Focus
August 2022

The Evolving AI Arena in the Neighbourhood: Implications and Options for Pakistan

Ayesha Zafar

The Evolving AI Arena in the Neighbourhood: Implications and Options for Pakistan

AYESHA ZAFAR*

Introduction

China is building one of the largest and world's highest cloud computing data centre in the high-tech zone of the Tibetan capital Lhasa with the aim to influence regional tech services. Cyber warfare, which can be referred to as the fifth dimension of warfare between the two regional powers in the region (i.e., China and India), have been developing since the turn of the 21st century. Both adversaries claim to have achieved major advancements in the Information Technology (IT) infrastructure and cutting-edge technology such as AI, Cloud Computing, Big Data, and the Internet of Things (IoT) in the sector, exacerbating the already existing rivalry for the regional clout. According to the Government of India, the state has allocated a handsome amount of INR 798.87 billion (i.e., $10.11 billion) to its IT and telecommunication sector for FY 2022-23.[1] Whereas, China which stands second in the National Cyber Power Index (NCPI) 2020,[2] is investing an envisioned $1.4 trillion in a state of the art fifth-

* Ayesha Zafar is an Intern at Cyber Security Program, Institute of Regional Studies, Islamabad.

generation wireless technology for advancement in IT between 2020 to 2025.[3] Both countries understand the very nature of future wars, and are therefore, pooling resources for the consolidation of their respective cyber powers.

The chaos in the South Asian cyber atmosphere is on the surge. After obtaining a considerable regional military clout, India and China are vying for influence in cyberspace as well to maintain their hegemonic postures, creating greater vulnerabilities for other states in the region. While, on the one hand, China's National Tibetan Plateau Data Centre bears great importance, on the other hand, Microsoft's deal with India to establish its fourth data centre in the country sufficiently provides grounds to contemplate the increasing cyber vulnerability in the region.

Chinese National Tibetan Plateau Data Centre

China, with a total investment of 11.3 billion Yuan, aims to build the world's highest altitude cloud computing data centre in its autonomous region of Tibet.[4] With the first phase of construction completed, the complex is now ready to undertake trial operations to ensure that everything functions properly. The data centre, which will be built in three parts, is projected to be completed in five to six years. Officials predict that once constructed, 70,000 cabinets would be placed at the facility, and its yearly income might exceed 10 billion Yuan. The project aims to fulfil the data storage needs of China's major provinces and neighbouring countries including Pakistan, Nepal, Myanmar, and Bangladesh. China aims to provide services in the fields of distance data learning, data backup, video rendering, and autonomous driving via this facility. With this headway, China is

the fourth country globally with the largest number of data centres in the world with 447 data centres at present.[5]

Microsoft's Largest AI Data Centre in Hyderabad, India

At the beginning of the year 2022, Microsoft, i.e., one of the biggest tech firms of the world announced its largest investment in India. With the planned investment of INR 150 billion (i.e., approximately $1.88 billion), Microsoft aims to build its fourth data centre in Hyderabad, after Pune, Chennai, and Mumbai.[6] According to Microsoft, the setup will be one of the largest in India and will be committed to helping clients in becoming a part of the world's largest cloud infrastructure by enabling them to thrive in an AI-oriented digital economy. The facility maintains its objective of providing data solutions and advanced security to government organisations, enterprises, and developers while upholding a competitive advantage in the Indian digital economy. The facility will be operational by the end of 2025.

AI Centres and the Complexity of Data Centre Facilities

As the hegemonic posture of the two mighty adversaries in the region is reverberating in every realm of security, the AI-oriented defence approach for algorithmic warfare cannot be disregarded in this context. The construction of two of the greatest data centres in the region indicates the very nature of the emerging competition for which AI is an essential tool. The unprecedented cyber race characterised by algorithms and AI has already begun which posits a war of *all against all*. In light of this,

there is a possibility that both countries are building their AI bastions under the garb of data centres. With the offset of China's strategic plan to become the world leader by 2030 in the realm of AI,[7] China's appetite in the field has increased unprecedentedly. China, with an estimated investment of $150 billion,[8] is forging its robust domestic industry to surpass its prime rival, the US.

Likewise, India is also pushing itself hard in the AI race with its heavy investments in AI research and defence systems. India released its National AI Strategy in 2018, intending to acquire global hegemony, technologically. According to the Indian National Association of Software and Service Companies (NASSCOM), the AI industry is anticipated to boost India's GDP by $450-500 billion by 2025 with its digitised IT, media, and telecommunication industries.[9] Apparently, both countries evince a great inclination towards AI advancements. Taking this into consideration, it can be anticipated that these mighty technological infrastructures may be regional threats, for they may serve as the AI research and production centres feeding on regional intellegentised sensitive pieces of information for statistical and predictive analysis of the regional dynamics and production of AI-oriented technologies. Regional actors or stakeholders, particularly Pakistan due to its nuclear power status, must be heedful of the challenges that these AI centres could pose.

Analyzing The Concealed Threat from India

The India-Israel MoU on Cyber Security Cooperation and the Pegasus Spyware Attack

In 2018, India and Israel signed a Memorandum of Understanding (MoU) to further cybersecurity cooperation with

the intention of increasing human resource development and business-to-business cooperation.[10] In 2020, both countries signed another MoU on operational cooperation in the realm of cyber security.[11] Additionally, both countries recently signed another MoU in June 2022 to further consolidate defence cooperation in the cyber arena by combining Israel's technological and operational experience with India's extraordinary development and market potential. Both countries' pledge to collaborate in mutual cyber resilience *ipso facto* poses a mutual threat for Pakistan to deter, for both have adversarial orientations towards Pakistan. In light of the above India-Israel defence cooperation, Israeli spyware Pegasus bears great importance. A little retrospect will elucidate Pakistan's serious concerns over the alleged eavesdropping and espionage attempts by Israeli spyware on ex-Pakistani Prime Minister Imran Khan.[12] The mobile phone infiltration and surveillance software is a product of Israeli firm NSO Group Technologies. As confirmed by the Amnesty International, in 2021, the aforementioned spyware was reported to collect personal information from hundreds of human rights activists, political leaders, journalists, and lawyers. Imran Khan's mobile phone hacking was associated with India's widespread surveillance by the then IT Minister Fawad Chaudhry and Pakistan's Foreign Office considering Indo-Israel defence collaborations in the recent past.

Pakistan, however, quickly forgot the gravity of the matter, as the administration had other problems to deal with. Nevertheless, the incident dragged the pointer on how the Israeli-India mutual cyber resilience can be a great menace to Pakistan's sovereignty. It is noteworthy that Israel's former PM Benjamin Netanyahu was himself targeted using the same software. It is

more about India enjoying the already established Israeli cyber muscle by tactically using Indo-Israel strategic ties, not Israel being interested to spy on Pakistan. These recent developments of India-Israel Cyber Defence MoUs and the Pegasus spyware attack on Pakistan by the Israeli firm for gathering sensitive data are important links for the study of potentially developing AI centres in Pakistan's neighbourhood.

Potential Implications for Pakistan

India's Digital Outlook

Despite India's strong efforts, China greatly outpowers India in the AI realm. India is yet to form its comprehensive AI infrastructure. Therefore, it appears like India is greatly benefitting from western expertise in AI technology. India appears to use its Quadrilateral Security Dialogue (QUAD) connections for its steps forward in AI advancements and in exchange providing data collection and data analysis of the region to its western allies, for India is the one sure friend of the west in this region. However, its own data itself is at threat as it can be wielded by its western allies, and for that, it will have to harness ingenuity to ensure freedom of its own data.

Cyber Espionage

The fact remains highly relevant that due to limited awareness and lower education rate, the people of Pakistan are more prone to misuse of cyber technologies which would benefit the country's adversary seamlessly. For espionage in the contemporary dog-eat-dog world, India may not require physical agents like Kulbhushan Yadav when it could take advantage of Pakistan's poor cyber capabilities. Alternatively, it can easily

obtain information and directories for behavioural analysis of Pakistani people through cyber espionages via data breaches, hacktivism and spyware and, use the information to stage its capabilities for disruptive effect in case of conflict/war in future. Also, such actors/agents themselves can benefit from AI tech in Pakistan using their AI generated data to outreach to religious/sectarian outfits trying to target activists or media persons as well as steal data from Pakistani government databases to falsify identities used in terror attacks and hinder the follow-up investigations. With little awareness and greater access to internet services, people of the 5th most populous country in the world Pakistan are appearing to pummel their own country's sovereignty by making themselves vulnerable.

Silent Sentry: A Leap Forward in Disputed Kashmir Surveillance

In July 2022, Rajnath Singh, the Defence Minister of India, launched 75 AI-oriented defence surveillance robots aimed to be deployed at the Line of Control (LoC) in New Delhi. According to reports, many of these surveillance robots have been deployed as well.[13] Among them, one of the most attention-grabbing products was the Silent Sentry, a vital technology created by the Indian Army's design office to fill holes in surveillance networks. This high-tech surveillance by the Indian defence will supplement the AI centres for generating statistics and predictive analysis for any future conflict in the disputed region, providing India with the upper hand and Pakistan's overlooking of this threat may cost the country and the people of Kashmir.

Gearing Up for the Next War

With the appreciation to an interconnected world with globalisation and the thriving usage of Information Technology, data has become the biggest asset in the world. India appears to be heedful of this reality. It cannot be argued that the next or perhaps the one after the next conflict between India and Pakistan will be entirely a cyber or AI war as India still adheres to conventional and sub-conventional doctrines to bother Pakistan but India's AI intelligence and technological development will confidently supplement its defence in the war. Kaspersky, a Russian cyber security firm in its report *Cyber Threats to Financial Organisations in 2022* underscored India as one of the top 5 aims of cyber-attacks.[14] The firm's findings also highlighted that Pakistan and China would pose the greatest threat to India in this respect. With the increase in events of cyber strikes by Pakistan (although in retaliation), may it be honey trap or any hacking attack on media or ministries' websites, India seems to be preparing itself for any potential conflict with Pakistan with its AI arms and technological advancement. On the other hand, unfortunately, the danger and fear of such an unprecedented war between the two countries seems to have no legs in Pakistan. The country is not able to integrate AI into health or economy, let alone defence.

Pakistani Voters' Data Collection for Machine Learning

Data Collection entails aggregating data from multiple sources, including offline and internet sources, by scraping, collecting, and loading it. Expert.ai applies an artificial intelligence technology known as 'sentiment analysis' to comprehend the

emotions portrayed in social media messages. Expert.ai platform is provided by the Microsoft Azure public cloud. [15]This AI tech may be leveraged to dig out Pakistani voters' turnout and their choices in the elections and their psychological profiles just like in the 2016 US Presidential elections. This will assist the Indian administration in covertly involving themselves in the upcoming general election (foreign electoral intervention) by spreading misinformation and propaganda, attacking voters from opposite camps with bots attacks, and generating false reports on election candidates to generate an illusive narrative (similar to the Macron leaks[16]) and analysing the implications via AI tech.

Intellegentised Propaganda in Pakistan

Having observed Pakistan's great vulnerability towards propaganda and cyber exploitation, India is keenly aware of how it can sprout perilous predicaments for Pakistan using game-changing AI technology. Already, AI-powered technologies have been alleged to budding propaganda in the Brexit Referendum and the 2016 presidential elections to manipulate people. Surveillance with the help of radars, GPS tracking systems, social network analysis, interception of internet traffic, and hacking of digitalised assets is prevalent in the modern world. Better surveillance assists AI bodies to produce robust propaganda, the ruinous elements targeted toward the state's integrity. The data collected through surveillance tools can possibly fuel the propaganda machine of the hostile neighbour in Pakistan with the help of AI technology software.

Analyzing The Concealed Threat from China

Surveillance Concerns from TikTok and Huawei: Founded and Proven

China has appeared quite a few times in the probe regarding national security concerns of states with respect to the usage of Chinese applications and devices as surveillance tools by the Chinese administration. Since the year 2000, the US has been expressing concerns over Huawei-based telecommunication. The concern grew over the years with China's advancement in Information Technology and AI. As per an investigation carried out by the *Washington Post* in 2021,[17] the Huawei AI intelligence assisted government officials in identifying persons by voices, monitoring political figures of interest, managing ideological re-education, and detention centre monitoring.[18] As a result, several western nations barred Huawei equipment from their new 5G telecom networks, fearing that the corporation will aid Beijing in surveillance and sensitive data collection. As of now, all the 'five eyes' intelligence alliance countries (US, UK, Australia, Canada, and New Zealand) have banned Huawei from their 5G networks. Concerning Pakistan, it is important to highlight the ongoing legal suit between Business Efficiency Solutions (BES) and Huawei regarding spying in Pakistan started in 2021. BES imposed the allegations on Huawei explaining that both companies jointly worked for the Safe City project in Lahore and BES developed 8 software systems that worked to gather data from government agencies, regulate building access, analyse social media, and supervise drones. The Chinese company terminated the contract with BES, but still has not uninstalled the software, and according to BES, it is using the software to analyze the critical data from government agencies of Pakistan.[19]

In 2019, the Peterson Institute of International Economics, a US-based research centre, declared TikTok a 'Huawei-sized problem'. The Indian government, in 2019 and 2020, banned TikTok along with 58 other applications to protect the data and privacy of its citizens. In a similar vein, Azerbaijan and Armenia also banned the application during the 2020 Nagorno-Karabakh conflict stating that the application collected data and tried to spread disinformation in order to shape public opinion.[20] Similarly, the US under the Trump administration in 2020 and under the Biden administration in 2021 banned the TikTok and WeChat applications of China underscoring that the data security and data privacy of US citizens is compromised. Yet again, this year in January the Federal Communication Commission (FCC) Commissioner Brendan Carr emphasized that TikTok must be banned from the app store as the application uses backdoors for surveillance to collect users' draft messages, location information, voice recognition, web browsing and sends back data to Beijing, contrary to the company assurances on private data protection.[21] Hence, Chinese AI surveillance tools masked in Chinese-operated applications and devices are appearing to assist in its administration all around the globe in its massive appetite for data for predictive analysis of political advancements and identification of vulnerabilities of nations.

Potential Implications for Pakistan

Chinese Version of Cambridge Analytica: Access to SA Databases

Cambridge Analytica is a British analytical firm, which in the 2010s, collected the personal data of millions of Facebook users through an application called "This is Your Digital Life".

Cambridge Analytica collected the data from its psychographic data service for political advertising of Ted Cruz and Donald Trump in the 2016 US presidential elections. China, with its high ambitions of 2030 global AI hegemony, appears to be utilising its AI surveillance networks and data storage facilities for gathering sensitive information from the South Asian countries to which it is providing the facilities. While on one hand, the countries will be able to enjoy the data centre facilities, there also on the other hand will let their data wielded by the Chinese authorities. The South Asian region is already a volatile region, hegemony-ambitioned countries like China are expected to be inclined to have all sorts of data from the region in order to maintain their dominance.

Covert Data Collection of BRI Countries

The National Tibetan plateau Data Centre is a part of China's Belt and Road Initiative (BRI) with 149 participating countries. BRI is an ever-evolving infrastructural development foreign policy concept of China. This project has unequivocal geopolitical, geostrategic, defence, and technological implications. China's plan of nursing the developing countries' technological infrastructure will possibly help it acquire more intellegentised information via its facilities and enable China to align its position with those countries accordingly i.e cooperative or assertive.

State Surveillance and Privacy Concerns

Reiterating, China has been founded and proven to be using its backdoor-installed AI surveillance tools via its Huawei technology at Uyghurs' detention centres. Also, in 2019, objectionable images captured and leaked by the safe city

cameras and the BES vs. Huawei legal dispute on spying raised serious concerns over China's intense surveillance programs in the country. The event hints toward the Edward Snowden revelation of the National Security Agency (NSA) obtaining personal data through global surveillance without authorization. With the extensive use of Chinese- operated devices in security matters, Pakistan appears to be compromising its citizen's privacy and ultimately its sovereignty. More information from the surveillance tools tends to consolidate the AI bastions in China resulting in precise predictions for Pakistan. After economic dependence, access to national information and personal data of the citizens is apparently making Pakistan more vulnerable to bandwagon with China in every realm in the future.

Increased assertiveness for Chinese Security in Pakistan

China, from expressing its full confidence in Pakistani security institutions to demanding its own security presence in the country to protect Chinese assets, appears to shift its *modus operandi* of security in Pakistan. After the Confucius Institute attack in Karachi, the Chinese administration demanded its own security agency in Pakistan to protect its citizens and assets.[22] With the increasing political turmoil and the resurgence of terrorist activities in Pakistan, the pressure from China will possibly mount. The rising concern for Pakistan should not only be the increase of security presence but also the integration of AI technologies in its military commands. The R&D think tanks and the AI centres in China are consistently testing and producing AI-enabled defence technologies. As the intellegentisation of the Chinese military is becoming a fact, Pakistan must prepare itself

for the associated implications on its nukes, radar systems, scientists, and holistically all security stakeholders. Most important, with its explicit orientation toward decision-enabled AI combating with top priority on Unmanned Aerial Vehicles (UAVs),[23] China itself is yet to figure out the right balance between human and machine dimensions of decisions in military command and operational affairs.

Provocative Applications for Pakistani Youth

Pakistan imposed and lifted the ban on TikTok from 2020 to 2021 over unlawful content of obscenity and vulgarity.[24] Pakistan Telecommunication Authority (PTA) pledged to keep strict monitors on the platform activities but other Chinese-backed ghost companies are operating in the country as well suspected to be collecting data from the citizens who access the applications by providing all their credentials. Also, Chinese-origin applications such as Bigo and Uplive use sexually suggestive ads to lure people into 'installs', thus adding to their share value and datasets. These applications appear to be AI tools representing China's contentious goals with the use of its AI bastions. Consumer behaviour and personal data via these luring apps are expected to send back loads of data and add fuel to the AI predictive analysis tools back in China. The impacts of accessing these apps are two-fold: not only is China attempting to gather sensitive behavioural information but also apparently tends to influence personal preferences and behaviours.

Options for Pakistan

"Artificial intelligence is the future, not only for Russia but for all mankind. Whoever becomes the leader in this sphere will

be the ruler of the world", said Russian President Vladimir Putin highlighting the importance of AI in the contemporary world. Multibillionaire CEO of TESLA, SpaceX, and NeuraLink Elon Musk also stated that the 'most likely' cause of a third world war would be Artificial Intelligence. The salience of AI technologies can be comprehended by the efforts of countries that are pooling loads of investments across the globe in AI Research and technologies aiming to stay ahead in the AI race. Pakistani dilemma is that it is not even part of the race. Pakistan, with its meagre resources and constant internal instability, is unable to comprehend that the future of warfare is algorithmic and intellegentised, for which Pakistan is apparently not prepared. The above analyses show that China and India honing their AI capabilities will actually be detrimental to Pakistan. The country needs to be mindful of its vulnerabilities and should take impactful steps to counter the potential perils in the realm of cyber security and AI advancement.

Policy Recommendations

Following are some recommendations and policy options that Pakistan can adopt for strategic resilience and self-empowerment in this realm.

- Firstly, Pakistan, commendably, has been straddling the US-China dyad in its foreign policy approach since its inception. However, in the domain of technology and AI advancement, it is feasible for Pakistan to bandwagon with the emerging stature of China because Pakistan first needs to develop its robust technological structure which requires investments. The good news is that China, also, affirms to see Pakistan as technologically and digitally progressive, for the mutual trade

project CPEC holds its future in Pakistan's digital economy. Additionally, with the current position of Pakistan's cyber security and AI naivety, it is practical for Pakistan to align with top ranking global AI vibrancy country China in the constant war over our heads considering China's ongoing security conflicts with India, Pakistan's prime security concern.

Secondly, Pakistan can adopt a tit-for-tat approach by increasing its defence ties with Iran, Israel's prime adversary. Concern for cyber security has many legs in Iran due to Israeli threats to its nuclear capability, therefore, it can make a feasible ally with Pakistan in information sharing and collective deterrence against any cyber jeopardy. In practical, in order to explore this option, Pakistan first must find diplomatic solutions to existing discontentment due to ideological differences and to balance relations with Iran and KSA while enhancing the trust factor. Also, Iran does have cyber capability but not of strategic kind; increasing cyber defence ties does not imply assistance but rather mutual strategic and tactical cooperation and development.

- Furthermore, Research and Development (R&D) is the consequential element of any emerging sector in the states. Pakistan should initiate a collective effort (through collective funds) with other nations of the region and the Central Asian Republics (CARS) to forge consortiums for R&D in the realm of cyber security.
- In addition, a cyber nexus involving the intelligence of Russia, China, and Pakistan can be beneficial for all three actors given the dawn of a new multipolar world order characterised by perennial hidden wars. Mutual infrastructural projects and AI advancement will enable all to protect themselves and

collectively prepare for any possible cyber or algorithmic fiasco.

- Also, in order to boost AI-oriented tech start-ups and software companies in the country, Pakistan should establish a public initiative for Governmental Venture Capital Funds (GVC) which should be handled by the government agencies. These agencies should be responsible for pooling and regulating funds for entrepreneurial AI start-ups.
- With that, Pakistan should strictly focus on the cyber hygiene of its citizens. Guidance on the proper usage of gadgets with privacy protection should be given to Pakistani citizens using effective tools of Electronic Media, Social Media, and campaigns run by concerned administrative structures.
- Consequentially, Pakistan should work on the nuisance of misinformation and fake reports. For this, Pakistan and China are already exploring the opportunity of creating a media platform funded by China to counter misinformation and hate news. Both countries are putting efforts into creating an International stature media outlet that resolves to achieve 'information dominance' by countering western fabricated narratives.[25] Pakistan needs to participate in the venture effectively, for such a venture will help subdue internal chafe in the country as well.
- Most importantly, the salience of the National AI strategy cannot be overlook by any other overt/covert or any internal/external strategic plans for AI security. With the consolidating presence of AI structures in the region, it is an immediate need for Pakistan to formulate its National AI strategy.

- Lastly, it is imperative for Pakistan to understand that opening channels for negotiations and peaceful solutions to disputes is the most critical aspect of reducing any kind of fear and danger.

Notes and References

NOTE: The term intellegentised warfare is used by the Central Government of China referring to the advancement in military combat technologies.[1]

1 Finance Ministry of India, *Expenditure of Government of India*, (New Delhi, 2022), 10, https://www.indiabudget.gov.in/doc/Budget_at_Glance/bag6.pdf.

2 Julia Voo,Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy, Anina Schwarzenbach, "National Cyber Power Index 2020," *Harvard Kennedy School BELFER CENTER for Science and International Affairs*, (September 2020): 21-29, https://www.belfercentre.org/sites/default/files/2020-09/NCPI_2020.pdf.

3 *Coco Liu, and Yuan Gao,* "China's Vast Blueprint for Tech Supremacy Over U.S.," *Bloomberg*, 24 January 2022, https://www.bloomberg.com/news/articles/2022-01-23/china-s-vast-blueprint-for-tech-supremacy-over-u-s quicktake#:~:text=China%20is%20investing%20an%20estimated,with%20billions%20of%20connected%20devices.

4 "China setting up world's highest-altitude cloud computing data centre in Tibet," *The Economic Times*, 29 October 2020, https://economictimes.indiatimes.com/ news/defence/china-setting-up-worlds-highest-altitude-cloud-computing-data-centre-in-tibet/articleshow/78932514.cms?from=mdr.

5 Christof Baron, "Number of data centers worldwide 2022, by country," *Statista Research Department*, 23 May 2022, https://www.statista.com/statistics/1228433/data-centres-worldwide-by-country/.

[6] FE Bureau," Microsoft aims to build its fourth data centre in Hyderabad, after Pune, Chennai, and Mumbai," *Financial Express*, 8 March 2022, https://www.indiatoday.in/cities/hyderabad/story/microsoft-to-set-up-india-largest-datacentre-region-in-hyderabad-1921729-2022-03-07.

[7] Poul Mozour, "Beijing Wants A.I. to Be Made in China by 2030," *The NewYork Times*, 20 July 2017, https://www.nytimes.com/2017/07/20/business/china-artificial-intelligence.html.

[8] Poul Mozour, "Beijing Wants A.I. to Be Made in China by 2030," *The NewYork Times*, 20 July 2017, https://www.nytimes.com/2017/07/20/business/china-artificial-intelligence.html.

[9] Sri Kishna," Two decades of AI: Where does India stand today?," *Analytics India Magazine*, 16 March 2022, https://analyticsindiamag.com/two-decades-of-ai-where-does-india-stand-today%EF%BF%BC/.

[10] Ministry of External Affairs Government of India, *List of MoUs/Agreements signed during the visit of Prime Minister of Israel to India,* (New Dehli, 2018), https://mea.gov.in/bilateral-documents.htm?dtl/29356/List_of_MoUsAgreements_signed_during_the_visit_of_Prime_Minister_of_Israel_to_India_January_15_2018.

[11] "India and Israel sign agreement to expand collaboration in dealing with cyber threats," *The Economic Times*, 16 July 2020, https://economictimes.indiatimes.com/news/defence/india-and-israel-sign-agreement-to-expand-collaboration-in-dealing-with-cyber-threats/articleshow/76998307.cms.

[12] "Pegasus snooping: Pakistan probes whether PM Khan's phone hacked," *Aljazeera*, 20 July 2021, https://www.aljazeera.com/news/2021/7/20/pegasus-snooping-pakistan-imran-khan-phone-hacked.

[13] Jigyasa Sahay," Silent Sentry: How Rail-Mounted Robot Artificial Intelligence Will Enhance Surveillance Along LoC," *India.com,* 13 July 2022, https://www.india.com/science/silent-sentry-how-rail-mounted-robot-artificial-intelligence-will-enhance-surveillance-along-loc-kashmir-5510329/.

[14] Aditya Bhan, Sameer Patel," Cyber Attacks | Pakistan emerges as China's proxy against India," *Observer Research Foundation*, 15 February 2022, https://www.orfonline.org/research/pakistan-emerges-as-chinas-proxy-against-india/.

[15] Bill Betcher, "9 Burning Questions About the Expert.ai Platform and Their Answers," *expert.ai,* 19 May 2022, https://www.expert.ai/blog/9-burning-questions-about-the-expert-ai-platform-and-their-answers/#:~:text=The%20expert.ai%20Platform%20is,implemented%20on%20their%20private%20cloud.

[16] Megha Mohan," Macron Leaks: the anatomy of a hack," *BBC Trending,* 9 May 2017, https://www.bbc.com/news/blogs-trending-39845105.

[17] Eva Dou," Documents link Huawei to China's surveillance programs," *The Washington Post*, 14 December 2021, https://www.washingtonpost.com/world/2021/12/14/huawei-surveillance-china/.

[18] Vincent Ni, "Documents link Huawei to Uyghur surveillance projects, report claims," *The Guardian*, 15 December 2021, https://www.theguardian.com/technology/2021/dec/15/documents-link-huawei-uyghur-surveillance-projects-report-claims.

[19] Ibid.

[20] "Tik Tok fails operating in Armenia," *ARMENPRESS,* 1 October 2020, https://armenpress.am/eng/news/1029718.html.

[21] Pranav Dixit, "An FCC Commissioner Wants TikTok Removed from App Stores After BuzzFeed News Found American User Data Was Repeatedly Accessed In China," *BuzzFeed News*, 30 June 2022, https://www.buzzfeednews.com/article/pranavdixit/tiktok-report-user-data-fcc-response.

[22] Adnan Aamir, "China wants own security company to protect assets in Pakistan", *NIKKEI Asia*, 28 June 2022, https://asia.nikkei.com/Politics/International-relations/China-wants-own-security-company-to-protect-assets-in-Pakistan.

[23] Kartik Bommakanti, "A.I. in the Chinese Military: Current Initiatives and the Implications for India," *Observer Research*

Foundation, February 2020*,* https://www.orfonline.org/wp-content/uploads/2020/02/ORF_OccasionalPaper_234_AI-ChineseMilitary.pdf.

[24] PTA, Twitter Post, 20 July 2020, 11:58 p.m., https://twitter.com/ptaofficialpk/status/1285287980370931712.

[25] "Pak, China plan to create media house to challenge West's 'info dominance," *Hindustan Times*, 7 June 2021, https://www.hindustantimes.com/world-news/pak-china-plan-to-create-media-house-to-challenge-west-s-info-dominance-101623069334228.html.