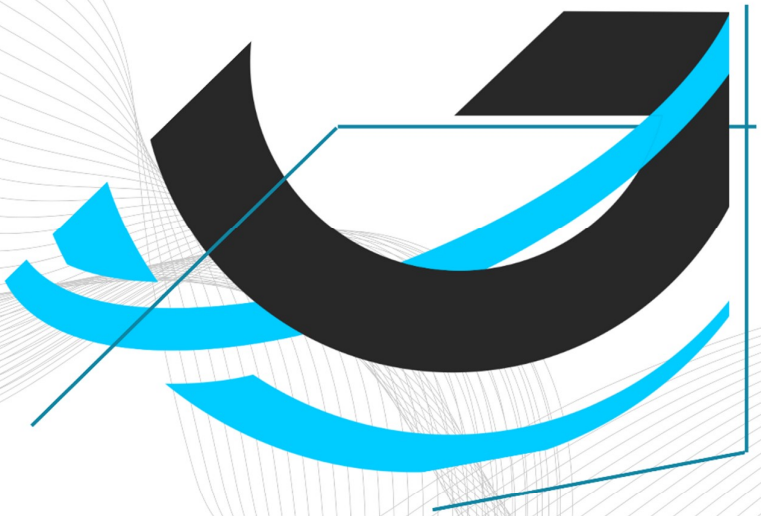
p-ISSN : 2708-2121 | e-ISSN : 2708-3616
DOI(Journal): 10.31703/gsssr
DOI(Volume): 10.31703/gsssr/.2024(IX)
DOI(Issue): 10.31703/gsssr.2024(IX.I)

www.gsssrjournal.com

Global Strategic and Security Studies Review
surveilling humanity

GSSSR

GLOBAL STRATEGIC & SECURITY STUDIES REVIEW



VOL. IX, ISSUE I, WINTER (MARCH-2024)

HumanityPublications
sharing research
www.humapub.com
US | UK | Pakistan

Double-blind Peer-review Research Journal
www.gsssrjournal.com

Humanity Publications(HumaPub)
www.humapub.com
Doi:https://dx.doi.org/10.31703

Article Title

The Role of AI in Hybrid Warfare: A Case Study of Pakistan's Cybersecurity Landscape

Global Strategic & Security Studies Review

p-ISSN: 2708-2121**e-ISSN:** 2708-3616

DOI(journal): 10.31703/gsssr

Volume: IX (2024)

DOI (volume): 10.31703/gsssr.2024(IX)

Issue: I Winter (March-2024)

DOI(Issue): 10.31703/gsssr.2024(IX-I)

Home Page
www.gsssrjournal.com

Volume: IX (2024)
https://www.gsssrjournal.com/Current-issues

Issue: I-Winter (March-2024)
https://www.gsssrjournal.com/Current-issues/9/1/20234

Scope
https://www.gsssrjournal.com/about-us/scope

Submission
https://humaglobe.com/index.php/gsssr/submissions

Google Scholar

Visit Us

Abstract

Technological advancements driven by artificial intelligence (AI) impact social, economic, and military sectors. This research paper explores the relationship between AI and cybersecurity in hybrid warfare. While AI boosts economic development and social betterment, its militarization poses significant risks, especially in asymmetric warfare, where AI-guided attacks can undermine targeted states' economies, infrastructure, and institutions. The paper emphasizes the role of neural network technologies in cyber operations and defense strategies. The absence of legal norms for AI in military actions exacerbates the threat of cyber-terrorism. Focusing on Pakistan's weak cyberinfrastructure, the paper highlights the challenges and opportunities for nuclear-armed states. To strengthen the argument this study implies the case study of Pakistan which faces serious cyber-attacks and cyber operations. Pakistan is known as a theater of Hybrid warfare. So these cyber-attacks and other hybrid strategies can be used against Pakistan to paralyze it.

Keywords: AI, Cyber-Warfare, Cyber Terrorism, Pakistan, Hybrid Warfare

Authors:

Hira Bashir: Associate Research Officer, Centre for International Strategic Studies, Azad Jammu and Kashmir, Pakistan.

Wajiha Zarish: MPhil Scholar, National Defence University, Islamabad, Pakistan.

Rimsha Malik: (Corresponding Author)
Associate Research Officer, Centre for International Strategic Studies, Azad Jammu and Kashmir, Pakistan.
Email: rimsham156@gmail.com

Pages: 86-93

DOI: 10.31703/gsssr.2024(IX-I).08

DOI link: https://dx.doi.org/10.31703/gsssr.2024(IX-I).08

Article link: http://www.gsssrjournal.com/article/A-b-c

Full-text Link: https://gsssrjournal.com/fulltext/

Pdf link: https://www.gsssrjournal.com/jadmin/Auther/31rvIolA2.pdf

Humanity Publications (HumaPub)
www.humapub.com
Doi:https://dx.doi.org/10.31703

Citing this Article

08		The Role of AI in Hybrid Warfare: A Case Study of Pakistan's Cybersecurity Landscape						
		Author	Hira Bashir Wajiha Zarish Rimsha Malik		DOI	10.31703/gsssr.2024(IX-I).08		
Pages		86-93	Year	2024	Volume	IX	Issue	I
Referencing & Citing Styles	APA	Bashir, H., Zarish, W., & Malik, R. (2024). The Role of AI in Hybrid Warfare: A Case Study of Pakistan's Cybersecurity Landscape. *Global Strategic & Security Studies Review, IX*(I), 86-93. https://doi.org/10.31703/gsssr.2024(IX-I).08						
	CHICAGO	Bashir, Hira, Wajiha Zarish, and Rimsha Malik. 2024. "The Role of AI in Hybrid Warfare: A Case Study of Pakistan's Cybersecurity Landscape." *Global Strategic & Security Studies Review* IX (I):86-93. doi: 10.31703/gsssr.2024(IX-I).08.						
	HARVARD	BASHIR, H., ZARISH, W. & MALIK, R. 2024. The Role of AI in Hybrid Warfare: A Case Study of Pakistan's Cybersecurity Landscape. *Global Strategic & Security Studies Review,* IX, 86-93.						
	MHRA	Bashir, Hira, Wajiha Zarish, and Rimsha Malik. 2024. 'The Role of AI in Hybrid Warfare: A Case Study of Pakistan's Cybersecurity Landscape', *Global Strategic & Security Studies Review*, IX: 86-93.						
	MLA	Bashir, Hira, Wajiha Zarish, and Rimsha Malik. "The Role of Ai in Hybrid Warfare: A Case Study of Pakistan's Cybersecurity Landscape." *Global Strategic & Security Studies Review* IX.I (2024): 86-93. Print.						
	OXFORD	Bashir, Hira, Zarish, Wajiha, and Malik, Rimsha (2024), 'The Role of AI in Hybrid Warfare: A Case Study of Pakistan's Cybersecurity Landscape', *Global Strategic & Security Studies Review,* IX (I), 86-93.						
	TURABIAN	Bashir, Hira, Wajiha Zarish, and Rimsha Malik. "The Role of Ai in Hybrid Warfare: A Case Study of Pakistan's Cybersecurity Landscape." *Global Strategic & Security Studies Review* IX, no. I (2024): 86-93. https://dx.doi.org/10.31703/gsssr.2024(IX-I).08.						

e-ISSN:2708-3616 Volume: IX (2024) Issue: I-Winter (March-2024) p-ISSN:2708-2121

Global Strategic & Security Studies Review
www.gsssrjournal.com
DOI: http://dx.doi.org/10.31703/gsssr

Pages: 86-93 URL:https://doi.org/10.31703/gsssr.2024(IX-I).08 Doi: 10.31703/gsssr.2024(IX-I).08

Title

The Role of AI in Hybrid Warfare: A Case Study of Pakistan's Cybersecurity Landscape

Contents

Abstract

Technological advancements driven by artificial intelligence (AI) impact social, economic, and military sectors. This research paper explores the relationship between AI and cybersecurity in hybrid warfare. While AI boosts economic development and social betterment, its militarization poses significant risks, especially in asymmetric warfare, where AI-guided attacks can undermine targeted states' economies, infrastructure, and institutions. The paper emphasizes the role of neural network technologies in cyber operations and defense strategies. The absence of legal norms for AI in military actions exacerbates the threat of cyber-terrorism. Focusing on Pakistan's weak cyberinfrastructure, the paper highlights the challenges and opportunities for nuclear-armed states. To strengthen the argument this study implies the case study of Pakistan which faces serious cyber-attacks and cyber operations. Pakistan is known as a theater of Hybrid warfare. So these cyber-attacks and other hybrid strategies can be used against Pakistan to paralyze it.

Authors:

Hira Bashir: Associate Research Officer, Centre for International Strategic Studies, Azad Jammu and Kashmir, Pakistan.

Wajiha Zarish: MPhil Scholar, National Defence University, Islamabad, Pakistan.

Rimsha Malik: (Corresponding Author) Associate Research Officer, Centre for International Strategic Studies, Azad Jammu and Kashmir, Pakistan.
Email: rimsham156@gmail.com

Keywords: AI, Cyber-Warfare, Cyber Terrorism, Pakistan, Hybrid Warfare

Introduction

In the current age, AI plays a very significant role in every domain. AI is effectively playing its role in different domains like social, economic, and now military as well. In the social and economic domain, the role of AI is to enhance the strategies and methods that can boost the economy of the country. And in the social sector to improve the lives of humans.

AI technology applies to speech recognition, biometric systems like fingerprint identification, mobile mapping, navigation and traffic control and management, manufacturing, supply chain operations, data acquisition, and targeted online advertising.

AI in the Military: The application of AI in the military sector is well-developed, which improves general military performance. The US Department of Defense describes this as combat capability,

which is concerned with the attainment of certain combat features and is affected by modernization, structure, preparedness, and sustainability. (Adib Bin Rashid et al., 2023)

Cyber Warfare: Certainly, the internet has changed conventional warfare, particularly through hacking attacks on commercial and governmental organizations. It will also be seen that AI and autonomous systems are expected to contribute significantly to future warfare.

Neural Network Technology: Neural networks as AI technologies are widespread in cyber operations and can be used in ITS, environmental prognosis, information filtering in social networks, and financial markets. These technologies are crucial for the defense of armies.

Military Decision-Making: There must be lots of information about resources and capabilities and that includes human resources, vehicles, types of equipment, and artilleries among others. These decisions can be aided by integrated frameworks that combine high and low-level decision-making strategies and plans with the aid of a number of methods in AI. Neural Network Technology: Neural networks are widely used in information warfare and can be used in ITS, FMC, ENV, and SMC. These are some of the major technological advancements crucial in warfare.

Making choices in the Military: Decision-making in this field involves information on the available resources such as personnel, gadgets, cars, weapons, artillery, etc. Besides, these decisions might be aided by AI through integrated frameworks that use a range of AI techniques for the processing of comprehensive plans and high-level strategies (The Upwork Team, 2023).

However, the militarization of AI can have more negative impacts than positive. Following the third military revolution states started to build up technology based on AI which is more fast and robust in nature. Military application of AI is an emerging domain and many states have ambitions in this domain. The advancement in the domain of AI can change the strategic landscape. The technology based on AI also possesses the potential to change the future global nuclear order. With the passage of time, AI technology is improving. So, this technology can transform the nature of warfare in the future. So the military application of AI will enhance state defense and security. However the militarization of AI will bring serious challenges for states security. In the current age, this domain also has an impact on hybrid warfare. There are five features of hybrid warfare which are "Synergy, ambiguity, asymmetry, innovative disruption, and battle over psychology" (Sheikh, 2021).

All of these five features of hybrid warfare with the integration of AI will receive "strategic modality" (Azad, 2022). So the technology acquired with the integration of AI can be used as a tool of hybrid warfare. AI can be more lethal when it comes to asymmetric warfare because this technology possesses the potential of "Complete Disruption" and has the power to "hijack every domain of life" (Sheikh, 2021) of the target state. The militarization of AI possesses the power to paralyze the economy, social organizations, and institutions of an enemy state. To regulate the AI domain there are not any bilateral agreements, international law, and organizations. So its impact can be more lethal. In terms of the military: AI is integrated with the technology of land, air, sea, space, and cyberspace. All these domains can be used the launch a hybrid attack against the enemy state. So because of having smart, accurate, and disruptive fractures, we can say that "AI is the key enabler of hybrid warfare" (Hanlon, 2018).

The militarization of AI is a very vast domain. It's very difficult to cover every aspect of AI in a single study. So, this study will only discuss the role of AI in the cyber domain and furthermore, this study will discuss how the cyber domain can be used as a tool of hybrid warfare. To strengthen the argument this study will also cover the case study of Pakistan to explain how the cyber domain is being used to launch cyber-attacks in Pakistan. As I chose the case study of Pakistan because Pakistan lacks in this domain and there are many vulnerabilities of Pakistan in the cyber domain. According to the federal minister (IT) Syed Amin ul Haque Pakistan faces over "900,000 hacking incidents" (Express Tribune, 2023) on a daily basis. While the opponents of Pakistan like India, the US, and Israel are far away from Pakistan in this domain.

Research Methodology

When it comes to research methodology, the qualitative method of research is used to explore the facts and formulate the result. As a research design, this research applies exploratory research and case

studies. In this research, the case study of Pakistan is analyzed to understand how AI in terms of the cyber domain can be used as a tool of hybrid warfare. This research is qualitative, and data is collected through secondary sources. Secondary sources included research papers, news articles, opinion papers, journal articles, and official policy documents to analyze different aspects of the study. And 'case study method of analyses is used.

Theoretical Framework

As a theoretical framework the "securitization theory" is applied to strengthen the argument. Barry Buzan and Ole Weaver gave this concept, "securitization theory focuses on the role of institutional actors such as political leaders in articulating and labeling threats, emphasizing how it is these actor's position of power over the wider public and ability to impact state policy that makes them legitimate securitizing actors" (Buzan & Waever, 2003). Moreover this theory "based the meaning of security upon the socially constructed practice among actors" (UKEssays, 2018). As cyberspace is a manmade domain. This domain for social use can enhance and improve the standards of life but the use of cyber in the military domain brings challenges for states and also possesses the potential to threaten human life. So when cyber is being used as a tool of hybrid warfare it would have serious implications for both states and mankind.

Military Application of AI

There is not any single definition of AI due to a lack of consensus over this domain because of its complexity. But for this research, AI is defined as "robots or machines which can perform the task autonomously and these robots and machines possess the ability to perform a task which normally requires human intelligence." (Britannica, n.d.) There are four main elements that are essential for the development of AI which include deep learning, computing powers, big data, and algorithms. AI is categorized mainly into three types. This division is based on the capacity, capability, and ability of a machine to perform tasks:

1. ANI (Artificial Narrow Intelligence) (Spiceworks, 2022). The machines that fall under this category can perform tasks like “translation, speech, and image recognition.” These machines require less computing power, data learning, and simple algorithms.
2. AGI (Artificial General Intelligence) (Lutkevich, 2022). The machines that fall under this category possess the ability of "autonomous consciousness which is near to human Intelligence" (Rafiq, 2021). These machines are able to do complex tasks like understanding problems, formulating plans, and solving complex problems. So these machines require multifaceted computing complex algorithms and big data.
3. ASI (Artificial Super Intelligence) (Mucci & Stryker, 2023). These machines can be described as humanoid robots that will possess capabilities and intelligence even higher the humans.

So, because of such smartness application of AI is applied in different domains to perform tasks quickly and easily. Currently, AI is successfully performing roles in medicine, agricultural areas, and industrial domains, for manufacturing of goods, health care domain, and the military. This research is focused on the military application of AI and discusses the technology that mostly falls under AGI. In the domain of the military according to "Dimitri Scheftelowitsch” (Scheftelowitsch, 2019) there are two types of applications of AI in the military:

1. The first type is described as “autonomous robotic devices.” For example UAVs, drones underwater autonomous vehicles, and autonomous tanks.
2. The second type is described as "stationary application." Such kind of applications can be seen in BMDs, radar systems, ISR, nuclear command and control, early warning systems, surveillance, and cyber capabilities.

Cyberspace as a Tool of Hybrid Warfare

Cyberspace is a manmade domain and potentially can be used in the military domain to attack the enemy state. According to Kuehl "A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information-communication technologies" (Robinson, Jones, & Janicke, 2015).

With the recent advancement in cyber warfare, there have been more and more frequent incidences of asymmetrical threats to state-based databases and decision-making processes. Hybrid warfare methods have impacted advanced technical defense, including Iran's industrial control facilities successfully targeted by the Stuxnet virus that exposed crucial data and rendered pre-arranged control over manufacturing machinery (Kaunert & Ilbiz, 2021). This underscores the urgent need for countries like Pakistan to adequately enhance their cybersecurity arrangements. As it has been seen in recent times Pakistan has faced many cyber-attacks in financial markets, commerce, health sectors, energy, and national security sectors. It was when there was a weakness in almost every bank in Pakistan during November 2018 including embezzlement of vast amounts of money (Li & Liu, 2021).

Such scenarios for some reason call for effective standards and practicable measures aimed at enhancing the structures and frameworks of national security threats in warfare have evolved not only physically but also virtually; people have graduated to state aggression, propaganda, and spying as part of cyber weapons. Amid these threats and to form a common front against cyber warfare, new information and cyber strategies, standard operating procedures, and tangible capabilities are needed. Current solutions are not adequate, and that is why it is necessary to develop and implement complex cyber security approaches promptly if the emerging threats are to be effectively countered (Safitra, Lubis, & Fakhrurroja, 2023).

In the current age, we frequently come across the word cyber warfare, cyber warfare refers to the "exploitation of cyberspace" for military interest and as well to launch cyber-attacks against the target actor. So such cyber-attacks and exploitation can be defined as "Cyber warfare can be a conflict between states, but it could also involve non-state actors in various ways. In cyber warfare, it is extremely difficult to direct precise and proportionate force the target could be military, industrial, or civilian or it could be a server room that hosts a wide variety of clients, with only one among them the intended target" (Beidleman, 2009). So there can be seven types of cyber-attacks which are named as "Espionage, Sabotage, Denial of services attack, Electrical power grid, Propaganda attacks, Economic disruption and Surprise attack." To launch these attacks states build up offensive cyber tools by using AI like malware worms and viruses. Likewise states also develop defensive tools for the security of cyberspace. The term hybrid warfare is defined as "the synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects" (Cullen & Kjennerud, 2017). To understand the AI as a tool of hybrid warfare it's important to know that it's the age of globalization in which people are connected through different communication networks. Military state actors and other organizations also use this technology in their daily life routines.

Cyber warfare, as a form of hybrid warfare, is more threatening. But yes, even if industrialized countries have taken high-end technologies to protect their cyber-space to some extent, loopholes are still there. But, in the present world more prone to cyberwarfare threats include countries such as Pakistan which do not have the resources to invent new technologies or technology systems. The unstable scenario in Pakistan has led to the lack of focus on this important subject which worsens the condition of Pakistan's online problems.

When it comes to cyber-attacks these networks and communication sources are vulnerable to cyber-attacks. Likewise in cyber domain information, propaganda is a very common tool used by states to achieve their interest. So when a cyber-attack occurs it creates synergistic effects. So cyber-attacks when occur without any exclusion impact the military and population. Ducaru says that "the cyber-attacks about hybrid warfare can be called the cyber domain of hybrid warfare." The Russian strategy against Ukraine is an example of a hybrid war, Russia in its strategy used cyber warfare, EW, information warfare, and physical attacks on communication networks to fulfill its interests like annexation of Crimea. Then US launched the attack against the nuclear facility of Iran by using a "malicious computer worm" named Stuxnet. So by using the cyber domain states can attack their enemy while sitting far away and by sending a virus they can get the desired result. Now there is not any need for big militaries to fight the war. In current age the AI AI-based technology and tools are there to fight the war on behalf of states. So offensive cyber tools can be used to launch both kinetic and non-kinetic cyber operations.

Cyber Warfare and Case Study of Pakistan

This issue focuses on how developments in artificial intelligence and cybersecurity have influenced the current cyber threats and countermeasures. It is expected that the expenses as a result of cybercrime will be about $10. 5 trillion each year by the year 2025, with ransomware attacks projected to cost $265 billion each year by the year 2031. Unsurprisingly, generated AI by hackers has increased the rate and intensity of cyber-attacks with 85 % of cybersecurity experts pointing to it as the root cause of the increased cases of cyber incidents (Morgan, 2020). This has raised fears of privacy violations, invisible phishing, and the progression of cyber-attacks in terms of frequency and speed. The average data breach cost is on the increase, which now stands at $4. 45 million all over the world by 2023. This indicates that the U. S. is at the top of the list with higher costs of data breaches at $5. 09 million. Remote work intensifies these perils besides adding major costs to breaches. Manufacturing and healthcare sectors are among the most targeted industries; the mean cost of a healthcare breach is around $10,950,000. IT protection spending is expected to increase by 14%. 3% in 2024 when cyber risks are on the increase hence the rationale why advanced cybersecurity policies and precautions are required to minimize the potential risks that come with AI criminal activities (Fox, 2024).

Pakistan lacks in the domain of cyber as compared to its enemy states like India, the US, and Israel. So most of the time Pakistan faces cyber-attacks from these states. The following table shows the rank of Pakistan in the Global Innovation Index.

Table 1

Global Innovation Index Comparison

Country	Rank (2019)	Rank (2022)
India	52	40
Pakistan	105	87
Sri Lanka	89	85
Bangladesh	116	102

SOURCE: World Intellectual Property Organization, 2022

As shown in Table 1 the rank of India in the Global Innovation Index 2022 is 40 among 132 states while Pakistan ranked at 87. So India because of its progress in the AI domain is having edge over Pakistan. There are many vulnerabilities in Pakistan in the cyber domain. Some vulnerabilities of Pakistan are discussed in Table 2:

Table 2

Pakistan's major vulnerabilities in cyber-space

Vulnerability	Reasonability	Effect
NADRA	Keeping the record of the population.	If the system of NADRA gets hacked by an enemy state it can used against Pakistan to achieve the desired result. And it can be devastating.
National Power Control Center	It's responsible for the "power distribution" of WAPDA.	If this system gets attacked then the power system of Pakistan can be paralyzed. This power system can exploited with the employment of other instruments of hybrid warfare to create a synergistic effect.
Pakistan's Sui Gas network	Providing Energy.	This system heavily depends on cyberspace for regulation. If this system receives a cyber-attack Pakistan can face a serious energy crisis.
Communication Networks	Communication and Connectivity.	Four submarine cables are being used to connect Pakistan to the global internet. If these cables receive attack from the enemy Pakistan will face failure of internet connectivity.

The following table shows some vulnerabilities of Pakistan in the domain of cyber. If Pakistan faces any attacks on the above-listed domains then would create a synergistic effect and will bring a serious crisis for Pakistan. There are a number of cyber-attacks which are listed against Pakistan. This article covers two cyber-attacks to strengthen the argument. First "Operation Hangover" in 2009-10 India launched massive espionage activities against Pakistan along with other states. Its details were revealed by a Norwegian firm named "Norman Securities" in 2013. The main aim of this operation was to gather information related to security matters in Pakistan (Fagerland, Kråkvik, & Camp, 2013).

Then the spying program of the US was named PRISM (Greenwald & MacAskill, 2017). It was also again for espionage purposes. Because of this program, the national security of Pakistan was undermined and information of many officials of Pakistan was gathered. Then Israel also aided India in launching cyber-attacks against Pakistan related to nuclear weapons through information and media propaganda. These campaigns mostly have a psychological impact that terrorists can approach the nuclear weapons of Pakistan. India-Israel nexus also launch a cyber-attack against Pakistan to isolate it in the region (The Diplomat, 2020).

So, Pakistan remained in turmoil from 2005-15, these cyber-attacks can be linked with other hybrid incidents happening at the same timeframe. In the current scenario Pakistan is facing political and economic unrest along with cyber-attacks like attacks on FBR (Shabaz, 2021) and audio leaks of officials show Pakistan is again under cyber-attack. And more recently Pakistan is also faced terrorist attacks. All these events are happening in the same time frame. Using the cyber domain along with other hybrid strategies can put Pakistan in a devastating situation

Way Forward for Pakistan

In the past and most recently Pakistan has faced a lot and received serious cyber-attacks. Pakistan gradually realizes the importance of the cyber domain. It is because, due to the multifaceted nature of hybrid warfare, it becomes imperative to work on strengthening Pakistan's cybersecurity apparatus as a critical aspect of safety. The initial step is to introduce senior politicians to the subject, prove that hybrid warfare is a present threat, and propose a full-scale countermeasures concept. It should be an end-to-end approach initiated and managed by a specific ministry, potentially including the creation of a unified narrative that tackles mis/disinformation and improves national morale. This work is associated with considerable financial, material, and human expenses; it is necessary to report to the Prime Minister and Parliament. For effective addressing of these threats, it hence calls for;

The country needs to develop a broad policy that would incorporate civil-military Integration vital when implementing the policy is especially important in combating cyberspace threats. This means pulling the relevant stakeholders from different fields in order to create more threat vectors and also rewriting the military threat hypotheses to fit all the aspects of hybrid threats. This is through the enhancement of relations with friendly nations for the enhancement of digital shields and the adoption of worldwide best practices concerning cybersecurity as the major stands. To ensure that Pakistan has a properly defended cyber infrastructure, it is necessary to influence the universities developing Policies and technology.

Therefore, employing the youth or training young cyber warriors, is vital in order to invest in human resources which will help in building a strong framework of cybersecurity. Such personnel should be able to deter several facets of hybrid threats within small, and professional teams. Also, reducing the imports of technology through the development of hardware and software manufacturing is important. Hence it respects the property and reduces the risks of wiretapping and hacking incidences. Last, it is essential to energize defensive information processes within and concerning the state and social media in an attempt to disseminate more pleasant narratives and counter undesirable broadcasts. That is why it is necessary to introduce orders and ideas, create themes that would increase patriotic feeling and morale in the society, as well as counter all the threats of hybrid warfare, and maintain Pakistan's cybersecurity.

Pakistan is trying to secure the cyber domain and has taken several initiatives for the security of the cyber domain. Following initiatives have been taken by Pakistan in this regard, "Prevention of Electronic Crimes Ordinance (PECO), Prevention of

Electronic Crimes Bill 2015, Prevention of Electronic Crimes ACT 2016, and establishment of National Response Centre for Cyber Crime under the auspices of Federal Investigation Agency (FIA)." Cyber-attacks against Pakistan harm the military as well population. So Pakistan needs to create awareness among the people regarding this domain. Currently, Pakistan is in a defensive mood to deter the enemy in the cyber domain Pakistan needs to build up offensive cyber tools along with defensive ones. It needs time to invest in this borderless domain as Pakistan is among the top 10 countries that are vulnerable to cyber threats. At the international level, there should be a regulatory body that solely deals with emerging issues regarding the cyber domain for international security.

Conclusion

Integration of AI in the military domain especially cyberspace with offensive tools can be more lethal and devastating for a state. Studies show that AI-based technology has been used several times as a tool of hybrid warfare. The cyber domain is the most frequently used domain along with other hybrid strategies to create a synergistic effect. The use of cyber domain along with other strategies can be seen in the case of Pakistan, the Russia-Ukraine conflict, use of Stuxnet against Iran. These studies show that states prefer to use cyber domain against states because it's cheap and a small malicious computer worm can cripple a whole state. Cyber-attacks also keep the attacker secret. In such attacks, states don't face any blame or trial. So we can say that AI is a potential tool of hybrid warfare because when it's applied the five features of hybrid warfare which are synergistic, battle over psychology, disruptive innovation, ambiguity, and asymmetry receive strategic modality. Pakistan is not an exception in this regard. On a daily basis, Pakistan faces a number of cyber-attacks. Pakistan needs to build up more advanced infrastructure to fight in the domain of cyber. To secure the cyber domain Pakistan needs to invest more in this domain and also needs to build more advanced and sophisticated cyber tools to enhance the security of the cyber domain.

In order to address current and emerging threats and challenges AI brings to the cybersecurity environment it is necessary to develop a coherent tactical and strategic concept, which implies the understanding of how AI affects the world of cybersecurity while recognizing the opportunities provided by AI-based security and threats emerging through the use of AI by the adversaries. To be effective at preventing novel threats in AI, recognizing the latest trends, technologies, and research in AI and cybersecurity is extremely important. Using IAST and RASP as AI-based security tools can help safeguard against AI attacks while having the AI adapt to evolving threats. System security also needs to be cultivated within organizations in order to promote a culture of secure development, where personnel also receive updated regular security briefings and training. Interacting with the security community, such as the exchange of information and ideas with security specialists, researchers, and citizens, enhances the possibility of creating appropriate countermeasures to known or emerging threats from AI in the cyber domain.

To effectively prepare for new and different threats, one must implement a long-term security plan that reviews and refreshes security strategies, procedures, and systems periodically and funds ongoing security R & D. Last but not least, the assessment of legal and ethical factors ensures that the envisioned application of AI in cybersecurity is aligned with data protection legislation, ethical guidelines, and company policies. By following these recommendations, and addressing the rapidly advancing AI-based cyber threat environment, developers, organizations, and users can assist in preserving their digital assets and promoting and supporting a safer internet for everyone. The advancement of AI technologies is still continuous and we should be vigilant, be informed of the experiences of other people, and foster cooperation to come up with better and safer AI technologies.

References

Azad, T. M. (2022). Cyber warfare as an instrument of hybrid warfare: A case study of Pakistan. *South Asia Journal of South Asian Studies*.
Google Scholar Worldcat Fulltext

Beidleman, S. W. (2009). *Defining and deterring cyber war* (pp. 9-10). Army War College, Carlisle Barracks, PA.
Google Scholar Worldcat Fulltext

Buzan, B., & Wæver, O. (2003). *Regions and powers*. https://doi.org/10.1017/cbo9780511491252
Google Scholar Worldcat Fulltext

Fox, J. (2024, April 30). Top Cybersecurity Statistics for 2024. *Cobalt labs*. https://www.cobalt.io/blog/cybersecurity-statistics-2024
Google Scholar Worldcat Fulltext

Greenwald, G., & MacAskill, E. (2017, July 14). Boundless Informant: the NSA's secret tool to track global surveillance data. *The Guardian*. https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining
Google Scholar Worldcat Fulltext

Kaunert, C., & Ilbiz, E. (2021). *Cyber-attacks: what is hybrid warfare and why is it such a threat?* The Conversation. https://theconversation.com/cyber-attacks-what-is-hybrid-warfare-and-why-is-it-such-a-threat-164091
Google Scholar Worldcat Fulltext

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126
Google Scholar Worldcat Fulltext

Lutkevich, B. (2022, April). What is artificial general intelligence (AGI)? - Definition from WhatIs.com. *SearchEnterpriseAI*. https://www.techtarget.com/searchenterpriseai/definition/artificial-general-intelligence-AGI
Google Scholar Worldcat Fulltext

Morgan, S. (2020, November 13). *Cybercrime costs the world $10.5 trillion annually by 2025*. Cybercrime Magazine. Retrieved from https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
Google Scholar Worldcat Fulltext

Mucci, T., & Stryker, C. (2023, December 18). What is artificial superintelligence? | IBM. *IBM*. https://www.ibm.com/topics/artificial-superintelligence
Google Scholar Worldcat Fulltext

Rafiq, A. (2021). *Militarisation of artificial intelligence and future of arms control in South Asia*. Institute of Strategic Studies Islamabad (ISSI).
Google Scholar Worldcat Fulltext

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & Security*, *49*, 70–94. https://doi.org/10.1016/j.cose.2014.11.007
Google Scholar Worldcat Fulltext

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability*, *15*(18), 13369. https://doi.org/10.3390/su151813369
Google Scholar Worldcat Fulltext

Scheftelowitsch, D. (2019). The state of artificial intelligence: An engineer's perspective on autonomous systems. In V. Boulanin (Ed.), *The impact of artificial intelligence on strategic stability and nuclear risk: Euro-Atlantic perspectives* (pp. 27-28). Solna, Sweden: Stockholm International Peace Research Institute (SIPRI). https://www.sipri.org/sites/default/files/2019-05/sipri1905-ai-strategicstability-nuclear-risk.pdf
Google Scholar Worldcat Fulltext

Sheikh, H. (2021). AI as a tool of hybrid warfare: Challenges and responses. *Journal of Information Warfare*. https://www.jinfowar.com/journal/volume-21-issue-2/ai-tool-hybrid-warfare-challenges-responses
Google Scholar Worldcat Fulltext

Spiceworks. (2022, March 22). What is narrow artificial intelligence (AI)? Definition, challenges, and best practices for 2022. *Spiceworks*. https://www.spiceworks.com/tech/artificial-intelligence/articles/what-is-narrow-ai/
Google Scholar Worldcat Fulltext

The Upwork Team. (2023, August 16). How AI is used in decision-making processes. *Upwork*. https://www.upwork.com/resources/ai-in-decision-making
Google Scholar Worldcat Fulltext

UKEssays. (2018, November). Understanding the context of securitization theory philosophy essay. *UKEssays*. https://www.ukessays.com/essays/philosophy/understanding-the-context-of-securitization-theory-philosophy-essay.php?vref=1
Google Scholar Worldcat Fulltext

Rashid, A. B., Kausik, A. K., Sunny, A. a. H., & Bappy, M. H. (2023). Artificial intelligence in the military: An overview of the capabilities, applications, and challenges. *International Journal of Intelligent Systems*, *2023*, 1–31. https://doi.org/10.1155/2023/8676366
Google Scholar Worldcat Fulltext