy. Similarly, the Joint Doctrine of Indian Armed Forces, released in April 2017, stresses the importance of cyberspace operations in support of military operations. During 2016-17, India concluded 17 agreements/MOUs with a number of countries, including the US, UK, France, Australia and Israel to standardise the cybersecurity infrastructure.[37]

India is one of the leading software exporting countries in the world and produces more than 100,000 IT professionals each year. With this huge advantage in terms of financial resources and human expertise, it is

[35] Randall R Dipert, "Other-Than-Internet (OTI) Cyberwarfare: Challenges for Ethics, Law and Policy," in *Military Ethics and Emerging Technologies,* ed. Timothy J Demy et al. (Oxon, New York: Routledge, 2014), 229-248.
[36] Ibid.
[37] Rafiq, "Increasing Cyber Threats to Pakistan," 4.

potentially in the position to develop offensive cyber capabilities and deploy cyberwarfare against Pakistan. As the former Indian Naval Chief, Admiral Suresh Mehta, pronounced, "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' cyberwarfare capability."[38] This indicates that India and Pakistan, after fighting land, air and sea warfare, can potentially engage in cyberwarfare.

Although a large scale cyber-attack against Pakistan has not taken place as yet, cyber skirmishes between India and Pakistan are becoming commonplace. India has professionally trained hacker groups such as ICA and Hindustan Hackers Organisation. Web vandalism and cyber espionage are the known cyber tools that India is currently using against Pakistan. However, the Indian capability to attack Pakistan's critical infrastructure should not be ruled out. According to the Indian newspaper *Hindu*, an Indian cybersecurity organisation claimed that it penetrated into the critical infrastructures of Pakistan, including defence infrastructure.[39] Moreover, the Indian cyber threat to Pakistan becomes more serious when it is seen in the context of India-Israel cybersecurity cooperation under the garb of their comprehensive security cooperation. The two countries have established cooperation in cybersecurity with a special focus on Human Resource Development (HRD). In this regard, Israel's Talpiot training programme is both inspirational and instrumental to upgrade the Indian cybersecurity architecture. Established in the 1970s by the Israeli Defence Forces, Talpiot is known for producing cybersecurity experts and it was allegedly involved in the Stuxnet cyber-attack against Iran's nuclear programme in 2010.[40] In short, India can potentially launch offensive cyber-attacks against Pakistan.

[38] S M Hali, "Indian Cyber Weapon Capability," *South Asian Monitor*, July 29, 2017, https://southasiamonitor.org/news/i/n/24434?title=i&type=n&nid=24434

[39] "Pakistan's Infrastructure Systems Vulnerable: Cybersecurity Expert," *Hindu*, November 1, 2016, http://www.thehindu.com/news/cities/chennai/Pakistan%E2%80%99s-infrastructure-systems-vulnerable-Cyber-security-expert/article15419881.ece

[40] Madhulika Srikumar, "India and Israel's Cybersecurity Partnership Could be a Potential Game Changer," *Wire*, July 10, 2017, https://thewire.in/diplomacy/india-israel-cyber-security-partnership

Readiness Challenge of Pakistan

The digital world is so vulnerable to virtual threats that no country can claim to have achieved fool proof cybersecurity; however, the states can maximise the security of IT systems. In its March 2018 report, Symantec, a corporation that maintains the world's largest cyber threat databases, warned that cyber threats are increasing in number and becoming diverse with every passing year. The key findings of the report unfolded further growth in the cyber threat spectrum over the course of 2017.[41] It highlights that attacks on the Internet of Things (IoT) have increased by 600 per cent. Moreover, the attacks through malware — a malicious software to cause damage to computers — have increased by 200 per cent while Ransomware — malicious software that blocks access to a computer for ransom — is accessible to even common criminals. More alarmingly, in 2017, the new variants of mobile malware witnessed an increase of 54 per cent and approximately 24,000 malicious mobile apps were identified each day.

The Symantec report focuses on data collection related to cybercrime threats to civilians only. When security and politically motivated cyber-attacks are taken into account, the cyber threat landscape becomes more dangerous. In response to ever increasing and diversifying cyber threats, the states undertake various measures to attain cybersecurity. The UN specialised agency International Telecommunication Union (ITU) measures the commitment of the states to cybersecurity taking five criteria into account: legal, technical, organisational, capacity building and international cooperation. In terms of their commitment to cybersecurity, the states can be categorised as leading, maturing and initiating sates. Singapore, the US and Malaysia are the most committed leading states ranking first, second and third on ITU's GCI report list of 2017.[42] India, China, Bangladesh, Iran and Pakistan are categorised as maturing states holding 23rd, 32nd, 53rd, 59th and 66th position on the 2017 GCI respectively.[43] In general, the report indicates that the states are better in undertaking legal measures for cybersecurity but lack in capacity for countering the cyber-attacks.

[41] "Internet Security Threat Report," Symantec, vol. 23, 5-6, https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf
[42] GCI 2017, 17.
[43] Ibid.

Although Pakistan falls in the list of maturing states in terms of commitment to cybersecurity, an analysis of its performance in each of the aforementioned criteria depicts a poor picture. This is particularly true in consideration of the seriousness of cyber threats to the country. The ITU's report on Pakistan's cyber wellness profile shows that it has not adopted sufficient legislative measures for cybersecurity.[44] The Electronic Transaction Ordinance 2002 (ETO 2002) provided for legal protection of e-commerce penalising violation of privacy and damage to the information system. ETO's limitation to cover other various cybercrimes was regarded as the major inadequacy. To deal with cybercrime comprehensively, Prevention of Electronic Crimes Ordinance 2007 (PECO 2007) was adopted but it was repealed in 2009 after failing to approve it as an Act. Lately, Pakistan has promulgated the Prevention of Electronic Crimes Bill 2015 (PECB 2015) which covers a wide range of cybercrimes — cyberterrorism, hate speech, spamming and cyber-stalking, electronic forgery and fraud and interference with critical infrastructure.[45] However, the PECB has been criticised for undermining the freedom of speech, containing vague language and granting unrestricted powers to the PTA.

Regarding technical measures for cybersecurity, Pakistan has the bodies, namely Pakistan Computer Emergency Response Team (Pak CERT) and Pakistan Information Security Association ─ Computer Emergency Response Team (PISA-CERT). Their services range from providing information on cyber threats to providing assistance and capacity building in cybersecurity. In addition, the Senate Defence Committee has established Pakistan Research Centre for Cybersecurity under the Cybersecurity Task Force. Further, Pakistan launched first-ever National Centre of Cybersecurity (NCCS) at Air University, Islamabad in May 2018.[46] However, the country does not have an official cybersecurity framework to enforce cybersecurity measures of international standards.[47] Moreover, it does not follow a certification framework for agencies or

[44] "Cyber wellness Profile ─ Islamic Republic of Pakistan," ITU, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Pakistan.pdf
[45] Daanika Kamal, "Policing Cybercrime: A Comparative Analysis of the Prevention of Electronic Crimes Bill," Jinnah Institute, Policy Brief, January 18, 2017, 3-8.
[46] Afshan S Khan, "NCCS to Develop Tools to Protect Pakistan's Cyber Space," *News*, May 22, 2018, https://www.thenews.com.pk/print/319672-nccs-to-develop-tools-to-protect-pakistan-s-cyber-space
[47] "Cyber Wellness Profile."

professionals dealing with cybersecurity. Consequently, Pakistan has until now failed to establish a governmental agency or develop a significant number of public sector professionals for cybersecurity in accordance with internationally recognised standards. In short, the country seriously lacks attention, planning and initiatives with regard to capacity-building in the cybersecurity domain.

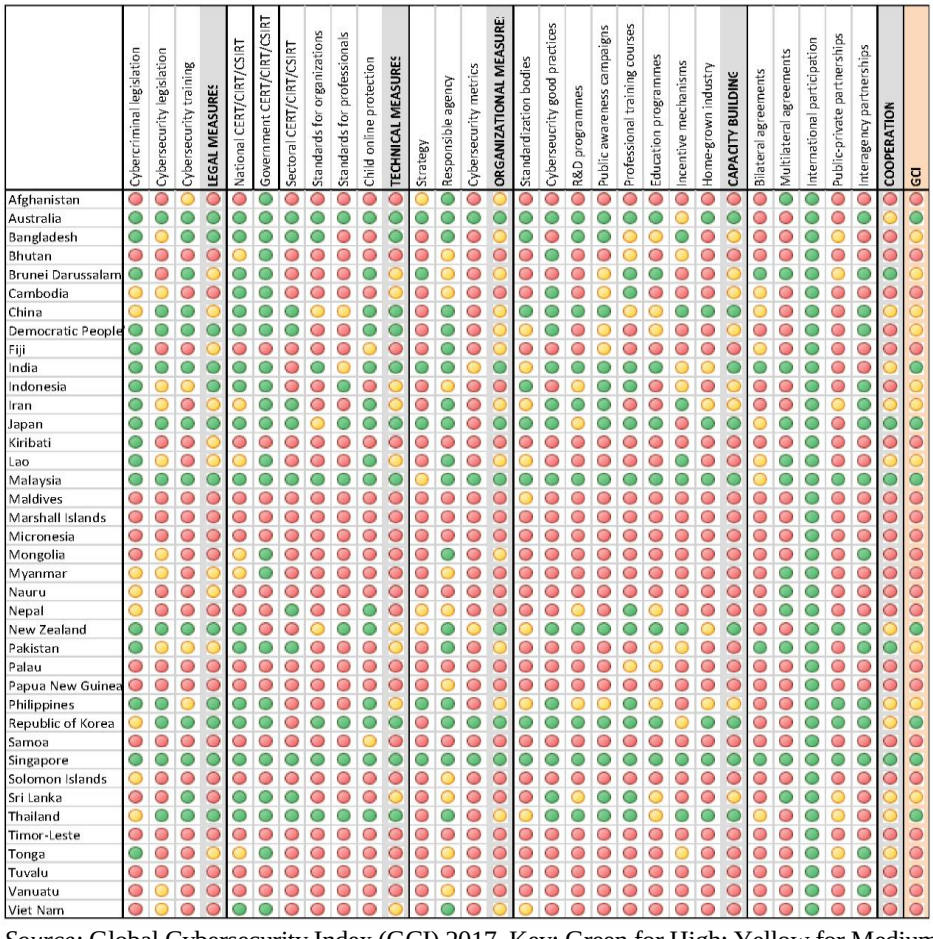
In terms of organisational measures, Pakistan's performance again remains quite poor. While the country formulated Digital Pakistan Policy in 2017, it still does not have a cybersecurity policy or strategy. Moreover, there is no full-fledged agency or department committed to the task of cybersecurity. Rather, the NR3C, a unit of the FIA, deals with cybercrimes. Then, there is a problem of institutional capability. The NR3C is allegedly deficient in resources and facilities to track down the anonymous activities of the hackers.[48] Moreover, Pakistan has some white hat or ethical hackers but their expertise in cybersecurity remain unutilised. Finally, it does not have an effective institutionalised system of coordination among various civil and military agencies dealing with cybersecurity.

Given the transnational nature of cyber threats, cybersecurity is a global challenge and, hence, needs collective and collaborative measures at the international level. To this end, the ITU has so far failed to develop a consensus among member states for a UN-wide framework on cybersecurity. However, it urges the member states to establish regional and multilateral cooperative regimes for information sharing, investigation and prosecution related to cyber offences. In this regard, Pakistan's cyberlaw provides for 'international cooperation.' The country has the membership of the International Multilateral Partnership against Cyber Threats (ITU-IMPACT) and participates in Asia Pacific Security Incident Response Coordination Working Group (APSIRC-WG).[49] However, cybersecurity does not appear as a high priority on the country's agenda for international dialogue and agreements.

[48] Talha Khan, "Cybercrimes: Pakistan Lacks Facilities to Trace Hackers," *Express Tribune*, February 1, 2015, https://tribune.com.pk/story/831178/cybercrimes-pakistan-lacks-facilities-to-trace-hackers/

[49] "Cyber Wellness Profile."

Figure No. 1
Cybersecurity Scorecard: Asia and the Pacific



Source: Global Cybersecurity Index (GCI) 2017, Key: Green for High; Yellow for Medium; Red for Low

Conclusion

The ICT revolution and ubiquity of the internet, experienced by the contemporary world, create plenty of opportunities but pose a great many challenges as well. The fast communications and e-governance yielded by the ICTs are accompanied by various cyber threats ranging from hacking, serious and organised cybercrime and cyber-extremism to cyberwarfare. Pakistan experiences fast growing internet access and deployment of online

administrative and service systems by both public and private organisations. This exposes the country to all aforementioned cyber threats since it confronts a hostile regional and domestic security environment and lacks cybersecurity.

Pakistan falls in the list of those countries which are frequently targeted for espionage. Important Pakistani government websites are often hacked by the Indians who operate in an organised way. Pakistan's banking sector has been facing increasing cybercrime in recent years. Further, Pakistan is potentially vulnerable to the vindictive cyber-attacks by terrorist groups. Most importantly, as the warfare enters the fifth domain — cyberspace — after land, air, sea and space, Pakistan can prospectively face the Indian cyber warfare, particularly given the Indian cyber offence policy, cyber skirmishes between the two countries and the tendency of a sudden outbreak of tensions between them.

The UN-specialised agency ITU, which measures the commitment of states to cybersecurity, categorised Pakistan as a maturing state ranking 66th on GCI of 2017. The country has shown a degree of improvement in legislative measures for cybersecurity but its progress in establishing technical bodies, organisational frameworks, institutional capacity and international cooperation remains lacklustre. Therefore, Pakistan needs to place the objective of cyber preparedness high on policy agenda and undertake extraordinary initiatives towards cyber securitisation. In this regard, the foremost requirement is to formulate a cybersecurity policy which accommodates the prerequisites of both e-governance and cybersecurity. The policy framework for cybersecurity should be holistic and integrated in the sense that it should align the objectives of all concerned economic, administrative and security institutions. Secondly, various security agencies are engaged in cybersecurity activities but lack coordination and cooperation among them.

To address this anomaly, Pakistan needs an integrated institutional framework which interconnects the infrastructures and services of relevant agencies and creates coordination and cooperation among them. Finally, Pakistan should undertake the discourse of technification and awareness about cybersecurity among internet users. The former involves an effective capitalisation on the skilled human resource while the latter involves education and sensitisation of normal individuals regarding cybersecurity.