ADOPTING A STRATEGY OF URGENCY TO ACHIEVE CYBER RESILIENCE

Ali Anjum[*]

Abstract

Cyberspace has emerged as a distinct arena of power contestation. It is increasingly being viewed as a potent instrument capable of advancing "in" and "cross" domain interests of nation-states. National cyber drives by the contemporaries as well as the overt militarisation of this domain have also been covered to reflect the strategic priority of countries while hinting at the potential of cyber threat which exists during peace and war. The paper also presents the national cyber environment which cuts across the civil as well as defence sectors primarily relying upon public indicators and statistics. Like the physical/ traditional spaces of warfighting, cyberspace has also been visualised as a constituent of critical and vital space/ assets falling in corresponding threat zones. Finally, the author suggests quitting the policy of laissez-faire by proposing a framework to overcome existing gaps/ challenges and achieve cyber resilience.

Keywords: Cyber, Security, Defence, Resilience, Pakistan.

Introduction

The term "cyberspace" was first coined in 1982 by Canadian-American author William Gibson as the "creation of a computer network in a world filled with artificially intelligent beings".[1] After its first use in public/ academic sphere, it has gained much more prominence in the recent decades by attiring itself as suited to various authors, organisations and outfits. One of the widely accepted academic precept defines cyberspace as "a time-dependent set of interconnected information systems and human users that interact with these systems".[2] Off late, however, owing to its Omni-present nature, observers have concluded the cyberspace has become a distinct arena of power contestation by various states across the world.

Alongside it, conduct of war in 21st century – curtailed by nuclear deterrence – has also visibly transmuted primarily into non-kinetic domains with cyber as its one of the major critical capabilities.[3] This non-kinetic option has generated an inter-state race to achieve cyber superiority over adversaries,[4] primarily due to evasive legal boundaries,[5] problems of attribution,[6] and cross-domain effects.[7] The capabilities in cyberspace (both defensive and offensive) have thus enabled the states

[*] Ali Anjum is an independent researcher based in Islamabad.

to exercise options beyond physical/ traditional politico-diplomatic cum economic-military spaces and have enabled alternate responses in times of crisis and/or expressing of discontent.[8] Therefore, response options in the cyber domain have afforded undeniable flexibility to the decision makers during the management of the escalation ladder through diversified liberty of action as well as carving an acceptable 'notion of victory'. In this pretext, it is imperative to acquire requisite capabilities in an increasingly important cyberspace, while understanding the contemporary cyber pursuits and domestic threat environment before contemplating a comprehensive national cyber response.

The paper is organised into five sections. After building the requisite background from historical roots to the current potential of cyberspace, a short survey of the contemporary cyber milieu has been presented incorporating various factors including "cyber governance/command & control", "cyber resilience", and the perceived peculiarity of each nation-state. Thereafter, Pakistan's domestic cyber environment is covered at length. It reflects qualitative/quantitative facts before summarising existing gaps – at policy, organisations, legal and technical levels – inhibiting suitable national cyber response. Next, threat actors have been enumerated before presenting a national cyber terrain vis-a-vis the threat environment. This cyber terrain has been developed based on cross-domain knowledge and is expected to serve as a guide to appreciate cyber threats as well as mounting suitable responses. Lastly, a strategy of urgency is advocated at the national level to overcome existing gaps and harmonize/consolidate the national cyber response in the final section.

Contemporary Cyber Milieu – A Short Survey

Global cyberspace has become competitive due to its vast cross-domain potential and a race towards achieving cyber superiority over others.[9] In this context, it is vital to understand the undertakings of important regional and global powers to sift international best practices as well as the latest trends in cyber governance and command & control.

United Kingdom. With deeply entrenched public awareness/consciousness of data privacy/security, the UK tops the global cyber security ranking. The national framework, however, is decentralised defensive to expand the responsibility as much as possible keeping in view the character of cyberspace but accumulating the best national cyber offensive potential at one place for the conduct of centralised operations. In a literature survey, involving number of cyber ready countries, only the UK has publicly disclosed the restraints on its cyber operations from the perspective of human/ethical values. Moreover, London also claims for noncollaborative conduct in cyberspace which demonstrates high moral standing of English society in such a non-regulated space. Since 2020, National Cyber Force (NCF) of the UK is a centralised offensive component which has elements of MI-6, Ministry of Defence, and General Communications Headquarters. It is mandated to conduct operations against threat actors which cause disruption as well as prevent terrorism.[10]

United States of America. Being the leader in innovation and application, its national framework is decentralised responsibility for defensive and offensive operations. Although decentralisation of defensive cyber is a forgone conclusion, the distributed responsibility for the conduct of offensive operations stems from its latest acclaimed Cyber Deterrence Initiative.[12] Raised in 2010, US Cyber Command is one of the eleven unified combat commands of the US Department of Defence headed by a General Officer with a mandate of conducting full-spectrum cyber operations globally in real-time against adversaries. In an overall Global Cyber Security Index, the US remains at 2nd place, only after the UK.

China. Beijing has a peculiar national framework for cyberspace i.e., extremely centralised in both visibility of defensive operations as well as the conduct of offensive operations. President of China is the competent authority who exercises power through Cyber Space Administration of China (CAC).[11] Its tiered provincial-level administrations have taken China to the modest cyber security ranking of 27th. While China is perceived to prioritise civil targets over military due to their inherently less escalatory nature, it has not expressed any offensive cyber operation against the potential adversaries till date. The People Liberation Army Strategic Support Force (PLASSF) is unified space/cyber force headed by a General Officer since 2015 which conducts intelligence, technical reconnaissance, electronic countermeasures, cyber operations, and psychological warfare.[12] With a highly unified information warfare strategy, China appears to be the only country which is perceived to have a cyber-capability which can be exercised wirelessly through electronic warfare means.

Russia. Russia has a national cyber framework which is decentralised defensive and centralised offensive operations. Being the primary adversary/threat for the West in the aftermath of cyber interactions in the last decade, Kremlin is alleged to have hired services of private firms to advance/conduct trans-frontier cyber operations giving rise to the notion of 'cyber terrorism'.[13] Moscow's famous Information Operations Troops (of General Staff Branch Directorate) are responsible for conducting full spectrum cyber operations since 2014 including mandate of protecting Russia's military computer networks from cyber-attacks.[14] The incident of Snowden leaks in 2014 is considered a watershed moment in cyberspace after which the Eastern part of the world also commenced their cyber initiative in response to NSA's alleged espionage ventures.[15]

Israel. Israel sits at the crossroads of east and west. It leverages its position and strategic relationship with a range of global/regional powers. It also promotes itself as the victim of alleged cyberterrorism. Its cyber security culture as well as power is considered second to none and enjoys the extra-rich collaboration between the defence and civil cyber sectors. Tel-Aviv has a national cyber design which is centralised technical control and decentralised execution of offensive and defensive operations. With an advantage of high-grade intelligence and collaboration, it takes at its credit – albeit wittingly – the success of 'Stuxnet' attacks against Iranian nuclear facilities along with the US.[16] The recent controversy of leveraging "Pegasus Spyware" for advancing political cum economic interests reflects that Israel is well ahead in the global cyber competition.[17] At defence forces level, its General Staff (C^4I & Cyber Directorate) is functional since 2010 and has the responsibility for the defence of military assets, whereas Military Intelligence Directorate and Mossad enjoy the mandate for the conduct of offensive operations. Its current cyber security ranking of 39 is considered biased given its defensive and offensive cyber capabilities acknowledged across the globe.

India. In an overall construct, national framework for Indian cyberspace is decentralised defensive and centralised offensive operations. As of today, while Delhi is vigorously advancing its cyber collaborations within QUAD alliance as well as other technologically advanced countries,[18] it has the advantage of leveraging its position in the region for focused US collaboration in the cyber domain.[19] India has recently established Defence Cyber Agency (DCA) in 2021 which works at the tri-services level to integrate space/cyber/special forces effects in the overall framework of 5th generation warfare.[20] This tri-services agency is not only responsible for monitoring/responding to cyber breaches, it also has the mandate for conducting offensive operations. Although India stands at the cyber security index of 47, its current endeavours and rich human resource potential is bound to enhance its cyber potential in medium to long term.[21]

In a nutshell, although strategic national culture has always remained important in understanding a country's behaviour in a given environment, it however has attained added significance while measuring the efficacy of national cyber resilience/response and their attained cyber security indices.

Where Does Pakistan Stand in Cyber Conglomerate?

From the beginning of the twenty-first century, worldwide public-private partnerships have revolutionised the utilisation of cyberspace. Off late, Pakistan has also made significant progress in the realms of information technology (IT). Broad contours of the domestic cyber environment are explained in the ensuing paragraphs. At the strategic level, there are multiple states mainly China, Afghanistan, and Iran which partially depend on the internet backbone passing through Pakistan. Moreover, China's PEACE cable which runs from Western Europe to Southern Africa also passes through Pakistan. On the other hand, Pakistan itself is connected to the international internet traffic grid through half a dozen sub-sea cables. As of today, tele-density lies at 85%, ranking 67th in the world, wherein 189 million people use mobile phones. Among mobile phone users, 108 million are 3G & 4G subscribers, whereas 110 million are broadband subscribers. The estimated social media outreach in Pakistan is 70-75 million.[22] In parallel, numerous government organisations rely on internet to render services to masses. These organisations include departments dealing with heavy repositories/caches of data which may have significant value in the national security paradigm. A case in point is NADRA which maintains the digital footprint for the entire population. State Bank of Pakistan, besides dealing with digital transactions, is advancing a regulatory framework for 'Digital Bank' aiming at growing e-commerce to USD 1 billion by end of 2022. Other core governmental online services marking use of internet includes safe city projects, cash disbursements, verification services and e-filing of tax returns etc. On the other hand, in military domain, communication and surveillance platforms are also partially dependent on internet services. Taking a lead from Army's great initiative of digitisation at the turn of 21st century, the military is aiming at achieving net-enabled cap by 2025 including automation of battlefield management to achieve optimal efficiency in fighting future wars. This brief stocktaking of existing national cyber eco-system demonstrates the increasing and indispensable reliance of civil as well as defence sector on information, communication, and technology (ICT) systems operating in various threat zones of cyberspace. Therefore, the efforts for 'Digital Pakistan' warrants identification of vulnerabilities/gaps and threat assessment to mount suitable response.

Vulnerabilities and Gaps

Expansion of IT sector has revolutionised the national cyber spectrum since the turn of century. The focus, however, remained on ICT services. Commensurate cyber security safeguards were not put in place, further adding to cyber vulnerabilities at national level. Contrary to global best practices, Pakistan's efforts in achieving cyber protection remained fragmentary, thus lacking cohesiveness. Major vulnerabilities/gaps have been covered in ensuing paragraphs.

Pakistan has been declared least committed country in Asia Pacific on cyber security, ranking 67th in World Cyber Security Index.[23] Even till-date, cyber security is not accorded high priority, whereas regional and global powers have kept cyber security in a list of top priority. Moreover, cyber security seldom figures out in Pakistan's strategic security calculus. The national cyber security flag-bearer, i.e., National Telecommunication and Information Security Board (NTISB) have also not demonstrated the drive and capacity to undertake warranted initiatives. Furthermore, ICT industries adopt different perspective on cyber security. In parallel, however, Ministry of Defence is reported to have made steady progress owing to sensitivities annexed with defence related to its ICT systems. Amid transformation of IT sector, reliance on internet has increased. Bulk of equipment/technology/software comes from foreign countries. Majority of data services are provided by foreign servers which also include webhosting of governmental websites.

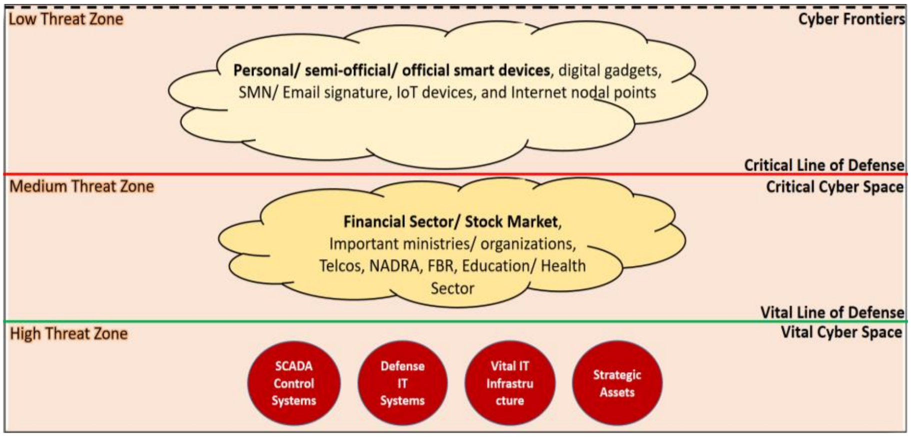
Presently, Pakistan does not possess state owned telecommunication equipment as well as operations. The situation has been further exacerbated by non-indigenous social media network (SMN) platforms. With meagre internet monitoring mechanism, Pakistan is clearly lacking the required capacity to respond to cyber breaches/attacks. On top of it, the country also lacks requisite strategic culture of awareness further complicating the overall cyber situation. The gamut appraisal of cyber situation thus reveals the lacklustre cybersecurity apparatus and response of Pakistan at national level primarily due to lack of synergy at interorganisational level. Summarily, as of today, Pakistan is less configured to offer a coherent response against prevailing cyber threat spectrum.

At the policy and strategic level, there is a lack of national direction as cyberspace is not a focus area in the national security policy of Pakistan. Also, there exist regulation and compliance inadequacies including data protection, identification of critical/vital IT infrastructure. At the organisational level, there is absence of national and effective sectoral cyber security authority/organisations and non-existence of national information assurance centre. It is worth mentioning that Air University Islamabad has established a national "Cyber Centre of Excellence'. In the legal domain, criminal legislation exists (including IFTA-2013, and PECA-2016) but adequate technical implementation framework is lacking[28]. Cybercriminals operate undeterred due to ineffective prosecution. Promulgated SMN rules are often challenged in courts. On the technical side, there is absence of national internet filtering mechanism and control over internet services. Fragile/fragmented defensive response against cyber breaches at national and sectoral level. Although national cyber response centre is in the process of raising, sectoral cyber response mechanisms, however, are functional in relative isolation and working without required synergy.[29] The national security standards are also not standardised. There is limited digital forensics capability and technical auditing through Pakistan Forensics Science Agency (PFSA) as well as limited indigenous capability for development of secure equipment.

National Cyber Threat Assessment

Taking stock of the national cyber environment, major cyber threat actors appear to be nation-states. However, cyber criminals, hacktivists, terrorist groups and thrill-seekers add to the mosaic, thereby complicating the threat landscape. Corresponding motivations for these additional actors also range from geopolitics to secure financial gains including ideological vengeance and/or spread satisfaction or discontent.

Appreciating cyber threats have always remained a challenge for the policy makers and strategists – mainly due to opaqueness of threat actors' vis-a-vis the magnitude/intensity of cyber breaches. Moreover, chief characteristics of a cyber-threat actor remains non-attribution amid poorly regulated/prosecuted cyberspace. Owing to these constraints, subjective (rather than objective) effort has been made to crystallise national cyber terrain from the perspective of targets rather than threat actors – impelled from the effects rather than the ways and means employed. Developed canvass has been kept close to the concepts of physical space (see figure below) for easy assimilation at appropriate level.


Low Threat Zone
Cyber Frontiers
Personal/ semi-official/ official smart devices, digital gadgets, SMN/ Email signature, IoT devices, and Internet nodal points
Critical Line of Defense
Medium Threat Zone
Critical Cyber Space
Financial Sector/ Stock Market, Important ministries/ organizations, Telcos, NADRA, FBR, Education/ Health Sector
Vital Line of Defense
High Threat Zone
Vital Cyber Space
SCADA Control Systems
Defense IT Systems
Vital IT Infrastru cture
Strategic Assets

Visualization of Cyber Terrain vis-a-vis Threat

The emerging national cyber threat landscape has been visualised in three distinct zones with boundaries delineated in the form of "cyber frontiers", "critical line of defence" and "vital line of defence". They have been labelled as low/medium/high threat zones from the perspective of state – which may be taken as a guideline and can differ as per the applicability environment. It may also be noted that these threat zones have been depicted in depth to create semblance with traditional spaces of warfighting. It is also important to note of national critical and vital cyberspaces (vis-a-vis threat zones) and spread of corresponding public, private and defence sector entities.

Proposed National Cyber Initiative

While Pakistan has done relatively well to deal with the threats in vital cyberspace, requisite defensive measures are found inadequate against low and medium zone threats. The eastern neighbour has adequate cyber offensive potential – augmented by its strategic collaboration with technologically advanced countries - which can be employed for subversive and disruptive actions against Pakistan. On the other hand, Pakistan also presents a rich attack surface due to absence of required strategic culture leaving its ICT infrastructure extremely vulnerable. Lack of indigenization, increasing reliance/ dependence on foreign origin ICT equipment, and absence of potent accreditation laboratories add more risk to already fragile cyber security situation in the country. The decision-makers at the national level cannot therefore afford to continue the policy of laissez-faire amid obtaining national cyber environment, which is indeed grim. Existing gaps and vulnerabilities juxtaposed with evolving threat mosaic merits adoption of strategy which must prioritise the prevalent risks posed to national security in cyberspace.

Strategy - From Pendency to Urgency

The nature of cyberspace is primarily non-lethal. A breach or an ingress by a threat actor remains mostly unobserved especially when the target lacks cyber sense and is not aware of adversarial designs/motives. On the other hand, threat actors with various motives frequently remain in a state of contact/maintain ingress in the national critical/vital cyber assets (shown in the above figure) for espionage only without having any fear of accountability. Therefore, the policymakers at large are not fully aware of the consequences or at best are reluctant to accord priority to the domain of cyber security. This paper argues to follow the "strategy of urgency" (instead of pendency) and undertake tiered initiatives to achieve desired goals.

National Level

To commence a national cyber drive, constitutional make-up is a must to augment/formulate a framework for national cyber governance and steer its execution/implementation. Therefore, the establishment of a 'Cyber Command Authority' (CCA) is suggested at the national level which may be chaired by a technocrat. While the head of the proposed CCA is suggested to be part of the 'National Command Authority' (NCA), a dedicated national cyber security advisor is also recommended to bridge the governmental-organisational gap. Further, CCA is suggested to take charge of the cybersecurity of entire civil (public and private entities) as well as defence sectors. Next, NTISB (an already existing organ) should be mandated to take charge of public sector outfits, whereas a separate organisation is recommended to be raised for ensuring the cyber resilience of critical private sector entities. On the other hand, the defence sector should also be reconfigured to include a tri-services cyber directorate responsible to offer comprehensive response against evolving cyber threats against armed forces. The CCA is recommended to undertake the following major tasks:

- Formulating and updating national cyber security policy/strategy and ensuring its implementation.
- Strategizing response to improve cybersecurity in low, medium, and high threat zones.
- Identifying gaps between desired ends and existing means by allocating required resources.
- Lead national cyber eco-system and meet the critical deficiencies in legal, technical and enforcement domains.
- Harmonising existing cyber defences in national critical and vital cyberspace in the short to medium term through under-command cybersecurity organisations.
- Formulate threat intelligence sharing mechanism between civil (both public and private entities) and defence sectors.
- Enhance visibility and seek improvement in national cyber security by establishing dedicated national/regional cyber security nerve centres to identify threats and generate suitable responses.
- Maintain a national catalogue of cyber vulnerabilities/threats and share details of breaches/cyber-attacks horizontally and vertically.
- Representation from and capacity building of Federal Investigation Authority (FIA) to undertake advance forensics augmenting effective prosecution.

- Pursue strategic collaboration (not alliance) with friendly countries in the cyber domain while carefully managing the cross-domain ramifications.
- Maintain a reserved seat for academia to enable/promote research and development in cyberspace through a public-private partnership aimed at the indigenisation of ICTs.
- Improving national awareness through electronic/SMNs as well as special documentaries to adopt a whole-of-society approach.
- Mobilise and pursue the regulation of cyberspace at appropriate global and regional forums.
- Forecast and meet the requirement of human/technical resources for the cybersecurity industry.

Civil Sector Level

The civil sector is primarily divided into public and private entities. A reconfigured NTISB and a newly raised private sector cyber setup should endeavour to overhaul cyber defences in national critical cyberspace. CCA is expected to assign the following tasks for the cyber resilience of its civil sector:

- NTISB to take the lead of public sector entities including government ministries and diplomatic offices, both inland and abroad.
- Private sector cyber setup to take charge of critical private sector outfits including financial, industrial, power/energy subsectors.
- Establishment of sector/subsector/organisational level cyber security nerve centres to identify threats and generate responses with an additional task to regulate/manage and influence cybersecurity.
- Engagement with all relevant stakeholders falling in national critical cyberspace to improve their organisational cyber awareness, identify the vulnerabilities, and advise/ensure necessary cybersecurity measures.

Defence Sector Level

A tri-services cyber directorate is expected to undertake the following tasks:

- Fill the existing gaps/voids in national vital cyberspace.
- Coordinate and advise improvement in cyber security of IT assets of each service/strategic organisation forming part of vital cyberspace including the defence industry.

- Capacity building for reliable hunt of backdoors (soft and hard) in the procured equipment/weapon platforms.
- Interface with the education sector to meet the technical requirements by using indigenous resources, as far as possible.
- Develop and harness the potential of emerging technologies.

Conclusion

Cyber power is indispensable to exerting cyber sovereignty. Off late, as 5th dimension of war, this power potential has actualised in several active military engagements. While nations and militaries are striving for force multipliers, cyber power has not only emerged as a force multiplier but also an enabler of primary non-kinetic response. Advancements, collaborations, and capabilities of contemporaries when viewed in the backdrop of prevailing cyber terrain reveal the risks posed by vulnerabilities and gaps in Pakistan's current cyber eco-system. Overcoming existing challenges in cyberspace is indeed an uphill task. However, if appropriate initiatives are taken at the national, sectoral, and institutional levels, Pakistan can reap the desired effects and advance its interests by leveraging the required cyber capabilities during peace and war.

References

[1] Benedikt, Michael, ed. Cyberspace: first steps. Mit Press, 1991.

[2] Sohrabi, Babak, Iman Raeesi Vanani, and Mohsen Baranizade Shineh. "Topic modeling and classification of cyberspace papers using text mining." Journal of Cyberspace Studies 2, no. 1 (2018): 103-125.

[3] Bachmann, Sascha-Dominik. "Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats-mapping the new frontier of global risk and security management." Amicus Curiae 88 (2011): 24.

[4] Klimburg, Alexander. "Mobilising cyber power." Survival 53, no. 1 (2011): 41-60.

[5] Trimble, Marketa. "The future of cybertravel: legal implications of the evasion of geolocation." Fordham Intell. Prop. Media & Ent. LJ 22 (2011): 567.

[6] Hare, Forrest. "The significance of attribution to cyberspace coercion: A political perspective." In 2012 4th International Conference on Cyber Conflict (CYCON 2012), pp. 115. IEEE, 2012.

[7] Gartzke, Erik, Jon Lindsay, and Michael Nacht. "Cross-Domain Deterrence: Strategy in an Era of Complexity." In International Studies Association Annual Meeting, Toronto. 2014. 9 Schmitt, Michael N., and Liis Vihul. "Proxy wars in cyberspace: the evolving international law of attribution." Fletcher Sec. Rev. 1 (2014): 53.

[8] Limnéll, Jarno. "The cyber arms race is accelerating—what are the consequences?" Journal of Cyber Policy 1, no. 1 (2016): 50-60.

[9] International Institute for Strategic Studies. "Cyber Capabilities and National Power A Net Assessment." (2021).

[10] Rodriguez, Roberto Miguel. "Comparison of NASA and the China National Space Administration." (2010).

[11] Kania, Elsa B. , and John Costello. "Seizing the commanding heights: the PLA Strategic Support Force in Chinese military power." Journal of Strategic Studies 44, no. 2 (2021): 218-264.

[12] Herzog, Stephen. "Revisiting the Estonian cyber-attacks: Digital threats and multinational responses." Journal of Strategic Security 4, no. 2 (2011): 49-60.

[13] Giles, Keir. ""lnformation Troops"-A Russian Cyber Command?" In 20113rd International Conference on Cyber Conflict, pp. 1-16. IEEE, 2011.

[14] Dencik, Lina, and Jonathan Cable. "The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks." International Journal of Communication 11 (2017): 763-781.

[15] Kliem, Frederick. "Why Quasi-Alliances Will Persist in the Indo-Pacific? The Fall and Rise of the Quad." Journal of Asian Security and International Affairs 7, no. 3 (2020): 271-304.

[16] Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to operations in 45 countries. 2018.

[17] Mahmood, Khalid. "Attitudes towards the internet: a survey of LIS professionals in Pakistan." Library Philosophy and Practice 2010 (2010): 1-10.

[18] Khan, Mahrukh. "Growing India-US strategic cooperation." Strategic Studies 37, no. 4 (2017): 97-117.

[19] Mohan, Pulkit. Ensuring Cyber Security in India's Nuclear Systems. Observer Research Foundation, 2020.

[20] Kong, Eric, Doren Chadee, and Revti Raman. "Managing Indian IT professionals for global competitiveness: the role of human resource practices in developing knowledge and learning capabilities for innovation." Knowledge Management Research & Practice 11, no. 4 (2013): 334-345.

[21] Chen, Thomas M. "Stuxnet, the real start of cyber warfare? [Editor's Note]." IEEE Network 24, no. 6 (2010): 2-3.

[22] Rafiq, Aamna. "Challenges of securitising cyberspace in Pakistan." Strategic Studies 39, no. 1 (2019): 90-101.

[23] Bashir, Sobia, and Faisal Shahzad. "Federal Investigation Agency against the Crime of Book Piracy in Pakistan." (2021).