Unity Journal
Vol.IV, 161-174, Feb 2023
Doi:https://doi.org/10.3126/unityj.v4i01.52237
Prithivi Narayan Shah Research Center
Directorate General of Military Training, Nepali Army
Kathmandu, Nepal.

Application of Artificial Intelligence in the Military: An Overview

Utsav Sharma Gaire*

Abstract

Modern-day research and innovation have expedited the proliferation of Artificial Intelligence (AI). Its impacts on society, economy, and power are ever-increasing. This paper highlights the remarkable advancements in the entire ecosystem of AI-associated technologies comprising machine learning, computer vision, natural language processing, robotics, brain-machine interface, etc., and their innovative usage in pioneering military technologies/strategies. This paper scrutinizes the unprecedented contingencies and challenges of AI application on three core facets of future defence, i.e., Autonomous Weaponry and Warfare, Intelligence, and National Security. Several powers in the "geopolitical chessboard" have already begun to exploit AI for military applications like intelligence analysis, surveillance, autonomous weaponry, reconnaissance, and logistics. This will eventually propel AI to be the new dimension of military strength evaluation and a pivotal entity for national security. This paper predicts the future of military applications, their constraints and challenges, and also recommends the steps to be pursued by technologically fragile countries like Nepal to acclimatize with these AI-induced transformations. The research will follow a qualitative methodology to analyse AI development and its military incorporation, challenges, and prospects. The review of the published articles, opinions, commentaries, and findings worldwide on AI-driven innovations underscores the results. In sum, the research aims to discuss the future of military applications in light of the burgeoning ecosystem of AI.

Keywords: artificial intelligence, cybersecurity, military strength, Nepal, security technology, contemporary challenges

Introduction

Artificial Intelligence (AI) is the engine driving the latest technological advancement. It can be referred to as the technology that endows machines with the capacity to perform tasks requiring 'intelligence'. Today, AI is emerging as an enthralling technology that can benefit the generations of humanity. AI proliferation in every sector has led to astounding progress.

* Civil Engineering Student at Thapathali Engineering College, Tribhuvan University
Email ID : Utsav.075bce141@tcioe.edu.np

The persistent research and innovation on AI have escalated advancements in every sector including impacts on the economy, society, and power-politics.

Economically, automation and digitization led by AI will have a significant impact on productivity and GDP potential. World Economic Forum refers to AI as the key driving force of the fourth industrial revolution (WEF, 2015). Research forecasts that AI could double annual global economic growth rates by 2035 (Szczepanski, 2019). PricewaterhouseCoopers forecasted that AI could contribute $15.7 trillion to the global economy in 2030. Out of this sum, consumption side effects share $9.1 trillion and increased productivity shares $6.6 trillion (PricewaterhouseCoopers, 2017). Also, the amount spent by companies on AI-related mergers and acquisitions was estimated as being 26 times larger in 2017 than in 2015 (Furman & Seamans, 2019). From these speculations, we can conclude that AI is substantially important in the future economy. AI along with its associated technologies is ubiquitously embedded into the different aspects of our lives without disrupting our comfort zone. They are already permeating various spheres of society with their broad range of impacts.

The health sector uses machine learning to predict treatment procedures, and breakthroughs in biotechnology and neurosciences. This combined with AI application will help manage and assess mental functions through implants (Malhotra, 2021). The tourism industry is revolutionizing with the introduction of virtual journeys through AR and VR technologies which creates more exciting experiences for tourists (Malhotra, 2021). Likewise, AI systems can be used to manage traffics, and predict flight delays (using computer vision) in the transportation sector (Gray, 2022). Similarly, the agricultural sector in planning to use AI systems for crop yield prediction, price forecasting, intelligent spraying, harvesting huge volumes at a faster speed (using robots), disease diagnosis, and suggestion of treatment procedures (Revanth, 2019). Through AI technologies, an intelligent learning system can be introduced in the educational sector which has the potential to improve teaching and learning practices, and boost students' performance and motivation. Furthermore, similar sectors like finance, art, and insurance will also transform by utilizing the nimble advancements of AI. For example, in Nepal, AI is used in smart restaurants where Robots serve the guests, and ride-sharing services like Pathao use AI to calculate the shortest way and fare of the trip (Suman, 2022). Many sectors of society are exclusively leveraging the progress of AI as explained above. Likewise, the military sector will be more advanced with AI integration which ultimately affects the power-political dynamics of the world, which will be explained below.

For a country to survive the tides and currents of power-political dynamics of the world, it should resiliently defend against its key security challenges, robustly handle its geopolitical complexities, and have a well-strengthened military. Military strength encompasses military strategy, doctrine, equipment, and warfare strategy as fundamental entities which intensify the combat readiness and sustainable capability of any military. The inclusion of AI will directly/indirectly affect these domains. The self-evolutional capabilities of AI make it crucial for the innovation/invention of advanced military strategies/technologies. As advancements are fostered, the operational approach of the militaries will start reshaping almost all domains i.e. land, sea, air, space, and information. Also, the modus operandi of several military applications like reconnaissance, surveillance, intelligence analysis, command and control, and logistics will be improved and enhanced as well. AI will change the operation of warfare, intelligence,

border security, cyber defense, emergency operations, counter-terrorism, and threat evaluation. With the change in functional and operational approach in all domains and applications, new paradigms of military power, geopolitical complexities, and national security issues will emerge which are discussed in the later sections of this paper. The military of any country should be well-acquainted with the advancements of AI to grapple with the operational benefits in these domains and survive the power-political dynamics.

This paper does not refer to AI in a sheer technical sense, but also includes the entire ecosystem of associated technologies/entities which exemplifies its computational and functional capabilities. These technologies are discussed later in the Advancements in AI entities section. It also predicts the functioning of an AI-equipped military, scrutinizing the three core facets of future defense i.e. Autonomous Weaponry and Warfare, Intelligence, and National Security with their encumbering challenges. In addition, it discusses how the global power-political domain is reshaping and big power competition is getting intense with the introduction of AI. Further, this paper charts the next steps to be undertaken by Nepal, in assessment of its present context, to acclimatize with the new AI environment

Literature Review

Scholarship is consistent in agreeing that AI advancement and its introduction have the potential to transform many sectors of our lives and society. AI, its upgraded hardware, availability of big data, and advancement in its associated technologies have collectively propelled the AI revolution in recent decades. Malhotra (2021) argues that the AI revolution will have intense ramifications in primarily five battlegrounds: economy, power, psychological control of desires and agency, metaphysics of self, and India's future. However, this paper only reviews the economic and power-political battleground for accomplishing its objectives. Regarding the economy, Schmidt (2022) claims that AI has the capability to transform every sector of the national economy and intensify global competition on digital platforms and services. Furman & Seamans (2019) state that AI will boost productivity growth but it may cause labour market upheaval. Likewise, government reports, leaders, and global platforms like World Economic Forum (WEF) have repeatedly endorsed AI's capability of transforming the military domain unprecedentedly.

The military domain will be more advanced with AI incorporation as it will extensively mutate the functional and operational approach of military applications. Malhotra (2021) claims that powerful countries are upgrading their military systems with smart autonomous weapons and advanced intelligence supported by higher computational and analytical abilities of AI. Hoadley & Lucas (2018), Schmidt (2022), and Svenmarck, Nilsson, & Schubert (2018) have similar claims. National security will also be impacted by AI's influence on the military and geopolitics. The National Security Commission on Artificial Intelligence (NSCAI) report of the US admits that the AI revolution will greatly impact their economy, national security, and welfare. Similarly, Schmidt (2022) asserts that the AI revolution will modify the way of exercising coercion and geopolitical influence on adversarial states. These claims from the scholars give a clear picture of the emerging new forms of tides and currents in the power-politics realm. Despite immense possibilities, there are several challenges that need to be taken care of before deploying AI applications for military purposes (Svenmarck et. al., 2018). The

RAND Corporation Report (2016) articulates several risks and challenges of AI integration in military applications.

To conclude, an analysis of the diverse literature of scholars showed enormous possibilities of AI incorporation transforming the aspects of the economy, military, national security, and power-politics provided the challenges are addressed effectively. This research, through proper interpretation and analysis of all these possibilities, tries to outline a basic futuristic conclusion i.e. AI will be a new dimension of military strength evaluation and a pivotal entity of national security. Up to now, the research done about AI hardly entails the impact of AI-driven developments on technologically fragile countries, like Nepal. So, this research aims to inspect such impacts and suggest some policy measures that a technologically fragile country can undertake to acclimatize to these transformations and their repercussions.

Methodology

This research follows a qualitative method to accomplish its objectives. The impacts of AI on various sectors are discerned following the recent news articles, magazines, and reports of several firms. The advancements in AI technologies are explicated through journal articles, books, opinions of think tanks, and online media platforms. The research attempts to explain the prospects of these advancements in the military domain. Several governmental and non-governmental reports, mainly report of the NSCAI of the US, the report of RAND Corporation, and other secondary sources are studied and interpreted to predict the operational approach of the above-mentioned three core facets of future defense. The research follows the analytical and interpretative approach to attest its core argument i.e. AI is the new dimension of military strength evaluation and a pivotal entity for national security.

A similar approach is adopted to analyze changing geopolitical dynamics and to determine the challenges of AI integration in the military. Content analysis of various online and other platforms is done to assess the situation of Nepal in AI development and its challenges. The challenges are then thoroughly navigated and measures that could help Nepal to make significant strides in AI development are proposed. The advanced mode of military applications of several countries is taken as a reference to introduce the AI-integrated military ways to defend against key security challenges of Nepal. The conclusions of the research are derived taking expert opinions, news articles, reports, and other sources into consideration to cover all bases.

Advancements in AI entities

Advanced hardware, big data, and associated technologies are foundational entities of AI. Nanotechnology, semiconductors, Graphical Processing Units (GPU), Tensor Processing Units (TPU), and so on are essential hardware for AI development. Big data is the bulk collection of different types of structured or unstructured or semi-structured datasets that are employed in the system to develop patterns or models. These models are of advanced intelligence which can be utilized in networking platforms or commercial sectors. Associated technologies of AI comprise machine learning, computer vision, natural language processing, robotics, and others which act as a force multiplier.

Machine learning is one of the key AI technologies which assists programs to learn by themselves through the data/experiences fed into it. It uses an adaptive learning technique. With

its exposure to unique data, the machine can identify patterns and adapt to them (Burns, 2021). Machine learning's coalition with the neural networks resulted in its marginal leap allowing the formulation of another superior technological approach called Deep Learning (Malhotra, 2021). Neural networks are modeled after the functioning of human neurons and deep learning trains the neural networks through the multi-layered processing of huge amounts of data. Thus, resulting in a magnificent rise in computational ability. Likewise, computer vision trains machines to analyze, interpret, and extract information from images, videos, and other visual inputs. Similarly, Natural Language Processing (NLP) augments AI capabilities by enhancing its ability to understand and interpret human language (NSCAI, 2021). It allows machines to recognize speech, summarize and make sense of spoken or written texts. Robots are known for performing specific and repetitive tasks but the permeation of AI in robotics will endow robots with the ability to perform complex and analytical tasks. Brain Machine Interface (BMI) functions as a link between the brain and machine, thus transforming the neuronal signals from the brain into actions as intended by the operator. The military usage of these advancements is discussed in the subsequent sections. The integration of these technologies with the military apparatus will bolster military proficiency by transforming the operational approach of any military application.

Both fronts of the Russia-Ukraine war deployed AI-enabled systems capable of collecting and analyzing battlefield data in ISR (Intelligence, Surveillance, and Reconnaissance) missions (Reşitoğlu, 2022). This news from the Russia-Ukraine war unveiled the changing dynamics of warfare brought about by AI. AI and its entities facilitate the innovation of game-changing military equipment and tactics. Further, weaponry can be upgraded through autonomous weapon systems. The autonomous weapon system will enhance diligence, speed, and overall performance thus providing substantial martial benefits (NSCAI, 2021). Conventional intelligence systems can be upgraded by AI-based autonomous systems capable of analyzing complex data and information which improves intelligence gathering, analysis, logistic system automation, and optimization (Suman, 2022). Several powerful countries are integrating their state and military apparatus with AI innovations/applications for their national security and interests which will emanate a new level of conventional and hybrid threats to any country. So, the domain of national security will also be affected by AI. Due to continuous innovation, advancement, and integration of cutting-edge technologies in the military sector, future defense is likely to be far more complex than the conventional one. The operational realm of three important domains i.e. Autonomous Warfare and Weaponry, Intelligence, and National Security will determine this complexity.

Autonomous Weaponry and Warfare

The advent of AI in the military propelled the emergence of new weaponry and warfare paradigms. Autonomous weapon systems have manifested themselves into real battlefields from science fiction movies. These systems can surpass human weaknesses as they can process complex sensory information from the battlefields and take instant action free of any emotions (NSCAI, 2021). With the advancement in Natural Language Processing (NLP), these systems can be controlled and operated by human commands. They are capable of offering consultations to the war commander and predicting the best tactics plan to be implemented in the warfare (Suman, 2022). Also, autonomous weapons enable the battlefields to expand and allow combat

to reach previously inaccessible places. They also allow the military to gobble up tactical and strategic advantages.

AI-empowered autonomous devices including unmanned aerial (UAVs), surface (USVs), and underwater vehicles (UUVs) can be employed to achieve tactical advantages in intelligence, surveillance, and reconnaissance (ISR) on the battlefields (Reşitoğlu, 2022). UAVs or drones, equipped with sophisticated cameras and sensors can be programmed to attack a specific individual or group of individuals by combining them with computer vision and satellite imaging--therefore reducing the collateral damages in military operations. The lethality of the air force can be increased with the help of a Multi-Domain Command and Control System which enables the troops to visualize the friendly and enemy forces. This system can consolidate data from air, sea, land, and cyberspace (Malhotra, 2021). Military training can be economized by the military simulations created using AI techniques (Campbell et. al., 1997). Autonomous systems can use predictive AI models for maintenance. The models should be capable of retrieving data from the system's engine and predicting when the next maintenance will be required. Similarly, artificial robotic warriors can also be of great military usage as they are capable of sustaining harsh climatic conditions and terrains without any supply obligations of food, medicines, and logistics. These warriors can also be employed to make war more humane reducing collateral damage and the number of humans participating in the war.

AI will transform the warfare mechanisms in every domain from undersea to outer space, including cyberspace and the electromagnetic spectrum. A new AI-dominated warfare paradigm is on the verge of a breakthrough. This is the warfare where algorithms came into play and battlefield advantage is attained by the side with adequate AI-enabled weapons in the field, quality and the amount of the adversary's military data, and best of AI-integrated operational mechanisms (NSCAI, 2021). Also, human-machine teaming can be improved considerably with the BMI (Brain Machine Interface) technology as it can assist warfighters in tasks requiring critical thinking, decision-making, and problem-solving (RAND, 2020). Every facet of warfighting will be equipped with AI changing the operational concepts of war. This warfare will not be confined to any specific platform or space rather break open into digital spaces through misinformation, disinformation, deep fakes, and cyberattacks. Any military which is vibrant in this paradigm of warfare equipped with the outstanding abilities of autonomous weapon systems will comfortably outmaneuver their adversaries. The enormous capabilities of the autonomous system have led to a rigorous arms race between powerful countries (Marr, 2021) raising humanitarian concerns all over the world. To address the concerns, 114 international leaders of the technology sector submitted a letter to the United Nations (UN) appealing to prevent an arms race stating autonomous weapons would "permit armed conflict to be fought at a scale greater than ever, and at timescales faster than humans comprehend" (Hoadley & Lucas, 2018).

Future evolutions in Natural Language Processing, computer vision and BMI will engender even greater possibilities for AI application in autonomous weaponry and warfare. As autonomous weapons are labeled as lethal weapons, their humanitarian, legal and ethical concerns should be addressed before integrating them into military applications.

Intelligence

The intelligence apparatus will benefit immensely by the higher computational and analytical capabilities of AI systems. The intelligence information grid will be flooded with numerous data incoming from the sensors, cameras, smartphones, and media and they will be strenuous to analyze (NSCAI, 2021). Also, the higher velocity of data inflow into any system makes it difficult to connect the dots in real-time. In addition, it is difficult to acquire legitimate and accurate data filtering misinformation and fake news from the huge volume. Higher capabilities of AI can augment the analysts to process the precise information from the high volume and velocity of data. Thus, automation of this laborious task helps a human analyst to take timely decisions efficiently and effectively.

AI-powered intelligence will be effective in dealing with counter-terrorism, border security, warfare, cybersecurity, emergency operations, and social threat evaluations. Surveillance of the hostile target is essential for counter-terrorism. Big data can train AI to predict the patterns and behavior of hostile targets and image recognition technologies can be employed to locate them. Through deep learning abilities, AI can detect any suspicious activities of those targets. Likewise, unmanned autonomous vehicles with sensors and cameras at different angles having a wide field of view can be adopted to check smuggling and other criminal activities along open borders. Also, virtual monitoring of borders with facial recognition technologies will be very effective for border security as the operating unit can be informed about hostilities on the border. Moreover, the sensitive areas along the border can be kept under permanent surveillance. AI-upgraded intelligence is used for indication and warning systems in any warfare (NSCAI, 2021). It can detect emerging threats on the battlefield enabling warfighting units to anticipate them before time and forge an effective counter-strategy to deter them.

Regarding cybersecurity, AI can decode the patterns in the data which helps to detect potential cyberattacks against any organization. It can also be used to power antivirus and check hackers from infiltrating any system. During natural calamities or hostile disruptions, the AI can quickly assess the affected areas and facilitate the identification of the areas in dire need of rescue operation and critical supplies. Thus, it organizes and accelerates the emergency response of any military. Through AI systems, intelligence analyzes the trends, patterns, and nature of information flowing in a community which helps to evaluate the threats of social disruptions. This will provide sufficient time for the governmental apparatus to elude possibilities of disruptions and establish law and order. From the aforementioned advancements and possibilities, it is reasonable to state that military intelligentsia will be transformed with AI. However, the intelligence unit should exclusively work on fake images/audio/video, identity intelligence, and human language technology in order to tackle the issues of deep fakes, audio/video manipulation, and disinformation.

National Security

Defense and Security Analyst Brigadier General (Retd.) Keshar Bahadur Bhandari writes "National Security is concerned with the protection and enhancement of the vital elements of state affairs that promote the well-being of the state." Though the core objective of national security remains intact over the course of time, the aspects of national security may evolve with

the changing international security environment. With the incorporation of AI, the international security environment will change leading to operational advancement of the existing domains and the emergence of the new domains of national security. National security incorporates a wide range of elements but this paper primarily focuses on military security, economic security, security of energy and natural resources, data security, cyber security, and others considering the impact of AI inclusion. Military Security is always at the forefront of national security which includes the ability of a nation to defend itself from any aggression, be it internal or external (Bhandari, 2022).

AI-upgraded combat power and deterrence, autonomous weapons, and highly advanced intelligence apparatus will dominate the future military domain. Any military lagging in these aspects will not be able to respond to major threats to national security. Similarly, economic security is also one of the crucial elements of national security. As AI-led automation and mechanization will irreversibly damage the labor markets, the job security of the population will be a major concern (Furman & Seamans, 2019). This irreversible damage creates economic division and leads to the emergence of new classes which may propel social division and imbalance in the long run. Hardware entities such as semiconductors, transistors, and so on are critical for an AI-dominated manufacturing industry and global economy. Thus, the production and supply of these entities will be strategically important for the economic security of a nation. The security of energy and natural resources complements economic security. Proper utilization, strategic use, and security of the available resources are essential to ensure economic progress. AI-powered unmanned systems, robots, and cybersecurity apparatus can be utilized for the security and proper utilization of these resources. The appetite for energy of the big powers for their economic ambitions leaves relatively smaller powers more vulnerable. Thus, every nation should have a detailed action plan for the strategic use of the available resources. Data security is also an emerging dimension of national security, discussed below.

Data is acutely important to AI technologies. Big corporate platforms and social media are tracking the individual's profiles curated with information on voting histories, criminal histories, car home ownership, divorces, litigations, health, credit history, interpersonal relations, gun ownership, religious leanings, and so forth. This data can be used as an input to train machine learning. The records of users' secrets and vulnerabilities can be misused subtly for power-political benefits as they can develop tailored models to influence and manipulate individuals and societies (Malhotra, 2021). Developed countries are now taking data security very sensitively. A cyber hack of millions of data from medical insurer Medibank rocked Australia. The parliament then discussed the distress caused to the many Australians due to this event (*BBC*, 2022). Cybersecurity is now becoming an indispensable entity of national security. Any unauthorized access or intrusion in the military and security sectors, economic sectors, and critical state apparatus will cause a serious threat. Cyber threats, digital assaults, and disinformation are the emerging ways that nation-states can use to exercise coercion against adversaries. AI-wielded cybersecurity apparatus is very essential for national security as it enables the security system of a country to detect attempted cyberattacks, vulnerabilities of the system, and automate the response to any attacks. Modern border security can be technologized by AI systems to effectively check smuggling, criminal activities, hostilities and assess border threats.

In addition, AI systems can address the concerns of other elements of national security such as terrorism, environmental security, community empowerment, human security, and political security. From these explanations, we can conclude that AI-driven geopolitical or strategic coercion can jeopardize the security of any nation. Also, human operators alone cannot defend against the upgraded warfare strategies, disinformation, terrorism, border hostilities, cyberattacks, drone swarms, attacks from autonomous systems, and other AI-driven tactics aimed at wrecking the state apparatus as AI is a must to deter these new level of threats. Thus, it is very reasonable that AI will be a pivotal entity for national security. Lastly, the military should be equipped with data security, cyber security other AI-wielded security apparatus along with the counter mechanisms for any AI-driven attacks to strengthen national security.

AI, Power-Politics, and Military Strength

The countries are facing AI-enabled threats/vulnerabilities, and big powers have already begun to exploit AI for their interests and geopolitical ambitions. The big powers are explicitly acknowledging the importance of AI which has led to the transformation of the power political domain. On July 20, 2017, the Chinese government unveiled its ambitious commitment to lead in AI by 2030 (Hoadley & Lucas, 2018). Russian President Vladimir Putin publicly announced, "Artificial intelligence is the future, not only for Russia but for all humankind. It comes with colossal opportunities, but also threats that are difficult to predict. Whoever becomes the leader in this sphere will become the ruler of the world" (Muller, 2017). Also, the NSCAI report of the US states "…. a strategy to defend against AI threats, responsibly employ AI for national security, and win the broader technology competition for the sake of our prosperity, security, and welfare." The aforementioned excerpts from the leader's speeches and reports of government bodies of the powerful countries express how the significance of AI has escalated in the global pursuit of power. The countries already advancing in AI can attain their national interests and geopolitical ambitions in unprecedented ways.

Any foundational AI entities such as hardware and big data can be used as a geopolitical weapon. Any strategic cutoff in the supply of AI hardware will severely affect the manufacturing and industrial sector. The supply of crucial electronic devices like semiconductors which are extensively used in automotive, medical, and communication industries will have tremendous tactical and economic value. As only a handful of companies based in South Korea and Taiwan have the capabilities of semiconductor manufacturing, big powers are assessing the geopolitical implications of this (Hussain, 2022). The US raises its concern over its chip security in its NSCAI report which states "the vast majority of cutting-edge chips are produced at a single plant separated by just 110 miles of water from our principal strategic competitor, we must reevaluate the meaning of supply chain resilience and security." Also, the semiconductor chip shortage cost $110 billion in revenue for the global automotive industry (*CNBC*, 2021). Similarly, big data of any country can be utilized as a strategic asset for power-political benefits.

As big data can be misused to create national security breaches through disinformation and societal manipulations, the concern about data collection, usage, protection, and transfer is changing the geopolitical landscapes. Big powers are now revealing their insecurity towards foreign technologies. China banned all foreign software and computers from government offices and institutions (*CNN*, 2019). In 2017, the US passed federal laws regulating the

foreign acquisition of US businesses containing data of more than one million American citizens (Malhotra, 2021). Likewise, the US restricted Chinese equipment in its networks conferring them as a threat to national security arguing that they could eavesdrop on sensitive US conversations (*CNN*, 2019). Thus, the conservative policies adopted by the big powers vividly depict that power politics will be rocked by the issues of data security in the future. Another emerging tool for the devastation of any country's confidentiality, military, financial and critical infrastructure sectors is offensive cyberattacks. AI can be wielded in offensive cyber operations to raise the mutational ability of malware, increase its resistance and intensify its devastation. According to Check Point Research, ransomware attacks increased by 102% worldwide in 2021. Ransomware attacks in the colonial pipeline of the US caused a loss of over $20 billion (Panettieri, 2022). Nepal also faced almost 800 cyberattacks in the year 2018 (Angbo, 2020). The military aspect of the power-political domain will also have several transformations induced by AI incorporation.

Every domain of the military i.e. weaponry, warfare, intelligence gathering, analysis, border security, internal security, combat strategies, rescue operations, surveillance, reconnaissance, and so forth, will advance functionally and operationally through AI. Any task operation in coordination with these advancements for acquiring geopolitical gains and fulfilling national interest will posit a new level of threats to the militaries which are less advanced and operate conventionally. Without an advanced military, any military cannot resiliently defy these threats, thus, military strength in the future will be defined by AI-robustness. Eventually, this will lead to the emergence of new classes of military i.e. military-haves (stronger and technologically advanced) and military have-nots (weak and technologically primitive). So, it is plausible that AI will be a new dimension of military strength evaluation in the future. Ultimately, the rigorous race of the big powers for AI domination in the aforementioned domains will be more intense in the days to come which may cause severe turbulences in the power-political arena of the world.

Challenges

AI integration in military applications has several ethical, operational, and strategic challenges to consider. Ethical challenges incorporate legal and moral obligations. One of the legal challenges is that the autonomous weapon systems of the military cannot function following the Law of Armed Conflict (LOAC) or International Humanitarian Law (IHL) (RAND, 2020). These systems are incapable of assessing the qualities that distinguish combatants and civilians which is not in compliance with the principle of distinction and proportionality of LOAC (RAND, 2020). As autonomous weapon systems can attack without any human authorization, it creates an accountability gap in their actions.

AI is an emerging and dynamic field and its innovators and creators are not fully acquainted with the capabilities of the system (Schmidt, 2020). It might lead to severe unintended consequences in warfare. As none can be held responsible for the unintended actions of the autonomous system, it creates a very crucial ethical gap in accountability. One of the challenges of AI is to address human rights, data rights, and privacy rights. AI-enabled systems can pervade into the individual's life and know their secrets and vulnerabilities. Also, the biases of the creators and unbalanced data input may lead to the formulation of models with

innate biases against a certain gender, sexuality, caste, race, religion, ethnicity, and so forth. At Amazon, a machine learning model of its recruiting engine showed bias against women (*Reuters*, 2018). The operational challenges of AI include constraints from innovation to the functioning of the AI-enabled system (RAND, 2020)

Data is the main challenge for the military in the innovation of technology. A massive amount of data from different spectra is required to train the machine learning models which is often difficult for military apparatus to amass (Svenmarck et. al., 2018). Another challenge lies in the testing and evaluation of the system. The evaluation is done in a controlled environment or laboratory which may not fully ensure its proper functioning in complex and unstructured environments (RAND, 2020). Also, AI is susceptible to data poisoning, hacking, and other technological infiltrations which might lead to its operational challenge i.e. adversarial attacks. Adversaries can use camouflage techniques to poison the input of the system and fool its algorithm or can infiltrate the machine learning models of the system to alter its functionality. The strategic challenges of AI incorporate risks that may threaten the stability of the international order.

AI-based autonomous systems can unintendedly escalate any conflict at the machine speed leading to terrible damages (RAND, 2020). These conflicts when fused with several miscalculations may exacerbate the situation taking it to the 'point of no return' where measures of diplomatic negotiations to resolve the situation might not work. As AI-based systems are very reliable in their performance, the leaders/military of countries might resort to these systems for any task operations. This may lead to conflict escalation. In addition, most of the AI-related research and innovations are publicly available which can be misused by any terrorist or similar groups to create severe disruptions. Therefore, to mitigate the possible risks, the ethical, operational, and strategic constraints of AI should be adequately addressed before wielding it to the military apparatus.

Artificial Intelligence in Nepal

Nepal has not made any significant strides in the field of AI in any sector. However, Banking and Financial Institutions (BFIs) are adopting AI-enabled technology in fin-tech, mobile banking, SMS banking, internet banking, e-wallets, and payment gateways (Niroula, 2021). Poor digital literacy, inadequate policies, economy and poor infrastructure, and so on are the problems hindering the AI-development in Nepal. As the global economic and security environment is transforming with the application of AI, Nepal and Nepali Army must adopt robust policies and implement them earnestly to adapt to the new AI environment. To utilize AI in nation-building and national security, Nepal should form a proactive council of think tanks, intellectuals, economists, defense analysts, strategists, and IT and AI experts to develop a comprehensive AI master plan with proper implementation guidelines. Our strategy should correlate with our foreign policies, national interests, aspects of national security, and form of governance.

Firstly, STEM (Science, Technology, Engineering, and Mathematics) education should be made more effective with the allocation of an adequate budget for AI research and development (R&D) to fuel technological development. AI should be introduced in disciplines of university education and defense institutes with sophisticated infrastructures and skilled educators. Secondly, the economic policy should be formulated such that it accelerates innovation

and digitization in every sector; the entire population can leverage the benefits of AI. To increase efficiency, transparency, and accessibility, the government should adopt digitization in its processes and services. Also, Nepal should exclusively research the possibilities of manufacturing any crucial AI technologies or hardware which will significantly boost our economy. In addition, diplomatic exchanges with advanced countries can be beneficial in forging strategies for AI development. With efficient diplomacy, Nepal can benefit from the spillover technological advancements of our immediate neighbors. Different campaigns should be launched in order to improve digital literacy and minimize the digital divide within the country. In addition, basic infrastructures of communication and technology should be made accessible in every nook and corner of the country. Like the state apparatus, Nepali Army (NA) should embrace AI to improve its operational efficacy and tactical approach to defend the key security challenges of Nepal.

The Nepali Army (NA) should establish its Research and Development (R&D) mechanisms and incorporate new highly skilled talents from the STEM field in the military to be acquainted with the ongoing developments in the military-technological realm. With AI-driven intelligence, the army can analyze information from all sectors and detect potential threats. Any unintended consequences such as border hostilities, social disruptions, terrorist attacks, and so on can be deterred. Both military and state apparatus should employ the modern intelligence mechanism to filter fake news and disinformation. Similarly, the NA should empower itself with a modern weaponry system and warfare tactics. The autonomous systems can help assess the effect of natural calamities in a complex topography which will improve the emergency response of the army. Also, the NA can remotely inspect the infrastructure development progress using AI technologies. Military and state should strengthen their cyber defense system with AI in order to protect their confidentiality and defy any foreign intrusion. AI has reshaped the geopolitical landscapes, so, the military and the state apparatus should be accustomed to the changing dynamics and frame the strategies as per our national interests. As any sector must be equipped with AI-enabled systems, it is also important that the concerns of individual liberty, data security, data rights, and the right to privacy of Nepali citizens are properly addressed.

Conclusion

This paper discussed AI advancements, their military usage, the operational outlook of the future defense, the power-political influence of AI, and the challenges of AI incorporation in the military to underpin its core argument i.e. AI is the new dimension of military strength evaluation and a pivotal entity of national security. Further, it has recommended that the steps be pursued by Nepal to attune itself to the changes brought about by AI. Despite several challenges, the world will witness major breakthroughs in AI. The developments occurring at an unstoppable pace can reorganize the world we live in. Besides acclimatizing to the changes and robustly defending our interests, we do not have other options. The technologically advanced military will be a boon for any country in the future defense and pursuit of power. Similarly, the big powers' race for geopolitical influence may cause several turbulences in the power-political realm.

To avoid any unintended consequences, the organizations like the UN should forge effective regulations and approaches to evade destabilization. Similarly, countries like Nepal

should frame their strategic plan to defend themselves from AI-induced repercussions. To accelerate technological development, we should set up aspiring national goals with a detailed action plan. Similarly, military applications and operations should be fortified with AI technologies. Nepal's geographic location has made it the land of geostrategic importance (Poudyal, 2022). Though it is very difficult to envisage future geopolitical approaches, Nepal should excessively research and familiarize itself with the new AI-wielded strategies that big powers are continually taking advantage of. The assessment of these new strategies along with the proper identification of threats and challenges should be done by both state and military apparatus to forge a comprehensive national strategy. Lastly, it is high time that Nepal understood the gravity of emergent AI issues, its implications, and vicissitudes, and pursue national aspirations with the strategic and responsible use of Artificial Intelligence.

References

Angbo, P. K. (2020). Hybrid threats in the National Security Context of Nepal. *Unity Journal*, *1*, 96-102.

Bhandari, K.B. (2022). *National Security and the State: A focus on Nepal*. Nepalaya Publication.

Binnendijk, A., Marler, T., & Bartels, E. M. (2020). *Brain-Computer Interfaces: US Military Applications and Implications, An Initial Assessment*. RAND.

Burns, E. (2021). Machine Learning. *TechTarget*. https://www.techtarget.com/searchenterpriseai/definition/machine-learning-ML

Campbell, L., Lotmin, A., DeRico, M. M., & Ray, C. (1997, October). The Use of Artificial Intelligence in Military Simulations. IEEE International Conference on systems, man, and cybernetics. *Computational Cybernetics and Simulation, 3*, 2607-2612.

Dastin, J. (2018). Amazon scraps secret AI recruiting tool that showed bias against women. *Reuters.*

Fung, B. (2019, Nov. 22). US Regulators rule that China' Huawei and ZTE threatens national security. *CNN.*

Furman, J., & Seamans, R. (2019). AI and the Economy. *Innovation policy and the economy*, *19*(1), 161-191.

Gray C. (2022). Four ways AI is transforming the transportation industry. *AI Magazine.* https://aimagazine.com/data-and-analytics/four-ways-ai-is-transforming-the-transportation-industry

Hoadley, D. S., & Lucas, N. J. (2018). Artificial intelligence and national security. *Artificial Intelligence and National Security*. Doi: 10.1007/978-3-031-06709-9

Hussain, T. (2022). The Geopolitics of New Oil: Semiconductors. *The Geopolitics.* https://thegeopolitics.com/the-geopolitics-of-the-new-oil-semiconductors/

Malhotra, R. (2021). *Artificial Intelligence and the future of Power*. Rupa Publications Pvt. Ltd.

Marr, B. (2021). The New Global AI Arms Race: How Nations Must Compete On Artificial Intelligence. *Forbes.* https://www.forbes.com/sites/bernardmarr/2021/05/24/the-new-global-ai-arms-race-how-nations-must-compete-on-artificial-intelligence/?sh=3eff3ff72702

Morgan, F. E., Boudreaux, B., Lohn, A. J., Ashby, M., Curriden, C., Klima, K., & Grossman, D. (2020). *Military applications of artificial intelligence: ethical concerns in an uncertain*

world. Rand Project Air Force Santa Monica United States.

Muller, C. V. (2018). *Philosophy and Theory of Artificial Intelligence*. Springer.

Niroula, A. (2021 Feb. 19). Banking in Nepal: Greater Use of AI. *The Himalayan Times*

NSCAI (2021). The Final Report. *National Security Commission on Artificial Intelligence*. https://www.nscai.gov/2021-final-report/

Panettieri, J. (2022). Colonial Pipeline Cyberattack: Timeline and Ransomware Attack Recovery Details. *MSSP Alert.* https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/colonial-pipeline-investigation/

Pham, S. (2019, Dec.9). China reportedly bans foreign technology in government and public offices. *CNN.*

Poudyal, B. (2022). Why Nepal Matters in the Geopolitical Chessboard. *Unity Journal*, *3*(01), 13-26.

PricewaterhouseCoopers. (2017) .*Sizing the prize*. https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf

RAND. (2020). Annual Report. https://www.rand.org/pubs/corporate_pubs/CPA1065-1.html

Reşitoğlu, Ş. (2022). Artificial Intelligence Russia-Ukraine War Series. *Tuic Akademia*. https://www.tuicakademi.org/artificial-intelligence-in-russia-ukraine-war-series/

Revanth. (2019). Toward Future Farming: Artificial Intelligence is transforming the Agriculture Industry. *Wipro.* https://www.wipro.com/holmes/towards-future-farming-how-artificial-intelligence-is-transforming-the-agriculture-industry/#:~:text=AI%20technology%20helps%20in%20detecting,to%20apply%20within%20the%20region

Schmidt, E. (2022). AI, Great Power Competition & National Security. *Daedalus*, *151*(2), 288-298.

Schmidt, E., Work, B., Catz, S., Chien, S., Darby, C., Ford, K., & Moore, A. (2021). *National Security Commission on Artificial Intelligence (AI)*. National Security Commission on Artificial Intelligence.

Suman, S. (2022). Augmented Intelligence for National Security and Development. *Unity Journal*, *3*(01), 245-252.

Svenmarck, P., Luotsinen, L., Nilsson, M., & Schubert, J. (2018, May). *Possibilities and challenges for artificial intelligence in military applications* [Paper]. Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting. 1-16.

Szczepanski, M. (2019). Economic impacts of artificial intelligence (AI). *Economics*.

Tidy, J. (2022, Nov 12). Australian police to Medibank hackers: 'We know who you are'. *BBC.*
Vincent, J. (2017). Putin says the nation that leads in AI 'will be the ruler of the world'. *The Verge.* https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world

Wayland, M. (2021, May 14). Chip shortage expected to cost auto industry $110 billion in revenue in 2021. *CNBC.*

WEF (World Economic Forum). (2015). *Shaping the Future of Technology Governance: Artificial Intelligence and Machine Learning*. https://www.weforum.org/platforms/shaping-the-future-of-artificial-intelligence-and-machine-learning