LESSONS LEARNED FROM 2020 AND CYBERSECURITY OUTLOOK FOR PAKISTAN IN 2021

FAROOQ NAIYER

What a momentous and "eventful" year 2020 has turned out to be. On top of the cyclical changes in technology and threats, a global pandemic has turned life upside down for businesses, governments, and consumers around the world.[1]

Anchored in changing reality societies strived for 'normalcy' via entire families logging in remotely, trying to keep school and work going. This tested the limits of what a home office could sustain. The privacy and security of a fully remote world was put front and center. With this in perspective, this paper dissects few cybersecurity highlights that had an impact across various sectors in Pakistan and looks at what potentially lies ahead in 2021.

There has been a noticeable uptick in cybercrime towards healthcare, education, municipal, and utilities sectors and other chronically understaffed and overburdened public institutions.[2] This is different from targeting large government entities and corporations, many of whom have resigned themselves to being targeted by state and non-state actors and can try to protect themselves from that onslaught. It is a different matter entirely when the targets are schoolchildren, or just ordinary people trying to go about their daily lives. Therefore, ransomware epidemic will continue during 2021, as the practice remains lucrative, relatively easy, and risk-free.

While cyber criminals are relatively predictable in their tendency to always choose the path of least resistance, the activities of nation-states are frequently more relentless and sophisticated — and as a result, more challenging for incident responders. More importantly cyber-attacks and covert use of cyber capabilities by nation-states have the potential to spark a major international incident. If there is one thing, nation-states and their policy-makers have learned from the exponential increase in cyber threats is that there has never been a better time to get involved in cybersecurity. The stakes are high and rising every day. Cyber defence is not a matter of choice for nations any more, it rather has to be an essential part of the national defence strategy.

[1] Irfan Mahar, "Impact of Covid-19 on Global Economy Structure," *Modern Diplomacy* (blog), April 22, 2020, https://moderndiplomacy.eu/2020/04/22/impact-of-covid-19-on-global-economy-structure/.

[2] Imran Mukhtar, "Pakistan Witnesses Rise in Cyber, Online Crimes," *The Nation*, October 29, 2020, sec. National, https://nation.com.pk/29-Oct-2020/pakistan-witnesses-rise-in-cyber-online-crimes.

Pakistan's Cybersecurity Readiness

The Global Cybersecurity Index (GCI)[3] measures the commitment of countries across the world to cyber security. The GCI was released in the first quarter of 2020 by the UN telecommunications agency International Telecommunication Union (ITU). The ranking was based on countries' legal, technical and organisational institutions, their educational and research capabilities, and their cooperation in information-sharing networks.

Meanwhile, the National Cyber Security Index (NCSI) is a global index,[4] which measures the preparedness of countries to prevent cyber threats and manage cyber incidents. The NCSI is also a database with publicly available evidence materials and a tool for national cyber security capacity building. The indicators of the NCSI have been developed according to the national cyber security framework. The fundamental cyber threats are:

1. Denial of e-services – services are not accessible
2. Data integrity breach – unauthorized modification
3. Data confidentiality breach – secrecy is exposed e

These threats directly affect the normal functioning of national information and communication systems and, through the ICT systems, electronic services (including critical e-services).To manage these cyber threats, a country must have appropriate capacities for baseline cyber security, incident management, and general cyber security development.

Out of the 160 countries assessed, Pakistan was ranked 66th with a national cybersecurity index of 42.86.[5] An Asian county to grab the highest rank was Singapore at 15th place. It is important to note that Pakistan had scored high in the areas of education and professional development, e-Identification and trust services, protection of personal data and fight against cybercrime. This can be attributed to the role that academia has played in offering certifications, diplomas, graduate and post-graduate programs in cyberssecurity and the work done by National Centre for Cyber Security (NCCS)[6] in the area of research and product development in cyber security. The role of Federal Investigation Agency's National Response Centre for Cyber

[3] "Global Cybersecurity Index," ITU, October 4, 2019, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

[4] "National Cyber Security Index", *e-Governance Academy Foundation*, n.d. https://ncsi.ega.ee/ncsi-index/

[5] "National Cyber Security Index: Pakistan's Rank," NSCI, accessed January 4, 2021, https://ncsi.ega.ee/country/pk/.

[6] "National Center for Cyber Security | Pakistan," NCCS, accessed January 4, 2021, https://www.nccs.pk/.

s

Crime (N3C) and Pakistan Telecommunications Authority (PTA) has been key in countering cyber-crime in Pakistan. Last but not the least the role of the National Database Registration Authority (NADRA) and FIA in e-identification and trust services has to be acknowledged.

The weak areas were cybersecurity policy development, cyberthreat analysis and information, protection of digital services and military cyber operations. This is tied in with the absence of a cybersecurity directorate/national Computer Emergency Response Team (CERT) in Pakistan.

Geopolitical Situation in South Asia

On August 5, 2019, India's Modi government revoked Article 370 of the nation's constitution,[7] thereby stripping the relative political autonomy that the occupied region of Jammu and Kashmir was exercising for seven decades. This action, assessed to be a significant deviation from the status quo, immediately preceded an increase in targeted intrusion activity from adversaries linked to India and Pakistan.

Next, in August 2020, Pakistani intelligence agencies tracked a major security breach by Indian hackers whereby phones and other gadgets of government officials and military personnel were targeted.[8] According to a statement by the Inter-Services Public Relations (ISPR), the cyber-attack by Indian intelligence agencies involved "a range of cybercrimes including deceitful fabrication by hacking personal mobiles and technical gadgets". Military's media wing stated that "various targets of hostile intelligence agencies are being investigated", while "Pakistan Army has further enhanced necessary measures to thwart such activities including action against violators of standing operating procedures (SOPs) on cybersecurity."

India happens to be the largest buyer of Israeli weapons and the current government of India is committed to consolidate the relationship further.[9] In 2020 India and Israel signed a Memorandum of Understanding to expand cooperation in cyber security to counter the challenges that might arise due to rapid digitization amid COVID-19. This

[7] "Article 370: What Happened with Kashmir and Why It Matters," *BBC News*, August 5, 2019, 370, https://www.bbc.com/news/world-asia-india-49234708.

[8] Naveed Siddiqui, "Indian Cyber Attack Targeting Gadgets of Govt Officials, Military Personnel Identified: ISPR," *DAWN* (blog), August 12, 2020, https://www.dawn.com/news/1574034.

[9] Zen Read, "Israel's Largest Arms Clients: India, Azerbaijan and Vietnam," *Haaretz*, March 15, 2018, https://www.haaretz.com/israel-news/israel-s-largest-arms-clients-india-azerbaijan-and-vietnam-1.5909811.

cooperation in cyber field has a high probability of developing into a strategic partnership in cyberspace as Israel is an established leader in international cyber landscape and India has much to gain from its advanced cyber capabilities. Similarly, the initiation of a new cold war between United States and China may push the United States (which again is a cyber-security partner of India) to support India as a counterweight to China in cyberspace.[10] The on-going military crisis between India and China has also opened avenues for cyber war between the 2 nations. A recent investigation by an Indian English language newspaper *The Indian Express* revealed that China is monitoring the online activities of at least 1,350 Indians, including key politicians and some high-profile individuals in the country. The list includes former presidents, prime ministers, and key businessmen.

Significant Cybersecurity Events in Pakistan in 2020

2020 was the year when record number of data breaches were reported. Though many countries that are ranked high on the national cybersecurity index also fell victim to them, Pakistan also had its share, though there are disputes on the currency and authenticity of the data.

Given the steep increase in phishing attacks by 600% globally; Pakistan also saw a dramatic increase in phishing campaigns posing to be from banks, NADRA, and other national and provincial organisations for harvesting personal identifiable information or duping users to send funds transfers or mobile top-ups.

In April 2020, a leading cybersecurity firm in Pakistan reported that it had discovered a data dump of 115 million Pakistani mobile users' data that had shown up for sale on the dark web.[11] The cyber-criminal behind this data breach had demanded 300 BTC (USD2.1 million) for the data. This indicated that financially motivated threat actors are active in Pakistan and organizations are becoming a victim of these cyber-attacks. The firm also mentioned that their team had analyzed the samples of the data dump that has been released on a popular dark web forum. The stolen data included users' personal details, such as full name, complete address, mobile numbers as well as national identification numbers. This claim was later investigated by

[10] Cheena Kapoor, "Military Standoff Apart, India, China Brace up for Cyber-Warfare," Anadolu Agency, September 18, 2020, https://www.aa.com.tr/en/asia-pacific/military-standoff-apart-india-china-brace-up-for-cyber warfare-/1977635.

[11] Iftikhar A. Khan, "FIA Asked to Probe 'Data Breach of 115m Mobile Users,'" DAWN, April 12, 2020, https://www.dawn.com/news/1548536.

PTA and FIA, however, no conclusive report was published in the public domain.

In September, 2020 K-Electric Pakistan's largest private power company suffered a Netwalker ransomware attack that disrupted online billing services, but not the supply of power. Soon afterwards, a leading cyber security company managed to obtain access to the Tor ransom payment page for K-Electric's attack, where ransomware operators demanded a USD 3,850,000 payment. The attackers also stated that they would release files stolen during the attack if the ransom was not paid. The Netwalker gang went ahead and released the data after their ransom demands were not met. A Pakistani cybersecurity firm which examined the archive contents, reported that it contained sensitive information like financial data, customer information, engineering reports, maintenance logs, and more. However, this breach was denied by K-Electric.

In November, 2020 access to Pakistan International Airlines' (PIA) internal network and customer database was up for sale on the dark web.[12] This information was confirmed by multiple cyber security news feeds. The hackers who were from Russia had offered to sell access to the internal network and customer database of PIA. The cybercriminals advertised domain admin access to PIA's internal network for USD 4000, while its customer database was listed for USD500. The purported hacker posted the advert for initial network access to PIA's systems on Russian and English dark web marketplace forums. A week later the airline's customer database went up for sale. The hacker's post in the forums stated that the database included customers' full names, phone numbers, and passport information. The airline has not acknowledged the breach incident, so far.

Disinformation Campaign by India and 5th Generation Warfare

In December 2020 a Europe based non-governmental organization, EU-DisinfoLab, released its second report on the goldmine of India's vast disinformation network. It, inter alia, revealed that a dead human-rights professor Louis Sohno, who died in 2006, and numerous defunct organisations were resurrected. They were used alongside at least 750 fake media outlets in a vast 15-year long

[12] Soumik Ghosh, "Pakistan International Airlines Data Breach Underscores Sharp Rise in Illicit Sales of Access Credentials," *CSO Online* (blog), November 20, 2020, https://www.csoonline.com/article/3598012/pakistan-international-airlines-data-breach-underscores sharp-rise-in-illicit-sales-of-access-crede.html.

global disinformation campaign to advance Indian interests.[13]

Upon further investigation, the disinformation watchdog found that they had suspicious links to a large network of think tanks, Non-Governmental Organisations, and fake news websites in over 65 countries. The network worked round-the-clock to create a 'mirage' of anti-Pakistan perceptions by influencing thought-leaders, policy-makers, international organisation, as well as the public at large. Srivastava Group of India sponsored this fake, dis-information network in 65 countries, including the US, Canada, Belgium, and Switzerland. The Group published *New Delhi Times* and *Times of Geneva Online* besides running a website "4newsagency.com".

The fake think tanks include, International Institute for Non-Aligned Studies, Women are Economic and Social Think Tank, the South Asia Democracy Forum, and Friends of Gilgit-Baltistan. Made Sharma ran outfits with just two administrative full-timers with no experts on South Asia actually ever employed by the network. Ms. Sharma, who posed as a self-styled 'international business broker', paid for the travel and accommodation of an unofficial far-right delegation of 23 European Union parliamentarians to Srinagar, on October 30, 2013. She was photographed with PM Modi along with other EU Parliamentarians who made the trip to Indian occupied Kashmir.

A fake Canadian think-tank

Think tanks and journalists of doubtful credentials spearhead India's worldwide disinformation campaign against Pakistan and China. For instance, Macdonald-Laurier Institute, a registered Canadian charity, is in the forefront. It published a Pakistan-bashing report 'Khalistan—A project of Pakistan' [14] which found mention in almost all leading Indian newspapers. The social-democratic Broadbent Institute (a think-tank on the political left) referred to the MacDonald-Laurier Institute as a 'right-wing charity'. The institute was established in 2010 as a registered charity funded by corporate and individual donors, including disguised pro-Indian lobbyists. Its political orientation is evident from the fact that it is named after two Canadian Prime ministers Sir John A. Macdonald and Sir Wilfrid Laurier.

[13] Zahoor Khan Marwat, "Indian Disinformation Campaign against Pakistan," *The News*, December 14, 2020, https://www.thenews.com.pk/print/758216 indian-disinformation-campaign-against-pakistan.

[14] "Statement on Criticism Regarding "Khalistan: A Project of Pakistan"," Macdonald-Laurier Institute, September 25, 2020, https://www.macdonaldlaurier.ca/statement-criticism-regarding-khalistan-project-pakistan/.

Another pro-India "think-tank" is the "International Terrorism Observatory" chaired by Roland Jacquard. Prestigious French newspaper *Le Monde* (The World) pointed out in 2015, 'he is the only member "without publications, without a website, without postal address, and without any legal existence".[15] He runs a bookstore stacked with books on 'Networks of Islamist terrorism'.

Future outlook and changing geopolitical situation

The changing geopolitical situation in the Middle East with various Arab nations now recognising Israel and developing better relations with it may have a trickle-down effect on Pakistan. As recently as May 2020, Israel claimed that they thwarted an attempted cyberattack on its water facilities,[16] with Iran believed to be the origin point. Israel responded with a substantial cyberattack on Iranian port facilities, causing chaos, malfunction, and limited infrastructural damage.

On the southeast Asia front, the geo-political situation has evolved a lot given the fact that China now has hostilities with India which did result in armed clashes in the Ladakh region. Moreover, the increased hostilities between China and certain Western countries have resulted in China being accused of targeting the defense and healthcare sectors of North America and South Asia.

Given the fact that the CPEC projects have taken off in Pakistan; this has led to adversaries planning to cause all kinds of hurdles and disruptions in the cyberspace and beyond.[17] China's plan to develop a 'Digital Silk Road' will also attract the attention of various adversaries. This initiative aims to broaden and deepen digital connections to other nations via the construction of cross-border and submarine optical cables, communication trunks and satellite information passageways, and the development of 5G networks.

For the 5G two aspects are important for policy-makers: First, is the understanding about who is providing the equipment for the rollout; and secondly, if there are any risks that must be mitigated against during the

[15] Amjed Jaaved, "India's Disinformation Campaign," *The Nation* (blog), October 11, 2020, https://nation.com.pk/12-Oct-2020/india-s-disinformation-campaign.

[16] "Cyber Attack Targets Israel's Water Supply – Analysis & Mitigation | Radiflow," Radiflow, accessed January 4, 2021, https://radiflow.com/blog/cyber-attack-targets-israels-water-supply/.

[17] Irteza Hassham and Priyanka Essrani, "Stimulation Of Cyber Security And CPEC," Technology Times, August 30, 2020, https://www.technologytimes.pk/2020/08/30/stimulation-of-cyber-security-and-cpec/.

rollout. Meanwhile, there are five ways in which 5G networks are more vulnerable to cyberattacks than their predecessors:

1. The networks have moved away from centralized, hardware-based switching to distributed, software-defined digital routing. Previous networks were hub-and-spoke designs in which everything came to hardware choke points where cyber safety and security could be practiced. However, in the 5G software defined networks that activity has been pushed outwards to a web of digital routers throughout the network, thus denying the potential for choke point inspection and control.
2. 5G further complicates its cyber vulnerability by virtualizing in software higher-level network functions formerly performed by physical appliances. These activities are based on the common language of Internet Protocol and well-known operating systems. Whether used by nation-states or criminal actors, these standardized building block protocols and systems have proven to be valuable tools for those seeking to harm others.
3. Even if it were possible to lock down the software vulnerabilities within the network, 5G networks are also being managed by software—often early generation artificial intelligence—which itself can be vulnerable. An attacker that gains control of the software managing the networks can also control it.
4. The dramatic expansion of bandwidth that makes 5G possible, creates additional avenues of attack.[18] Physically, low-cost, short-range, small-cell antennas deployed throughout urban areas become new hard targets. Functionally, these cell sites will use 5G's Dynamic Spectrum Sharing capability in which multiple streams of information share the bandwidth in so-called "slices"—each slice with its own varying degree of cyber risk. When software allows the functions of the network to shift dynamically, cyber protection must also be dynamic rather than relying on a uniform lowest common denominator solution.
5. Finally, of course, is the vulnerability created by attaching tens of billions of hackable smart devices (actually, little computers) to the network colloquially referred to as IoT. Plans are underway for a diverse and seemingly inexhaustible list of IoT-enabled activities, ranging from public safety things, to battlefield things,

[18] David Simpson and Tom Wheeler, "Why 5G Requires New Approaches to Cybersecurity," *Brookings* (blog), September 3, 2019, https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/.

to medical things, to transportation things—all of which are both wonderful and uniquely vulnerable. In July, for instance, Microsoft reported that Russian hackers had penetrated run-of-the-mill IoT devices to gain access to networks. From there, hackers discovered further insecure IoT devices into which they could plant exploitation software.

Next Steps for the Government in Cybersecurity ECO System

- **Treat cyber security as a National Security issue**

Cybersecurity is not just an IT issue.[19] It affects everyone working in government and beyond. In the best examples from the private sector, leaders champion education and awareness of cyber security, and present the risks in real-life terms, so that everyone understands what's at stake and how it affects their daily jobs.

Similarly, in the oil and gas industry, companies have tried to make cyber security an equally central part of their culture – alongside safety, and not just a 'compliance' issue. Employees are encouraged to think about what kinds of assets are at risk, and how they can prevent attacks and spot threats.

The governments need to adopt a similar mindset and make cyber security part of 'the national security strategy.

- **Embed more security into supply chain**

Governments everywhere are often heavily dependent upon a wide and complex web of service providers and contractors. With so many parties processing confidential information, the chances for leaks or theft are much higher. The best way to counter this challenge is by tightening up procurement processes. Contracts should embed cyber security. Ideally, suppliers should all be certified to an industry standard. Regular monitoring and independent audits can reassure the government that standards are being maintained, to avoid weak links in the chain. Most importantly, to make sure contractors drive the right behaviors when responding to a cyber security incident ensuring openness, transparency, and a willingness to work together when the worst happens.

[19] Muhammad Abdul Qadeer, "The Cyber Threat Facing Pakistan," The Diplomat, June 6, 2020, https://thediplomat.com/2020/06/the-cyber-threat-facing-pakistan/.

- **Collaborate with the private sector**

Given the success of other industries in combatting cyber threats (especially the financial sector), the government should consider harnessing some of this expertise. Collaboration can bring in fresh, external thinking as well as providing challenge, benchmarking, and peer comparisons.

Being prepared to share intelligence on actual and potential attacks also matters. After all, the kind of information floating around the criminal groups is often stolen from and used against a combination of public and private organizations, so it's in everybody's interests to work together.

- **Plan talent needs carefully**

Cyber crime is a growing phenomenon, and people with the skills to combat this threat are in high demand.[20] Today's governments cannot compete with private sector salaries, so it is hard to keep hold of the best talent. Workforce planning should assume that specialists may only stay for a few years, and look to create a production line of new, young talent to succeed them.

In future, government should widen its collaboration with private companies to include talent sharing. Cyber security specialists could rotate roles between the public and private sectors, as part of their natural career development. It would not just help the government; it would also give these individuals a higher professional profile.

In future, government employees should all see themselves as on the front line of identifying and responding to cyber crime.

Farooq Naiyer is a visiting fellow at Islamabad Policy Institute. He is the chief information security officer at ORION. He has vast experience in cyber-security, privacy, technology compliance, and assurance.

[20] Louis Columbus, "What Are The Fastest Growing Cybersecurity Skills In 2021?," *Forbes* (blog), November 1, 2020, https://www.forbes.com/sites/louiscolumbus/2020/11/01/what-are-the-fastest-growing-cybersecurity-skills-in-2021/.