Sociology & Cultural Research Review (JSCRR)
Available Online: https://scrr.edu.com.pk
Print ISSN: 3007-3103 Online ISSN: 3007-3111
Platform & Workflow by: Open Journal Systems

THE IMPACT OF SINO-US AI CYBER WARFARE ON PAKISTAN: CHALLENGES, OPPORTUNITIES, AND STRATEGIC IMPLICATIONS

Muhammad Zahid Bashir
Department of Political Science and International Relations, University of Management and Technology Lahore Punjab Pakistan.
zahidbashir001@gmail.com

ABSTRACT

The industrial revolution in the nineteenth century gave way to the strategic competition of the twentieth century, conventional and unconventional due to the nuclear factor. The third revolution of the military affairs of the 21st century was the advancement in electronic warfare and cyber warfare. In today's world, new global actors have appeared, and confrontation is taking place at all levels and in all sectors between Beijing and Washington. Cyberspace is recognized as the fifth warfare domain as the US armed forces and Chinese PLA heavily rely on cyberspace for message exchange, execution of operations and strategy. It shot the relation to a new era of cyber-arm race and remains strategic competition in cyberspace between the two nations. The present technological competition between China and Unites States specially in the field of Artificial Intelligence and cyber warfare has its implications for the many countries specially a country like Pakistan that is positioned strategically between the two global powers United Stated and China. This Paper will put light on the opportunities and technological challenges Pakistan will face in the rivalry of the big powers. Since this race in technology also comprises cyber security threats and reliance on the technology, it also contains opportunities for economic development and building of Pakistan's national security architecture. This paper aims to discuss the cybersecurity threats that have an impact on Pakistan; the impact of the relations between china and the USA economically and geopolitically; and the plausible strategic of solutions for Pakistan.

Keywords: *Cyber War, Cyber Security, Strategic Implications*

Introduction

The Global dynamics are reshaped due to the technological race specially in the field of the of artificial intelligence and cyber security. In the digital realm, AI is becoming the front tool in cyber warfare and transforming the nations defend and attack response. The significance of cyber warfare capabilities for militaries can also be gauged by former Chairman of the U.S. Joint Chiefs of Staff Gen. Martin E. Dempsey's statement in which he said, "We now live in a world of weaponized bits and bytes, where an entire country can be disrupted by the click of a mouse."[1] To connect this statement with the global security landscape, it is important to note that 20 countries (or more) have established dedicated military units to conduct cyber warfare.[2] Bulletin of the Atomic Scientists .Cyber warfare is not only detrimental to an adversary's military but can also handicap its economy, on which all the other elements of national power are dependent. [3]

China's Air Force Secretary Frank Kendall said on Oct. 29. that while China has made advancements in various military technologies, artificial intelligence (AI) could be a decisive factor in any future conflict. He noted that the U.S. and China are engaged in a "race for technological superiority," particularly in microelectronics and AI applications that could transform warfare dynamics.[4] He further said "But rather than use AI as a catch-all buzzword, Kendall said he thinks of it in terms of the "specific applications" to which it can be applied, such as pattern recognition, automation, decision-making, and support functions. "On the battlefields of Europe … and to some degree, in the Middle East" are proving that these applications are "changing the character of warfare," Pakistan will have an effect by this rivalry due to its geopolitical location, complex relationship with both the United States and China and heavily depending on foreign technology.

This research paper aims to brief how the SINO-US AI and cyber warfare competition will effect Pakistan having focus on broader geopolitical landscape, economic implications and cyber security vulnerabilities. This paper will also provide analytical suggestions for Pakistan after highlighting the opportunities, threats and trends that suggest strategic approaches for safe guarding Pakistani interest in the advancement of this digital world. Both countries have set AI as a prime asset with vast implications for national security, military dominance and economic competitiveness. The

US is currently winning the race of AI but China is also no far away from it. China has caught up driven by the massive state investment, revolutionizing the technology and access to large amount of data at large.

- **Application to Sino-US AI-Driven Warfare**
    I. **Power Maximization:** The present decline in diplomatic relations between China and the United States over AI warfare systems is a prime representation of Realists' concepts of power and domination. In this regard, both countries believe that enhancement of this technology will assist in the achievement of a more effective strategy of power in the world. The realist approach insists on a state's pursuit of power with regard to the other states, and thus capabilities in technological measures such as AI will be essential. Aspirational weapons systems, capability-oriented surveillance technologies, and emerging cyber tools are perceived as crucial enablers of enhancing or at least preserving national capabilities.

The Chinese and the Americans understand the importance of masterminding artificial intelligence in military situations. Fully autonomous weapon systems can lower the reliance on humans, enhance speed and accuracy in combat purposes and AI integrated intelligence sensors on the other hand, can strengthen the surveillance mechanism and overall awareness. Also, AI's involvement in cyber warfare gives one side in the struggle the capacities to intimidate, challenge or shield against cyber incidents, which also will form the global balance of forces.

In this power battle each player sees AI development not only as a change in their respective industries but as a tool that can determine the international balance of power. It was the competition that mirrors the tendencies that have been appearing in the international relationships during the past years: the technological leadership of a state becomes the key to its security and, consequently, to its leaders' ability to provide people with new opportunities.

II. **Security Dilemma:** The security dilemma between China and the United States has been intensified by their evolving relationship as near-peer rivals,

particularly in the realm of military technology, including AI advancements. As one nation increases its military expenditure to enhance its AI capabilities, the other perceives this as a direct threat, prompting a similar response. This cyclical dynamic of competition and reaction fuels mutual suspicion and heightens the potential for escalation.

Whenever one state begins developing such technologies of military application as autonomous systems, surveillance, or cyber capabilities, it puts another state on the alert as it perceives such inventions as a potential threat to its own positions. This creates a vicious cycle where any move by either nation to increase its military relative to the other is viewed as preemptive aggression and thus the other party responds with their own military buildup.

Such cycle creates a condition of continuous conflict as each actor strives to overwhelm the other with the fear of relative deprivation of power and security. The more a state increases its capability and readiness of using Artificial Intelligence in defending its territory, the more the other felt threatened to do the same hence top it up an arm race. Not only does this keep the rivalry alive, but it also sustains the structural characteristics of the security dilemma, in which both sides' actions are largely defensive; however, processes resulting from these actions make the participants themselves more unworried than when they started the action.

III. **Anarchic System:** Lacking global regulations on the use of AI in war more so, the anarchic international system increases competition. There are no treaties that would guide the work on constraining or regulating AI technologies, and without such international cooperation, states are free to act on their own behalf, putting the security of their nation above that of the entire population.

- **AI Applications in U. S Military Operations:** AI solutions in the US military activities are progressively increasing, and corresponding defense initiatives are developing into critical enablers of advanced capabilities and decision-making. Many of these applications have used artificial intelligence, big data and data mining, robotics and automation to enhance the military capability, efficiency and reduce risk

factors. Here's a brief overview of key AI applications in U.S. military operations:

I. **Predictive Maintenance:** Artificial Intelligence is being in use for predictive maintenance to anticipate equipment failure before they occur. AI technology can optimize maintenance schedules, decreasing downtime by data analyzing from different sensors.

II. **Smart Weapons:** Smart weapons having technology of AI has improved the target identification and engagement. This has increased the strike precision.

III. **Intelligence, Surveillance and Reconnaissance:** The analysis of images and video data has significantly improved the ISR system. This has enhanced on the identification and recognition of targets, ease and contribution to improved situation awareness on the theatre of war.

IV. **Command and Control System:** Real time data analysis and decision making has re shaped the command and control operations.

V. **Autonomous System:** The inventions of autonomous vehicles like drones and ground vehicles has made operations, surveillance and reconnaissance easy. These can not only operate auto but also can be operated by the intervention of the human.

VI. **Cyber Security:** AI is playing key factor role in better cyber security measures within the military. It has integrated the techniques like anomaly detection and predictive analytics to monitor networks for threats and act to cyber incidents in real time.

VII. **Target Recognition and Detection:** The development of machine learning algorithms are helping in the to improve target recognition and decreasing time to takes to engage enemy targets.

VIII. **Swarm Intelligence:** AI is being integrated for swarm intelligence applications in drone operations in which multiple drones can work together autonomously to achieve common objectives. It has increased the operational effectiveness many times as compared to single drone operation.

- **AI in China's Cyber Warfare Capabilities:** China is ramping up the use of artificial intelligence (AI) to improve its cyber warfare and making use of the technologies when doing both attack and defense. China established its cyber warfare unit in 1997 and it has developed into a modern cyber capacity structure. The initial creation of the Strategic Support Force (SSF) within the PLA has now been identified as an important part of the China's military strategy 5, where the PLA's use of artificial intelligence has regard to the modern warfare's cybersecurity and information operations.
  I. **Autonomous Systems:** Automated drones and vehicles are made that have the function to operate automatically or in groups. This also has improved their battle fields capabilities
  II. **Cyber Warfare:** Artificial Intelligence tools are in practical for cyber operations and detection of the threat and response to tackle that threat.
  III. **Information Warfare:** Artificial intelligence base algorithms are helpful in the detection of the misinformation campaigns, an aspect critical for cognitive warfare.
  IV. **Command and Control (C2):** The PLA is implementing AI-driven C2 systems that integrate data from multiple domains (land, air, sea, cyber) to improve situational awareness and decision-making processes.[6]
  V. **Data Analysis and Information Gathering:** Useful information is gathered from large datasets. This extracted information is important for intelligence gathering, allowed more decision making in cyber operations.
  VI. **US-China Cyber Conflict**: The two countries have invested heavily into the world of cyber intelligence, with tensions and disagreement between their national strategies in AI and cyber warfare marked by their competition. The major feature of the US approach can be said to be technology improvement through private sector funding and regulation by the government at certain intervals. The technology is

initiated by American firms as seen with these companies based in Silicon Valley while the government monitors their activities, offering basic support to make sure that military and intelligence facilities get advantage of the technology in question.

On the other hand, China follows more state-driven model in which state plays an active role in initiating and distributing new technologies. The Chinese government fully supports domestic companies and research institutions to help achieve rapid development in AI and cyber warfare. This top down approach allows Chinese to ensure its technological advancement aligns with national goals and to quickly make and implement large scale change.

There has been observable high activity regarding the development of the AI cyber warfare in both nations. Both are committed to creating weapons for defending their own cyberspace while at the same time trying to undermine the other side's. It remains a contest in the first place of cyberspace both horizontal and vertical and cyberattacks can be decisive in future wars.

Ultimately, the Sino-U.S. rivalry in AI and cyber warfare highlights the different strategic approaches to technological dominance, each with its own strengths and challenges. The race between the two powers to enhance their cyber capabilities reflects the growing importance of digital warfare in global power dynamics.

- **AI and Cyber Warfare:** AI-incited cyber warfare relates to the employ of robots in cyber warfare, deep fake videos, and intelligence systems that independently find their ways into the circuits of the counterpart. These innovations are a nod towards an entirely new generation of conflict that is slowly leaving the tactical plains of physical warfare and going entirely online.

Self-sustaining cyber warfare operations are those in which robots can carry out devastating, pinpoint assaults on enemy assets, slipping through recognized defense systems and disturbing a wide variety of targets. AI in deep fake videos can be run to influence the public opinion or to deceive the opponents by having realistic though fake videos, making the wars more complex.

Cyber mission capabilities improve through the use of AI intelligence systems for increased efficiency of analyses of adversary networks, for mapping of targets to be compromised, and for the employment of these exploits. Such systems can also work at a speed and extend that is not feasible for a human operator and thus can compromise targets quickly and efficiently.

Altogether these AI based technologies have changed the character of the war newer and challenging for both the sides. The digital war is not just fought on the physical front but also over information, control of an organization's networks and cyber spying. This change of war upsets traditional approaches to strategy and defense since threats are ever changing to suit the available technology. Employment of AI in cyber warfare has changed the warfare much, especially with reference to the warfare importance of cybersecurity, innovation and the imperative need to protect structures and information.

Pakistan's Geopolitical Position:

This paper explains that due to its strategic position between China and India, Pakistan occupies the strategic center of many of the most important geostrategic shifts. Having been an ally of China, Pakistan has gained immensely from the relationship with China through increased access to technical knowhow, State of art technologies and practical technology investments. Such relations have made formidable contribution to the development and modernization process of the economy of Pakistan especially in the defense technology and energy sector.

Nevertheless, the friendship between Pakistan and the United States is versatile and under tension. Although the US has been a frontline supplier of defense equipment and technology to Pakistan, which is seen as a strategic partner, it puts equal came at China as strategic competitor which paves way for complexity within tripartite relations. The U.S. always considers with suspicion the boosting cooperation between Pakistan and China especially when seen through the prism of the competition between Washington and Beijing. Nonetheless, Pakistan sustains good relation with the United States for security and economic interest while displaying strong commitment for purchasing American defense equipment but at the same time strengthening its bond with China.

This is not a simple tango, this placing of Pakistan within a new world order, making it a strategic power of rising significance. It needs to balance its ties with both China and the United States effectively and optimally use its geopolitical position and partnerships to balance for the interest of all its partners and allies. These geopolitical realities that place make Pakistan significant actor in any regional strategy and politics.

- **Technological Dependence**: As the ties between the two countries deepen, especially in the Belt and Road Initiative, Pakistan is facing a new set of issues touching the technological sovereignty and cybersecurity with the use of Chinese equipment, for example, the Huawei firm in telecommunications, 5G networks. On the other hand, due to constrained technological development within the country Pakistan still has to rely on international players for sophisticated AI and cybersecurity systems.
- **National Security**: National security concerns of Pakistan are multifaceted and the geographic location serves the role as reasons and obstacles faced by it. Currently, the country is in close proximity to conflict-prone areas, which include assaulting neighbors such as India, internal insecurity and security threats that strengthen the security instability situation in the country. Among such threats one can name the trends of growing cyber risks on infrastructure, military objects and the economy.
- **Military and Defense Networks**: Cyber-attacks can happen to Pakistan's military apparatus, which due to their critical nature for the security of the country, should not be affected by such hacks. The military is a key institution in the defense of the Pakistan and any misinformation of attack could result in the theft of the sensitive information and national defense strategies. These attacks can even disrupt the ongoing military operations.
- **Strategic Alliances:** Pakistan's alliance with China, particularly through initiatives like the China-Pakistan Economic Corridor (CPEC), places it firmly within China's sphere of influence. Indeed, this cooperation offers an immense economic and military resource development, investment, and access to superior technologies. But it cannot be without its dangers. Emerging cordial relations

with China may prove damaging to the long standing friendship with USA that has offered significant military assistance and cooperation in counter terrorism. The extension of economic and strategic cooperation with China poses the challenge of maintaining a correct relation with the other super power, the US, because the latter would see the cooperation with China as counter to its interests in the region as well as in the global struggle with China.

- **Balancing Act:** Emergence of this competition between china and US brings another dimension of foreign policy in Pakistan. Negative – they can overwhelm the other to a destructive level if integrated to either Chinese or American market. It is here that Pakistan has to calculate its balance of these relationships in the best interest of its own strategic security, growth and the stability of the region. This balancing act has the condition that while Pakistan have to put pressure on both super powers it shouldn't do anything that compromises it diplomatic independence. In general, those relations are of significance to continue the security, development and diplomatic power for Pakistan.
- **Security Concerns:** Application of AI in war can elevate the warfare systems in the region which turn invites competition and instability. Pakistan should anticipate a range of risks arising from the bilateral competition between China and the US, and local technological slowdowns, sabotage and cyber-attacks or technology embargo.
- **Economic Dependencies:** Despite the fact that China through CPEC has made considerable investment in Pakistan, the Pakistani's economy may be exposed to certain danger if they depend so much on China especially in a war like scenario. Excessive dependence of a particular power may lead to different weaknesses for Pakistan – both economically and strategically. The risks are to prefer one nation or region over the others, therefore, the solution is in the diversification of economic relations. Thus, for creating a healthier condition and making a diversification in dependence Pakistan should build stronger relations with multiple countries of the world which will lead to stability and security in economic and security interests of Pakistan in the long term.

Impact of Sino-US AI Cyber Warfare on Pakistan:

Cybersecurity Vulnerabilities:

Evidenced by the escalation of Sino-US cyberspace confrontation, major dangers to Pakistan emerge. Hacktivism, terrorism, and cyber espionage and warfare are elements are becoming more elaborate, and a nation like Pakistan being a soft target or an indirect victim or direct threat, which has least protection against cyber threats.

- **Critical Infrastructure**: New generation of Pakistan is linked with digital technologies to manage energy, financials, telecommunication and governance. A cyber-attack that employs Artificial Intelligence goes by and paralyzes these systems, destabilizes certain customized services, and brings anarchy to the economic activities. AI automated this approach and made the scheme faster and flexible, which makes it more difficult to counter it.

Example: In the same year, Pakistani power grid suffered a cyber-attack that while has not been directly pinned on state actors clearly exposed vulnerabilities of Pakistan.

- **Data Breaches and Espionage**: As has been seen both china and the US have been involved in hacking activities especially where the cyber espionages have focused on conducting penetrations in critical industries and governments data. Because of the small capability of Pakistan to protect figures and data, it becomes a suitable area of interest. Cyber terrorism may include cases whereby state actors obtain intellectual property, disrupt electoral processes or gain militarily intelligence and rival nations such as India may use cyber terrorism to gather intelligence on Pakistan's approaches to political and militarily. This can effect seriously to the ability of Pakistan's decision making and national security policies.

Technological Dependence on China

The cooperative relationship between Pakistan and China has become more advanced in terms of technologies such as, 5G networks, surveillance systems, and digital commanding systems. This dependence brings both, threats and opportunities for Pakistan in the context of rising Asian giants divided by Sino-American rivalry.

- **Huawei and 5G Infrastructure**: Pakistani decision to go with Huawei's 5G technology is raising eyebrows in western countries led by the US that accused Huawei of installing back doors for Chinese state-sponsor espionage. Competition between US and China may negatively affect Pakistan since most of the products it uses today is from Chinese technology companies.

Example: Several countries that use Huawei technologies have been crippled because of sanctions that the US imposed on the company. A similar situation might be experienced in Pakistan in the event that the US is forced to place sanctions or take a retaliatory action against China.

- **Surveillance Technologies**: China is exporting surveillance technologies to Pakistan to improve security and policing and in the near future, Pakistan may become overly dominated by Chinese technology. The following dependence can become important concerning Pakistan and its digital independence – one could be dependent on a foreign state, giving up control over the major nodes and data to China. While adopting such technologies, Pakistan is vulnerable to losing its independence in digital security/privacy as it would be controlled from outside. In order to effectively moderate Pakistan's digital domain or strategic depth, the country must closely guard its vulnerabilities that lie in dependency on foreign technology and invest heavily in the cultivation of the Pakistani cyber power.

AI in Military and Defense:

Automated weapons and AI-based cyber abilities are now the shared just-type in modern warfare due to its military use. The defenses of Pakistan are already quite robust but these technologies could also pose a threat and the doors to them are wide open in case of a war between the United States of America and China.

- **AI in Warfare**: Unmanned aerial vehicles, cyber warfare equipment, and artificial intelligence weaponized defense system have now defined the shape of modern warfare. As dependency on AI in warfare increases, Pakistan ought to ask: How will it protect against, or work to avoid the occurrence of, AI-based cyber terrorism in the future and will it

support the deployment of lethal AI-driven weapons in contemporary systems of warfare? Example: The increasing use of drones in military operations, such as the US's reliance on drone strikes, demonstrates how AI is altering the nature of combat. Pakistan needs to develop countermeasures to defend against similar AI-driven attacks.

Economic Implications:

The Sino-US tech clash disrupts supply networks and procurement of particular technology; these scenarios are not conducive to the Pakistan economy.

- **Supply Chain Disruptions**: Due to its status of being a developing country, Pakistan depends on many imports the most important being AI and semiconductors. This technology includes essential import commodities whose supply chain may be disrupted by the ongoing US-China trade wars or sanctions, slowing Pakistan's digitization and economic progress.
- **Opportunities in AI Adoption**: The current nature of Sino-US relations has a positive but threatening factor for Pakistan in terms of its ambitions of becoming a regional powerhouse. If Pakistan makes a careful approach to utilizing AI technologies, the country will be able to advance its economy on many fronts; most evidently in agriculture and health as well as in education. This way adopting and implementing AI the country will be able to skip those traditional industrialization steps and thus have enhanced efficiency and productivity. This would help the country to strengthen its economic structure so as to have a variety of partners instead of relying on one economic partner. Thus, by utilizing AI, Pakistan will be able to address the idea of competitiveness on the international level, as well as develop steady growth and, thus, make people's lives better.

Opportunities for Pakistan:

However, there are some benefits to share between Pakistan; primarily aimed at enhancing its technological sector in the case of Sino-US AI cyber warfare. By embracing AI and cybersecurity innovations, Pakistan can enhance its digital infrastructure,

improve security, and foster economic growth in the evolving technological landscape.

AI for Economic Growth:

Pakistan can leverage AI to drive growth in various sectors:

- **Agriculture**: AI technologies, such as machine learning and data analysis, can significantly enhance resource usage and increase crop yields. By analyzing data from sensors and satellites, AI provides real-time insights into critical factors like soil health, water levels, and weather conditions. These technologies help optimize crop production, monitor soil quality, and predict weather patterns, ultimately improving food security. With AI, farmers can make informed decisions on fertilization, pest control, and planting strategies, leading to better crop management. This results in higher yields, more efficient use of resources, and a more sustainable agricultural system, helping to meet the growing food demands.
- **Healthcare**: Another advantage of AI includes; The use of AI in the diagnosis and treatment of diseases owing to the convenience of sifting through large data sets when it comes to medical information, will lead to the discovery of diseases and the treatment of such, or as well as the prevention of diseases with AI collectively enhancing health of a nation and cost implications of diseases on economies. AI contain a lot of opportunities to develop the Pakistani healthcare system to a new level of diagnostic, prognostic and therapeutic abilities.
- **Education**: Pakistan Education System needs such technologies in order to invoke learning environment, since education technologies are smart enough to mend the shortages within few years and help to develop outstation child's talents who are isolated due to rural India like areas living in Pakistan. To close this chasm, these technologies present personalized approaches to content presentation, engaging, and Live lessons, and distant learning instruments and therefore provide for student in regions most inaccessible a good education. In pairing with a teacher AI can also help in managing the necessary paperwork and give an overview on the student's performance in order to give more attention in teaching. The impact of this innovation

can lead to improving educational equity so far as learners' outcomes it across the country.

Strategic Recommendations:

To avoid the corresponding risks and leverage the possible benefits of Sino-US AI cyber warfare, Pakistan should take some strategic actions. These are diversifying relationships in technologies from China and the US, developing indigenous AI and cybersecurity solutions; and co-ordination of policy and action between governments, universities and commercial entities. Moreover, there is a need to impart a stronger shape to its IT framework and focus on diplomatic relations to better protect its interests in the view of host technological dynamics.

- **Cybersecurity Frameworks and Policies**: There is another lack of a specific legislation that defines the rules of cybersecurity in Pakistan. This ranges from enhancing laws protecting data, developing standards of cyber security and encouraging hacking – ethical hacking. The successful development of technology companies depends on the existence of a sound legal basis to address the relevant risks.
- **Strengthen Cybersecurity Infrastructure**: Experts put their money in optimal technological security solutions, ensure the enhancement of the national security architecture, and set up specific divisions to protect the infrastructure. This will also help improve security in general with reference to highly important properties and infrastructure in a given society. Thus, focusing on the further strengthening of the existing security prevailing within the country is capable of significantly reducing the threats and promoting further enhancement of the security beneficence with regard to the authoritative control of the essential resources and the institutions.
- **Public-Private Partnerships:** In order to lay foundation of a sustainable approach toward cybersecurity ecosystem; there are three prime stakeholders in Pakistan they should involve academia, private and government sector. CYBER SECURITY RESEARCH 17 Government support, that is, sponsorship alongside business capital could be effective in boosting growth and provide human resource in the long run.

- **Diversify Technological Partnerships**: As a way of managing risks, it is important to look for technological partnerships outside of the usual partners that are the US and Europe. In order to avoid dependence on a few countries, Pakistan must also diversify its partnership and consider engagements with Countries from Asia, Africa and Latin America partners etc. It also deepens other forms of technological access and innovation and solidifies geopolitical relationships, which will be more adaptive in the long run whether there be uncertainties globally or not. Cisco's diversifying of technological alliances has suggested a better, safer environment for the economic and technological growth.
- **Invest in Domestic AI and R&D**: Thus, Pakistan needs to invest in research and development so that the country can design its solutions that can replace the dependence on foreign products and solutions. To fill these gaps, decision-makers in universities, research labs, and private enterprises must work together to build contemporary cybersecurity solutions needed in the country. Providing preference to local expert knowledge and raw materials, Pakistan can build up its computer security systems, ensure its technological sovereignty, and increase its competitiveness in the international market. This sort of teamwork will be instrumental in setting a foundation of robust, sustainable security frameworks meeting present and future cyber threats and safeguard national concerns.
- **Promote Digital Sovereignty**: Pakistan needs to start developing a proper AI ecosystem that would enable the country to protect digital assets and other important infrastructure. The four highlighted benefits of creating indigenous AI capabilities for Pakistan include; maintaining sovereignty, improving cybersecurity, and the reduced dependence on foreign technologies. The strengthening of AI defence capabilities will protect the national interests against new threats, so enhancing the positive AI impact and ensuring the Pakistan digital future, also enhancing the capability of the long-term economic and technology development.

- **Engage in Diplomacy**: One policy recommendation for Pakistan as a country is to maintain a balanced diplomacy. On one hand, Pakistan should persue and maintain strategic cooperation with china as it would bring investment, infrastructure and technology. In contrast, Pakistan needs to carved its stakes in technology and cyber security while bargaining with United States to guarantee supply of necessary defence and technological equipment. This two-pronged strategy would allow Pakistan to navigate around opportunities with these two powers while protecting its national security, its digital independence and its economic development as well as have good relations with the world's leading actors.

Conclusion

The Sino-US tension in Artificial Intelligence and cyber warfare therefore pose both threats and opportunity to Pakistan. On one hand, the growing cyber-attacks specially using AI has created a significant threat to Pakistan's National Security, important infrastructures and economy. The Sino American antagonism that features an emergent independent cyber warfare, could map Pakistan as an impending attack or target territory in this cyber war. From government based hackers, spies, or cyber-attacks on Pakistan's vital installations the dangers of being in the line of fire are all too real and increasing.

In building homegrown AI and enhancing cybersecurity, Pakistan has an opportunity not only to protect itself from cyber warfare but also be a regional power. The enhancement of cybersecurity measures, the further investment in Research and Development of AI and the enhancement of cooperation with national and international partners will improve the opportunities for new technological advancements, economic growth and strategic cooperation.

Uniquely navigating this aspect of an international system in a post-American World, and at the same time sustaining a robust technological standing, is going to be the defining moment for Pakistan's future in a world powered by technology, spearheaded by two dominant powers; China and America. A more explicit cybersecurity policy, development of AI appropriate to the needs of nations and regions, and incorporation of cybersecurity traits into the Pakistan economy and administration, the country can

decrease its vulnerability and adopt all of the opportunities that arise from participating in a technology oriented economy. July, through the international collaboration as well as the methodical plan on the multifaceted cybersecurity in Pakistan, this nation is capable to manage the conditions of this new age, achieving the defense of its interests and joining with furthering of the entire South Asian area.

References:

Nye, J. S. (2013). From bombs to bytes: Can our nuclear history inform our cyber future? *Bulletin of the Atomic Scientists, 69*(5), 8–14. https://doi.org/10.1177/0096340213501338

Nye, J. S. (2013). From bombs to bytes: Can our nuclear history inform our cyber future? *Bulletin of the Atomic Scientists, 69*(5), 8–14.

Nye, J. S. (2013). From bombs to bytes: Can our nuclear history inform our cyber future? *Bulletin of the Atomic Scientists, 69*(5), 8–14.

Kendall, F. (2023). U.S.-China race for technological superiority and AI. *Air & Space Forces Magazine*. Retrieved from https://www.airandspaceforces.com/kendall-us-china-race-technological-superiority-ai/

Ball, D. (2023). China's cyber warfare capabilities. *Strategic Studies Quarterly*.

Centre for Joint Warfare Studies (CENJOWS). (n.d.). China's algorithmic warfare: Strategic implications of AI-driven military operations. Retrieved from https://cenjows.in/chinas-algorithmic-warfare-strategic-implications-of-ai-driven-military-operations/

Nye, J. S. (2011). *The future of power*. PublicAffairs.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Clarke, R. A., & Knake, R. K. (2012). *Cyber war: The next threat to national security and what to do about it*. HarperCollins.

Kaplan, F. (2016). *Dark territory: The secret history of cyber war*. Simon & Schuster.

Rid, T. (2013). *Cyber war will not take place*. Oxford University Press.

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. RAND Corporation.

Goldsmith, J., & Wu, T. (2006). *Who controls the internet? Illusions of a borderless world*. Oxford University Press.

Kremer, J. F., & Müller, B. (Eds.). (2013). *Cyber security: A multidisciplinary approach*. Springer.
Healey, J. (Ed.). (2013). *A fierce domain: Conflict in cyberspace, 1986 to 2012*. Cyber Conflict Studies Association.