SOCIAL PRISM

Volume 2 Issue 2, 2025

AI in Modern Warfare: Impacts on Information Operations, Cyber Conflicts, and C2 Systems

Muhammad Umar Farooq Baloch – sardarzada1@gmail.com – Research Associate at National Defence University, Islamabad, powering Global Discourse with Elite Domestic & International Publications

Abstract

This research delves into the transformative influence of artificial intelligence (AI) on modern military operations, emphasizing its impact on information warfare, cyber conflicts, and command and control (C2) systems. With the rapid evolution of AI technologies, their incorporation into military strategies has introduced significant complexities, bolstering both offensive and defensive capacities. The initial section explores AI's application in information warfare, where AI-powered tools enable automation in strategies such as disinformation campaigns, targeted propaganda, and social media manipulation to disrupt adversarial communications and sway public opinion. It assesses the implications of cyber-attacks on military hardware and operations, emphasizing the growing reliance of military systems on digital networks and the vulnerabilities posed by cyber threats. The study further inspects the incorporation of AI into C2 systems, particularly in the realm of net-centric warfare and offers strategic insights for Pakistan to leverage AI and robotics in military operations. The research highlights the critical need for adapting to emerging technologies to safeguard national security in an increasingly interconnected digital era.

Keywords: Artificial Intelligence, Command & Control systems, Perception, Warfare, Emerging technologies

Introduction

Artificial intelligence has played a profound role in the military as well as the non-military domains of life. AI and robotics have revolutionised warfare tactics through the use of decoding machinery, nuclear missiles, spray fields, better healthcare, and precise communication that started from the Cold World and have been advancing ever since (Martin, 2021; Molder, 2010). As Russian President Vladimir Putin said, “Whichever country becomes the leader in Artificial Intelligence AI, would become the ruler of the world” (Casin, 2023). Recently, we see the pivotal role of AI and robotics in the Russia-Ukraine and Israel-Palestine war in the form of suicide drones, automated robot-snipers, nuclear force management, cyber defense etc. Due to the reduced risk of human casualties, cost of training, rations, supplies, and overall increased efficiency than the traditional method of war, many investments are continuously being made for development of AI and robotics, this, making it the future of warfare (Agarwala, 2023).

AI has also influenced information operations. An information operation aims to influence the adversary’s information and information system while also protecting their own information and information system (Kuehl, 2002). AI has impacted both offensive and defensive aspects of information operations. On the offensive side, it manipulates public opinion and the enemy’s decision through false information and misleading claims by using advanced AI algorithms (Gorodnichenko & Talavera, 2020). Moreover, it also helps in cyber offence by automating tasks such as patrolling, threat identification, and malware deployment (Mahdi & Zwitter, 2020). On the other hand, AI may also help to defend the IO by efficiently detecting any malicious activity in the algorithms and taking immediate actions and counteractions (Zuev et al., 2019).

Perception management has also become quite popular among warfare tactics, where hostile actors are used to spread misinformation and manipulate the public and commanders to perceive information differently through AI in the tactical, operational, strategic military tiers (United States Department of Defense, 2018). These tactics are used in the Israel-Palestine war and Ukraine-Russian war as well to manipulate information.

At a tactical level, the use of AI to produce misinformation and propaganda to manipulate the adversary's perception about their positioning in the battle ground, their intentions, strengths and weaknesses can help manipulate or disrupt the adversary’s decision making (Howard & Kollanyi, 2016). AI can also be used in the operational tier, hostile actors may use sophisticated AI technology to understand the military

plans and their execution in the adversary operational tier. It may also analyse news reports, public opinions, and media trends to identify any vulnerable information that could help to manipulate the adversary's perception management and make them doubtful of their own decisions (United States Department of Defense, 2018). Moreover, in the strategic tier, AI powered tools can play a very powerful and scary role. By predictive analysis of news reports, media trends, public opinions and by driving cyber misinformation campaigns to shape those opinions, they can also manipulate the geopolitical landscape, influence the mind of leaders and their strategies as well according to their own desires (Taddeo & Floridi, 2018).

Cyber-attacks and the military can also impact the military operations and hardware as well. They may compromise security protocols of military hardware like drones, tanks, or aircrafts and by hacking, they can also manipulate their pathways according to their desires (Rid, 2013). Hacking can impact the critical systems like communication systems, logistics, and weaponry guidance systems causing confusion and disrupting their operations. Moreover, it can also cause hesitancy in using cyber and AI technology due to hacking vulnerabilities limiting the military's power to deploy their strategies effectively (Libicki, 2009).

Although we have seen the power of AI in the command and control system, it may also lack in some areas of net-centric warfare. On one hand, it increases the efficiency of control and command decision making by analysing vast amounts of data and identifying vulnerable information, helping in decision making (Marine Corps Combat Development Command, 2017). On the other hand, these systems may also be vulnerable to hacking and cyber-attacks causing its credibility to be unreliable by manipulation of information. This may decrease the effectiveness of net centric warfare concepts. Another positive impact may include that it may help to analyse information from multiple sources efficiently, providing the commanders and control systems with a comprehensive and organised idea about the battle environment and help them in their decision making.

Multiple Studies have been conducted to elaborate the huge shift of the world from the conventional to the modern AI and robotics driven war tactics. It explains how the world is evolving and transforming from conventional/traditional methods to modern AI and automation determined combat tactics. Additionally, studies also specified the facets of the machine learning weapons and controlling them underneath the international humanitarian law. On the other hand, researches have overlooked how to analyse that in what terms AI and robotics has changed the military and war landscape and what potential risks and vulnerabilities are inherent in AI-driven military technology including the threat of cyber-attacks, hacking, manipulation by hostile actors etc. Thus, there is a need to investigate this area by focusing on the nature of changing war landscape and inherent vulnerabilities attached to it.

Research Methodology

The proposed research study utilized a mixed-methodology research design to understand the dynamic from traditional to modern AI and robotics driven military and war tactics. This approach combines both qualitative and quantitative research methods to provide a comprehensive understanding of the subject. Data was collected using both primary and secondary sources. Primary data was collected through surveys, interviews, and focus group discussions. Secondary data was collected from relevant literature, research articles, and other published sources. For quantitative part of the study, the researcher focused on conducting interviews from the experts on AI and robotics as emerging technologies.

However, the scope of interview can be extended to other experts working on emerging technologies such as AI and robotics and in what manner AI and automation has changed the military and war landscape. To provide robust and insightful data, the sample includes professionals from various sectors within the technology and AI fields. Sample size for this research is 100 that encompasses software engineers, data scientists, AI researchers, tech industry analysts, and automation specialists. The sample includes individuals who are familiar with AI driven technologies, including government officials, security personnel, and Technology experts. This analysis provide us with an un-biased approach towards exploring the potential advantages and disadvantages of using AI and robotics in warfare. For qualitative section, the study relied on secondary data published in peer-reviewed journals, books and government reports.

The data was analysed by using both qualitative and quantitative analysis methods. Qualitative data were analysed by using content analysis, while quantitative data can analysed by using statistical tools, such as SPSS or Excel. Moreover, ethical considerations was taken into account to ensure the research participants' confidentiality, privacy, and autonomy. The findings and conclusions is based on the analysis of the data collected using both qualitative and quantitative methods

Literature Review

AI and robotics has proven to build a radical change within the military strategies. Many studies have also been conducted to confirm this huge shift from the conventional to the modern AI and robotics driven war tactics. Some studies have specifically focused on tactical as well as strategic integration of AI and robotics in the military. Tactical applications include the use of intelligence systems at operational level, helping in complex decision making by threat assessment and target recognition etc. Several studies also defined the importance of Unmanned Aerial Vehicles (UAVs) and the use of automated machinery to reduce the risk of human personnel. AI may also be used in the military for predictive analysis or assessment such as past data, weather forecast, enemy movement and to predict and devise a future plan.

According to studies, AI has revolutionized the military strategies through advanced data processing and quick decision making which surpasses the traditional military tactics. This also helps in effective combat operability and effectiveness. AI has become so integrated into military that various studies and researches have been made to further make effective use of AI in the military. This includes discussion on its capabilities, opportunities, and potential risks. Furthermore, various AI applications have also been studied including object identification, military logistics, robotics system, understanding the effectiveness in the battlefield (Rashid et al, 2023).

Moreover, studies also suggest that AI and big data have played a transformational role in the field of Information Operations. Thus includes a huge paradigm shift from traditional warfare to an automated and effective decision making processes in fields of electronic and cyber warfare. The role of AI in information operations emphasizes on its analytical capabilities by analysing vast data sets which would otherwise require a lot of time. This may include image processing, pattern recognition and gathering of information through Open Source Intelligence (OSINT). This is particularly important in wars as it provides countries to adapt swiftly to any upcoming threats and make fast and effective decisions. AI also plays a huge role in cybersecurity as its algorithm helps to detect anomalies, potential vulnerabilities, and threats and warns in time for effective strategic decision making. Another important function of AI in information operations is its ability to distinguish between true and fake information due to its algorithms which prevents countries to make rash decisions that would backfire (Chaltiel, NA).

Perception management and AI combined play a strong role in devising strategic decision making in warfare perception management through AI emphasizes its importance in information warfare as well. Perception management works by understanding the way people perceive information and can be used for manipulation of public or the enemy in warfare. AI technologies help greatly in this regard. They understand the public sentiments and media consumption and can predict the outcome of an event with much faster and greater accuracy. In this way, military and government entities can deploy targeted propaganda information and tackle misinformation with more accuracy and speed. An example would include the Iraq war where AI driven perception management was utilized to shape public and media opinion and justify their military actions. Besides all this, AI can also help to automate content and tailor narrative according to the requirements and spread across media channels. This is particularly helpful as media information spreads within seconds and only AI can keep up with this pace (Kapoor, 2009).

On the other hand, studies also highlight threats related to AI's unreliable nature, as these algorithms are also susceptible to errors and don't always provide 100% correct results and thus can negatively impact the command and control system (Galliot, 2015). Studies also raise concerns over its ethical and legal implications due to its autonomous decision making processes which may also lead to undesirable results

oftentimes. Thus, it is important to devise ways for them to comply with international humanitarian laws (Thurner, 2013).

AI has rapidly become a part of our everyday life such as in finance, healthcare, education, military and so on. However, its use must be governed through an appropriate framework to prevent any inherent potential risks. However, this is not an easy task given the complex nature of AI and its fast paced evolution. For this, global standards must be delivered putting aside national boundaries. This cooperation among countries, private sectors, and society would prove to be effective in AI governance. Moreover, efforts should also be made towards making the AI system more reliable, fair, and interoperable without any biasness and privacy concerns.

Organizations like ISO and IEEE have been known to work effectively in making ethical guidelines for AI governance. This article also highlights role of AI in machine learning. As AI deals with the analysis of vast amount of data, the privacy of the given data must be equally considered. For this transparency and accountability of AI algorithms must be promoted to make this system more reliable. As far as role of AI in military is concerned, use of AI weaponries must be under specific guidelines laid by the international regulations. This is to prevent any misuse or proliferation of AI in warfare (Marwala, 2023).

FINDINGS

ROLE OF AI IN INFORMATION OPERATIONS (IO) & PERCEPTION MANAGEMENT

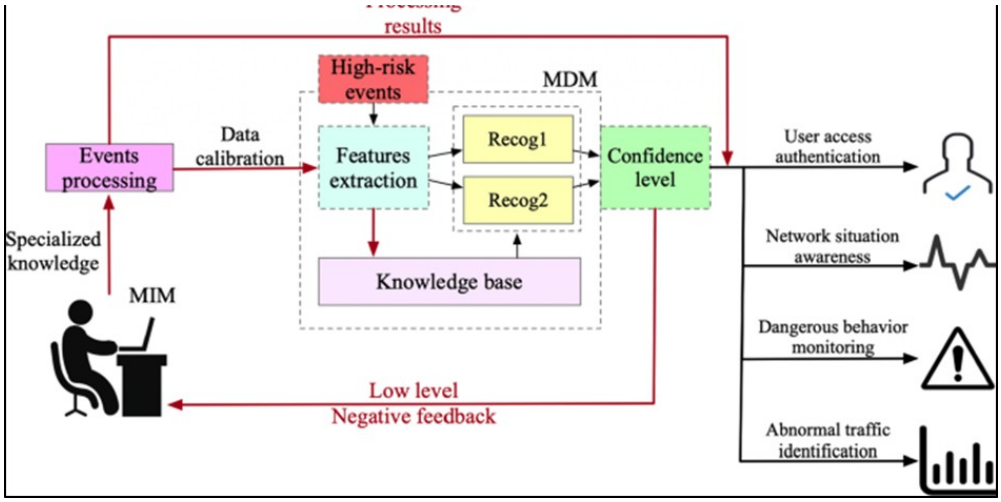
Offensive role of AI in information operations encapsulates the Exploitation of information that includes the new tracing of social media termed as AI algorithms that uses a person's messages, groups and scrolling data to identify susceptible characters. Alongside this, it can Change people's opinion on large scale by showing videos, posts and pictures regarding fake news. Moreover, it also play its role in cyber operations and attacks as it will be helpful by identifying similar attack strategies and by pointing at similar vulnerabilities. Besides, AI itself is used to target the weaknesses in AI for instance, evading detection and as poisoning training data as well. Offensive role of AI also alludes the Imitation and trickery, in which AI is so board in its functioning that it can even make and run fake accounts or groups that can get engage in false information and fake news spreading grounds.

Defensive role of AI in information operations includes the Recognition and credit in which AI can observe recurrent patterns in data to point out misleading of information or spreading of false news and also flags this for withdrawal and removal. Moreover, it also helps to find the Origins of cyber-attacks or misinformation aiding in spread of threat. Besides, it defensive role also plays its role in Content composure and Decision making in which Assignment of AI is to locate and identifying the misleading and illegal information and the ability to distinguish between legitimate and automated bots spread data and also gives potential cyber scenarios to get the idea before the real incidence occurs.

Due to the AI, automation of tasks that were monitored manually and it used to take a lot of time. For instance, NLP that's is the natural language processing and machine learning algorithms that can sift through the loads of information, can point out relevant information as well as can generate insights much faster than humans analysis would have done. This has approach in intelligence collection and gathering, in it the AI can rapidly explore social media, trending news and much more sources to mark trends and threats (springer, 2021)

Alongside other capabilities, AI tools can supply great decision-making abilities to provide predictive analytics as well as support to Decision systems. AI tools are powerful, with all these capabilities these tools can examine historical data and can make assumptions and predictions about trends of future that can help organizations make useful decision beforehand. In the circumstances and context of military and operations that require, AI can activate different outcomes and scenarios that will help in making of useful strategies and response to possible threats (springer, 2021). AI is also effective in supervising misleading and disinformation. With detection AI can flag and mark the false information on communication platforms and other social media. By observing patterns and identifying inconsistency, it helps in suppressing the spread of fake ill news and balancing the firmness of information system (springer, 2021).

ROLE OF AI IN CYBERSECURITY



AI plays a significant part in cybersecurity by defending information systems against intrusions. By identifying security issues early on and obtaining a prompt solution, a response to cyber threats can be achieved. This is essential for safeguarding private data and ensuring data and communication security in these operations. It has greatly increased offensive capabilities in the digital sphere, especially in the areas of psychological manipulation, cyberattacks, and disinformation. The use of AI to create and spread automated propaganda and misinformation is one of the main causes for concern. By taking advantage of algorithmic flaws and personal information, AI can produce and disseminate vast amounts of misleading information, increasing its impact and reach. (Schmidt et al., 2020). Furthermore, AI is being used more in hacking and cyberattacks to identify and take advantage of flaws in networks, digital systems, and personal communication tools, which poses serious risks to cybersecurity (Murchu and Wisniewki, 2018). In addition, by examining vast amounts of data to determine individual interests and creating personalised messages meant to influence beliefs or actions, AI can manipulate people. AI is a potent weapon in strategic information warfare because of its focused psychological impact. (Taddeo and Floridi, 2018).

Figure 1: Role of MIM (machine identity management) in protecting IS from cyber attacks

AI is also essential for strengthening defences against online attacks. Finding patterns and anomalies in online data is one of its primary uses in disinformation detection, which enables the prompt identification of inaccurate or deceptive content. Furthermore, AI is frequently used in cybersecurity systems to keep an eye on network activity, identify questionable activity, and react quickly to possible cyberattacks, enhancing overall cyber defence (Althobaiti et al, 2020). AI also makes it easier to analyse user behaviour and information patterns in order to spot unusual or potentially harmful activity, which greatly aids in the early detection and avoidance of security breaches (Bryson, 2018). AI is a crucial part of the current digital security environment because of these defensive capabilities.

INFLUENCE OF CYBER-ATTACKS ON MILITARY HARDWARE AND THEIR OPERATIONS

In the context of military operations and equipment, cyberattacks have grown to be a major concern, having a substantial impact on communications, logistics, and command structures. The growing integration of digital technologies into military systems makes them vulnerable. While increasing operational efficiency, this digital transformation also exposes vital infrastructure to cyber threats. National security is seriously threatened by attackers who can use these flaws to interfere with logistical operations, disrupt command and control systems, and trace communications.

Disrupting military operations is one of the most serious effects of cyberattacks. These assaults have the potential to seriously impair military forces effectiveness, impede battlefield manoeuvres, and postpone or paralyse mission objectives. High-tech weapons like drones, aeroplanes, and missiles are especially

susceptible to cyber manipulation in contemporary defence systems. Adversaries may use remote access to disable weapons, fabricate targeting information, or deceive decision-makers, all of which could have disastrous results. Such cyber threats have wide-ranging strategic ramifications. The distinction between conventional and cyberwarfare is blurred by cyberattacks, which enable adversaries to contest military superiority without engaging in direct combat. Opponents can accomplish their goals and erode strategic advantages by taking advantage of these digital weaknesses without going over the line into a conventional armed conflict.

Cyber operations in combat also bring up significant ethical and legal issues. Cyberwarfare has been incorporated into the laws of armed conflict through adaptations of international frameworks like the Geneva Conventions. These legal guidelines, which include the concepts of distinction, proportionality, and military necessity, guarantee that military cyber operations follow accepted standards. Cyberattacks have consequences that go far beyond simple technical issues. They have an impact on international relations, strategic outcomes, and the larger dynamics of world security. Addressing inherent cyber vulnerabilities is still one of the most difficult tasks in defence planning and policy formulation, especially as militaries continue to adopt cutting-edge digital technologies.

EFFECTS OF HACKING ON MILITARY HARDWARE

Military equipment, decision-making processes, and operational frameworks can all be negatively impacted by hacking. These effects can take many different forms, such as the alteration or deterioration of command and control systems, illegal access to private data, and disturbance via methods like denial-of-service (DoS) attacks. Attacks like these reduce the availability of systems and hardware, which hinders decision-making and operational efficacy during crucial missions.

Additionally, communication networks are frequently the target of cyberattacks, which can cause operational chaos and result in the theft of classified information. Such sensitive data loss or distortion may lead to poor strategic planning, mission failure, or misguided reactions. Another serious risk is supply chain attacks, in which compromised or fake parts are incorporated into military equipment, resulting in long-term dependency problems and system failures. These flaws could be used by hostile entities and cybercriminal organisations to obtain classified information about military tactics and technologies. In addition to jeopardising ongoing operations, this exposure gives adversaries knowledge about potential defences. Because of this, the military's dependence on digital systems in the absence of strong cybersecurity safeguards may prove to be a serious liability.

EXAMINING THE PROS AND CONS OF AI ALGORITHMS IN C2 SYSTEMS WITHIN NET-CENTRIC WARFARE

By processing enormous amounts of data quickly and accurately, AI algorithms have shown that they can improve speed and decision-making abilities. Commanders benefit from these algorithms' precise forecasts and customised solutions. AI can also combine information from various sources, including sensors, satellites, and drones, to produce a comprehensive situational awareness. In dynamic environments, this data fusion greatly enhances real-time responsiveness and clarity by enabling the detection of anomalies, threats, and patterns that human operators might overlook.

Another significant benefit is the automation of repetitive processes like communication, logistical planning, and data processing. AI-powered autonomous systems optimise logistics and daily tasks in real-time, freeing up human operators to concentrate on strategic planning. Flexibility is also offered by machine learning algorithms' learning and adaptability. AI systems can improve overall performance by adapting to shifting operational environments, learning from exposure, and improving mission planning. Furthermore, AI lessens the cognitive load on decision-makers by classifying and ranking data inputs. It offers important insights, draws attention to areas that need urgent attention, and facilitates better informed, stress-resilient decision-making.

Notwithstanding these benefits, there are a number of serious issues with the application of AI in command and control systems. Because AI systems are susceptible to cyberattacks, operational continuity, data integrity, and decision-making may all be at risk. In order to mislead or interfere with AI-driven operations, adversaries may take advantage of algorithmic flaws or alter input data. The problem of dependability and trust presents another difficulty. Commanders find it challenging to trust or comprehend

the reasoning behind AI-generated recommendations because complex machine learning models frequently lack transparency in their decision-making process. This inability to be explained could undermine trust in AI systems and prevent their widespread use.

Technical difficulties also arise when integrating with the military's current infrastructure. The majority of C2 systems are made up of diverse legacy technologies, and it takes a lot of time, money, and experience to align them with AI capabilities. Implications for the law and ethics are equally important. The need for precise legal frameworks is highlighted by concerns about accountability in autonomous and semi-autonomous operations, particularly with regard to the use of lethal autonomous weapons systems (LAWS). Legal and responsible military operations depend on upholding human oversight and adhering to international humanitarian law. Furthermore, relying too much on AI could make operations less resilient, particularly if there are unforeseen system failures or environmental disruptions that AI is ill-equipped to handle. Therefore, integrating AI into military systems requires balancing the risks involved with optimising operational benefits. Technical integration is necessary for effective implementation, but so are strict cybersecurity protocols, regulatory monitoring, and ongoing system performance assessments. When used carefully, artificial intelligence (AI) can greatly increase operational flexibility, situational awareness, and decision-making speed in network-centric warfare.

Perception management and information warfare have a lot in common with the role of AI in command and control systems. By processing and evaluating enormous amounts of data from multiple sources, AI-driven systems improve decision-making and help commanders stay situationally aware in situations that are changing quickly. Drones and other autonomous platforms increase operational efficiency even more, but they also bring up moral questions about accountability in combat. AI tools are being utilised more and more in the field of perception management to control strategic narratives and sway public opinion, particularly through social media and targeted messaging. These tools are useful for maintaining information dominance and combating false information in addition to disseminating information.

These applications do, however, carry some significant risks. Biases or inaccuracies that could impair operational judgements may be inherited by AI systems. AI integration in military systems creates new cybersecurity risks that need to be actively addressed to stop abuse. Concerns about public trust, transparency, and manipulation also come up ethically, especially when AI is used to sway the opinions or actions of civilians. If AI-driven operations are seen as unethical or lack transparency, public trust in military institutions may be damaged.

UNDERSTANDING PERCEPTION MANAGEMENT WITHIN THE 3 TIERS OF COMMAND AND POPULATION

Perception management at the strategic, operational, and tactical levels of military command is another area in which AI is crucial. At the strategic level, AI gathers and analyses data from social media, sensors, and intelligence sources to provide real-time analysis of public sentiment and world events. This improves a country's capacity to forecast and react to public sentiment and develop long-range geopolitical plans. AI systems assist in predicting societal trends and bolstering predictive planning initiatives to affect public opinion and expectations at the functional or operational level. At the tactical level, AI improves flexibility and responsiveness in perception management campaigns by automating social media monitoring, identifying false information, and responding with corrective messaging.

By personalising messages based on demographic and psychological profiling, AI enhances information operations at all levels and increases the efficacy of strategic communication. But these activities bring up important moral and legal questions. In order to protect privacy rights, prevent manipulation, and prevent unforeseen consequences, the application of AI in public perception management needs to be strictly regulated. To guarantee that AI-generated outputs follow moral guidelines and do not jeopardise the accuracy of the information being shared, human oversight is still essential.

Both military personnel and civilian populations have experienced conflicting effects from AI-driven perception strategies. By analysing real-time data and automating sentiment tracking, artificial intelligence (AI) improves situational awareness, operational efficiency, and resource management. Additionally, it thwarts disinformation efforts, maintaining confidence in military actions. However, AI's capacity to sway public opinion presents moral conundrums and raises issues with privacy, monitoring, and psychological

manipulation. The public's confidence in public institutions may be damaged if they start to doubt the reliability of information sources.

AI-driven perception management techniques have an impact on international narratives and foreign policy discourses in addition to domestic populations within the larger strategic framework. Clear regulatory guidelines are necessary for the use of AI in this field in order to guarantee responsible use, preserve public confidence, and protect human rights. AI technology is constantly changing the parameters of information warfare and military strategy, which emphasises the necessity of thorough policy frameworks and accountability systems.

Lastly, the application of perception management at the three levels of command and influence must be considered in order to comprehend its role in military operations. Perception management influences the long-term views of domestic audiences, foreign actors, and political stakeholders at the strategic level. To manage narratives and further national security goals, strategies like public diplomacy, psychological operations, and media manipulation are employed. At the operational level, the goal is to use culturally sensitive tactics, customised messaging, and civil-military cooperation to influence regional populations, stakeholders, and adversaries. Through direct engagement, rapid impact messaging, or psychological operations, tactical-level efforts aim to immediately affect civilian behaviour and enemy morale in designated operational zones.

At each of these levels, upholding moral principles, following the law, and being sensitive to cultural differences are essential for effective perception management. In order to modify strategies in response to changing operational conditions and societal dynamics, flexibility and adaptability are essential. All things considered, perception management powered by AI in military settings is a strong yet delicate instrument. Its strategic efficacy depends on its ethical application, technological robustness, and conformity to larger military and social norms.

India's Capabilities and Gaps in Analyzing the Impacts of Cyber-Attacks on Military Hardware & Operations

Even though India has made great strides in developing its cyber defence infrastructure, there is still a noticeable weakness in its capacity to evaluate and lessen the effects of cyberattacks on military equipment and operations. Today's cyber-threats include direct interference with military systems, communication networks, and command infrastructure in addition to data theft and espionage. It is essential to have a thorough grasp of how these attacks impact military functionality, readiness, and operational continuity.

To manage both offensive and defensive cyber operations, India has set up important organisations like the Defence Cyber Agency (DCA), which is part of the Integrated Defence Staff. To handle incidents and improve national cyber capabilities, this agency collaborates with CERT-In and the National Technical Research Organisation (NTRO). Despite these initiatives, India continues to face challenges in real-time threat visualisation across its military domains, unified frameworks for analysis, and strategic-level coordination.

India's ability to model and evaluate the operational effects of cyberattacks on intricate military systems, including command and control systems, communication satellites, radars, and automated weapons platforms, is one of the main drawbacks. The malware incident at the Kudankulam Nuclear Power Plant in 2019 brought to light the potential consequences of cyber intrusions and the susceptibility of vital infrastructure. The fragmented nature of follow-up studies and structured analysis of such incidents, however, suggests the need for better institutional learning and knowledge-sharing systems.

Additionally, interconnected systems like drones, GPS-guided munitions, and battlefield management systems (BMS) are increasingly the target of cyber threats. Each branch of the military Army, Navy, and Air Force tends to function in silos in the absence of a thorough inter-service cyber threat simulation framework, frequently responding to incidents rather than anticipating and planning for cyber disruptions. Joint doctrinal approaches to assessing the effects of cyber intrusions on operational tempo, decision-making, and battlefield manoeuvring are also not given enough attention. Although intelligence and technical assistance have been shared as a result of India's cooperation with foreign partners like the US, Japan, and Israel, the country's own capacity to analyse the effects of cyberattacks is still lacking. To

precisely assess possible risks to military hardware and operational readiness, there is an increasing need to develop sophisticated tools for risk modelling, scenario planning, and real-time diagnostics.

Areas where India Needs Enhancement in Analyzing Cyber-Attack Impacts on Military Operations

Although India has made strides in developing cyber defence capabilities, there are still a number of crucial areas that need to be improved in order to increase its resistance to cyberattacks that target military assets.

- At the moment, India lacks advanced tools capable of simulating extensive cyberattacks on military installations. High-end simulation capabilities are still being developed to model the impact of malware, ransomware, or denial-of-service (DoS) attacks on integrated platforms like satellite communications, automated surveillance, or missile defence systems. The military's capacity to anticipate system vulnerabilities and cascading failures is diminished in the absence of such modelling.
- Situational awareness and real-time intelligence are essential for effective cyber defence. Real-time threat intelligence integration across the armed forces is still lacking, despite India's establishment of the National Cyber Coordination Centre (NCCC) and CERT-In for monitoring and incident reporting. When evaluating impending cyber-threats and vulnerabilities to vital assets, predictive analytics which is fuelled by AI and machine learning remains underutilised.
- Outdated software or inadequate encryption protocols make military hardware especially legacy systems more susceptible to cyberattacks. India continues to take a patchy approach to systematic vulnerability testing and penetration auditing, frequently with no central oversight. Establishing thorough cyber defence postures requires identifying and prioritising vulnerabilities within interconnected systems, such as encrypted radio networks or battlefield communication devices.
- The absence of response mechanisms that are compatible across military services is another important drawback. Response activities frequently lack coordination in the event of a coordinated cyberattack that impacts all three branches, leading to conflicting strategies or delayed mitigation. Building a unified response mechanism that can handle complex attacks across operational domains requires the establishment of joint cyber operation centres, shared protocols, and information-sharing platforms.
- India needs to increase its investment in cyber R&D, create a pipeline of cybersecurity experts with specialised training in military cyber operations, and establish internal capabilities for red-teaming, or simulated cyberattacks. Although praiseworthy, current training programs are insufficient to develop a workforce that is cyber-ready and able to handle the military's changing digital environment.
- The 2013 National Cyber Security Policy of India established fundamental objectives for safeguarding vital information infrastructure. However, overlapping jurisdictions and policy fragmentation impede prompt decision-making in the absence of an updated, enforceable cyber doctrine designed for military use. To react quickly and forcefully to cyber-threats that target defence systems, institutional clarity and a revised strategic roadmap are required.

India has clearly recognised the strategic significance of digital security in contemporary warfare, as evidenced by its developing cyber capabilities. A solid foundation has been established by organisations like CERT-In and the Defence Cyber Agency. Nonetheless, there are still gaps in the knowledge of how cyberattacks affect military hardware and operations. Improving inter-service coordination, vulnerability mapping, simulation capabilities, and real-time threat assessment are all urgently needed. In order to effectively protect its military and national interests, India must adapt its cyber defence strategy to the rate of technological advancement as cyber warfare continues to redefine the nature of conflict.

COMPARATIVE ANALYSIS OF CYBER, INFORMATION OPERATIONS, COMMAND & CONTROL CAPABILITIES: INDIA AND PAKISTAN

There is a clear disparity between India and Pakistan's command and control (C2), information operations (IO), and cyber capabilities. To increase its military prowess, India has invested heavily in building its technological infrastructure, incorporating robotics and artificial intelligence (AI). Although Pakistan has made some progress, it is still lagging behind in terms of integrating technology and attaining strategic coordination.

A comparatively strong cybersecurity framework underpins India's cyber capabilities, with organisations like CERT-IN and NTRO playing crucial roles in threat mitigation and incident response. India's capacity to identify and counteract cyber threats has been further enhanced by the integration of AI.

There are still issues, though, like reliance on foreign technology and a lack of proactive threat intelligence. In contrast, Pakistan's cyber defence is dispersed and less effective due to the absence of a unified cyber command structure. Pakistan is more susceptible to sophisticated cyberattacks due to the lack of locally developed cybersecurity solutions, indicating a serious capability gap.

India has effectively used AI in the field of information operations to reshape narratives and combat misinformation efforts. India has been able to sway public opinion both domestically and globally by using sentiment analysis and sophisticated media monitoring tools. However, its attempts to create a cohesive strategy are hampered by a lack of agency coordination. However, by using AI for media monitoring and counter-disinformation initiatives, Pakistan has begun to improve its IO capabilities. Despite these initiatives, Pakistan is unable to manage perceptions and carry out psychological operations at scale due to a lack of funding and technical know-how.

AI integration has greatly enhanced India's command and control systems, leading to better operational efficiency and decision-making. These developments have improved military tactics and strengthened situational awareness. However, problems like incompatibility and vulnerability to cyberattacks continue to exist. However, because of its antiquated systems and scant use of AI, Pakistan faces more difficulties in this area. Pakistan's C2 systems are less effective and less flexible in situations that change quickly due to a lack of automation and real-time data processing.

Pakistan needs to develop a comprehensive plan to improve its military's capabilities in IO, C2, and cyber operations in order to close these gaps. A crucial first step is the establishment of a centralised cyber command, which would facilitate improved coordination of cybersecurity initiatives in the military and civilian sectors. Inter-agency communication, incident response, and real-time threat detection should all be handled by this command. While investments in the development of domestic cybersecurity technologies are crucial for lowering dependency on outside solutions, structured training programs would further enhance the capabilities of personnel involved in cyber defence.

Pakistan needs to implement a cohesive information operations strategy that uses AI to manipulate perceptions and carry out psychological operations. The nation's capacity to protect its narratives and thwart hostile campaigns would be strengthened by improved instruments for media monitoring and disinformation analysis. Monitoring hostile IO activity and creating proactive campaigns to sway public opinion should fall under the purview of specialised units. Working together with specialists in communication and the media could increase the impact of these programs.

Pakistan should give top priority to integrating AI into command and control systems in order to improve operational efficiency and decision-making. Situational awareness and responsiveness would be enhanced by automating repetitive tasks and putting AI-driven data processing systems into place. Ensuring seamless interoperability and secure communication between military units is equally important. Modernising Pakistan's C2 infrastructure to meet modern challenges will require investments in cutting-edge hardware and software systems.

A key component of these initiatives is capacity building. Pakistan needs to make investments in creating a skilled labour force by holding workshops, certifications, and training courses on robotics, artificial intelligence, and cybersecurity. These programs should focus on providing military and intelligence personnel with the technical know-how needed to maintain and run cutting-edge systems. To guarantee the responsible use of AI and autonomous technologies, ethical issues must also be taken into account, with open

Capability	India - Strengths	India - Weaknesses	Pakistan - Strengths	Pakistan - Weaknesses
Cyber Operations	Moderately robust cybersecurity framework, AI-enhanced threat detection	Dependence on foreign technologies, insufficient proactive threat intelligence	Initial steps in cybersecurity, some institutional focus	Fragmented cyber command, lack of indigenous technologies
Information Operations	Advanced media monitoring, sentiment analysis, effective narrative shaping	Lack of unified strategy and inter-agency coordination	AI-driven media monitoring and counter-disinformation efforts	Limited resources, less effective perception management
Command & Control Systems	AI-driven decision-making, enhanced situational awareness	Interoperability issues, vulnerabilities to cyber-attacks	Potential for modernization with external collaborations	Outdated systems, minimal AI integration, low automation

Figure 2: Comparative analysis of Pak-India strengths and weaknesses in cyber operations, IO, and C2 systems

policies that are in line with international humanitarian law. Building institutional and public confidence in these developments would be facilitated by the establishment of accountability measures. Although India has made great progress in improving its IO, C2, and cyber operations systems, Pakistan can catch up with strategic investments, domestic development, and capacity building. Pakistan can improve its military preparedness and resilience in a quickly changing, technologically advanced security environment by implementing these suggestions. Following table shows the comparative analysis of Pakistan-India strengths and weaknesses in cyber operations, Information Operations, and Command & Control systems.

Here's a structured table that provides solutions for Pakistan's weaknesses in each capability domain:

Cyber Operations	Fragmented cyber command, lack of indigenous technologies	Establish centralized cyber command, develop indigenous technologies, implement real-time threat monitoring	Enhanced coordination, improved cyber resilience, reduced reliance on foreign technologies
Information Operations	Limited resources, less effective perception management	Enhance AI-driven media monitoring, build dedicated IO units, improve resource allocation and partnerships	Effective counter-disinformation, improved narrative management, stronger psychological operations
Command & Control Systems	Outdated systems, minimal AI integration, low automation	Modernize C2 infrastructure, integrate AI for real-time decision-making, ensure interoperability and secure communications	Faster decision-making, better operational efficiency, increased adaptability in dynamic scenarios

Figure 3: Solutions for Pakistan's weakness in each capability domain

RECOMMENDATIONS & WAY FORWARD

1. National Level Recommendations

Pakistan needs to take a comprehensive approach at the national level to strengthen its strategic and technological capabilities. To supervise and coordinate information warfare and cybersecurity initiatives, a centralised National Cybersecurity Command (NCC) should be set up in the near future. This body must include representatives from the military, intelligence, civilian agencies, and the private sector and function under the direction of a high-level national authority. In order to strengthen society's resistance to cyberattacks and misinformation, the government should simultaneously start public awareness campaigns about digital resilience.

Pakistan must make significant investments in the development of domestic cybersecurity technologies in the medium term in order to lessen its reliance on imported hardware and software. Collaborations with private technology companies and academic institutions would make it easier to create state-of-the-art tools for AI applications and cyber defence. Cyber laws, data privacy, and sanctions for cybercrimes must all be included in a strong legal framework. Additionally, the government ought to set up research and development (R&D) centres specialising in robotics, artificial intelligence, and secure communication technologies.

Long-term technological innovation and self-reliance must be emphasised in a national strategy. A consistent supply of highly qualified professionals would be guaranteed by the establishment of top-tier cybersecurity universities and think tanks. In order to increase effectiveness and transparency and to foster global cooperation for exchanging cyber threat intelligence and best practices, efforts should also concentrate on incorporating AI into governance. Pakistan must make an effort to significantly contribute to international frameworks and standards governing information warfare, cyber operations, and artificial intelligence.

2. Armed Forces Level Recommendations

Establishing a specialised Cyber Command within the military with units for information warfare, offensive cyber operations, and cyber defence should be the main goal of short-term measures at the armed forces level. To guarantee smooth coordination, these units ought to be led by a single person. To upskill employees, structured training courses and workshops should be started right away. These should focus on secure communication protocols, ethical hacking, and cyber forensics.

For increased operational effectiveness and situational awareness, the military should implement AI-driven decision-making systems in the medium term. These systems can improve the precision of strategic decisions, process massive amounts of data in real-time, and automate repetitive tasks. All military networks must simultaneously implement strong cybersecurity measures, such as the creation of domestic encryption technology to guarantee secure communications. To effectively sway public opinion and refute hostile narratives, Pakistan's military should also build up its psychological operations (PsyOps) capabilities.

Command and control (C2) system modernisation ought to be given top priority in the long run. With the help of cutting-edge hardware and software, the military should strive for smooth interoperability across branches. The military would be able to create autonomous systems for combat, surveillance, and reconnaissance with investments in state-of-the-art AI and robotics technologies. Developing strategic partnerships with technologically sophisticated countries would also improve operational preparedness and knowledge exchange. Establishing ethical standards for the application of AI in military operations is necessary to guarantee compliance with humanitarian ideals and international standards.

3. Tactical Level Recommendations

Short-term tactical initiatives should concentrate on educating grassroots staff members about cybersecurity best practices and situational awareness. To reduce the risk of cyber intrusions, field units must be outfitted with secure communication tools and protocols. To get ready for cyber and information warfare scenarios, tactical units should also regularly practise drills and simulations. To react to and eliminate threats instantly, cybersecurity-focused quick reaction teams ought to be put into place.

Tactical units should incorporate AI-based tools for decision-making, target acquisition, and threat detection in the medium term. Enhanced situational awareness through real-time data analytics would significantly improve operational efficiency. Moreover, units should be provided with advanced counter-disinformation tools to identify and mitigate the impact of adversarial IO campaigns. Collaborative training with civilian cybersecurity experts could further enhance the tactical preparedness of the armed forces

In the long term, tactical-level operations must achieve full integration with modernized C2 systems. Field units should be equipped with AI-enabled autonomous systems capable of operating in diverse environments. Continuous skill enhancement programs, coupled with the deployment of advanced surveillance and reconnaissance technologies, would ensure that tactical units remain at the forefront of technological advancements. Additionally, fostering a culture of innovation at the tactical level would enable personnel to adapt quickly to evolving challenges in a technology-driven security landscape.

References

1. Martin, A. (2021, November 26). Robotics and artificial intelligence: The role of AI in robots. AI Business. https://aibusiness.com/verticals/robotics-and-artificialintelligence-the-role-of-ai-in-robots
2. Kovacs, A., & Molder, C. (2010). MAX-01: Multipurpose autonomous Explorer [Review of MAX-01: Multipurpose autonomous Explorer]. Research Gate. https://www.researchgate.net/publication/272148846_MAX-01_Multipurpose_Autonomous_X-plorer#pf1
3. Adib Bin Rashid, Ashfakul Karim Kaushik, Hassan, A., & Mehedy Hassan Bappy. (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
4. Casin, M. (2023, February 26). Artificial intelligence and robotics army in the war of the future: The new military revolution in security [Review of Artificial intelligence and robotics army in the war of the future: The new military revolution in security]. TASAM. https://tasam.org/en/Icerik/70279/artificial_intelligence_and_robotic_armies_in_the_wars_of_the_future_the_new_military_revolution_in_security
5. Agarwala, N. (2023, December). Robots and Artificial intelligence in the military [Review of Robots and Artificial intelligence in the military]. Research Gate. https://www.researchgate.net/publication/272148846_MAX-01_Multipurpose_Autonomous_X-plorer#pf1

6.
Roberts, H., Cowls, J., Morley, J., Taddeo, M., Wang, V., & Floridi, L. (2020). The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. AI & SOCIETY, 36(36). https://doi.org/10.1007/s00146-020-00992-2 7. PEI-Genesis. (2018). The Pros and Cons of Using AI in Military Divisions Worldwide. Google.com. https://www.google.com/amp/s/blog.peigenesis.com/thepros-and-cons-of-using-ai-in-the-military%3fhs_amp=true

8. Adib Bin Rashid, A. K., Hassan, A., & Mehedy Hassan Bappy. (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
9. Agarwala, N. (2023, December). Robots and artificial intelligence in the military [Review of Robots and artificial intelligence in the military]. Research Gate. https://www.researchgate.net/publication/272148846_MAX-01_Multipurpose_Autonomous_X-plorer#pf1
10. Casin, M. (2023, February 26). Artificial intelligence and robotics army in the war of the future: The new military revolution in security [Review of Artificial intelligence and robotics army in the war of the future: The new military revolution in security]. https://tasam.org/en/Icerik/70279/artificial_intelligence_and_robotic_armies_in_the_wars_of_the_future_the_new_military_revolution_in_security
11. International Committee of the Red Cross. (2023), what you need to know about artificial intelligence in armed conflict. *www.icrc.org*. https://www.icrc.org/en/document/what-you-need-know-about-artificial-intelligencearmed-conflict
12. Iqbal, S., Rizvi, S. W. A., Haider, M. H., & Raza, S. (2023). Artificial intelligence in security and defense: Explore the integration of AI in military strategies, security policies, and its implications for global power dynamics. *International Journal of Human and Society, 3*(4), 341–353. http://ijhs.com.pk/index.php/IJHS/article/view/337
13. Kovacs, A., & Molder, C. (2010). *MAX-01: Multipurpose autonomous Explorer* [Review of MAX-01: Multipurpose autonomous Explorer]. Research Gate. https://www.researchgate.net/publication/272148846_MAX-01_Multipurpose_Autonomous_X-plorer#pf1
14. Marwala, T. (2023, July 24). Militarization of AI has severe implications for global security and warfare. *United Nations University*. https://unu.edu/article/militarization-ai-has-severe-implications-global-security-andwarfare
15. Martin, A. (2021, November 26). Robotics and artificial intelligence: The role of AI in robots. *AI Business*. https://aibusiness.com/verticals/robotics-and-artificialintelligence-the-role-of-ai-in-robots
16. PEI-Genesis. (2018). the pros and cons of using AI in military divisions worldwide. *Google.com*. https://www.google.com/amp/s/blog.peigenesis.com/the-pros-andcons-of-using-ai-in-the-military%3fhs_amp=true
17. Roberts, H., Cowls, J., Morley, J., Taddeo, M., Wang, V., & Floridi, L. (2020). The Chinese approach to artificial intelligence: An analysis of policy, ethics, and regulation. *AI & Society, 36*(36). https://doi.org/10.1007/s00146-020-00992-2
18. Thomas, M. (2024, March 1). The risks of artificial intelligence. *Built In*. https://builtin.com/artificial-intelligence/risks-of-artificial-intelligence
19. Gorodnichenko, Y., & Talavera, O. (2020). Social media, sentiment and public opinions: Evidence from Brexit and US Election. European Economic Review, 127, 103411.
20. Mahdi, S. A., & Zwitter, A. (2020). Automation of cyber warfare. In Automation, Communication and Cybernetics in Science and Engineering (pp. 501-510). Springer, Cham.
21. Zuev, D., Kashevnik, A., & Smirnov, M. (2019). Machine learning based detection of anomalies in the behavior of an information system. In 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) (pp. 1947-1950). IEEE.
22. Hammoudeh, M., Nofal, S., & Noor, M. (2019). Towards autonomous adaptive cybersecurity: A reinforcement learning-based approach. IEEE Access, 7, 9255992574.

23. Howard, P. N., & Kollanyi, B. (2016). Bots, Stronger In, and Brexit: Computational Propaganda during the UK-EU Referendum. Available at SSRN 2798311.
24. Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. Science, 361(6404), 751-752.
25. United States Department of Defense. (2018). Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge.
26. Marine Corps Combat Development Command. (2017). Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century. https://apps.dtic.mil/sti/citations/AD1039982
27. Bradshaw, S., & Howard, P. N. (2018). The global disinformation order: 2019 global inventory of organized social media manipulation. Working Paper, 2018.1.
28. Nguyen, T. H., Grishman, R., & Hovy, E. (2016). Joint event extraction via recurrent neural networks. arXiv preprint arXiv:1606.01341.
29. Smith, C., et al. (2020). "Tactical Applications of AI in Perception Management: Analysing Social Media Data for Battlefield Advantage." Military Technology Journal, 35(4), 76-89.
30. Lin, H. (2016). Military Applications of Cyber Operations: Implications for Strategy and Doctrine. Centre for a New American Security (CNAS).
31. Lynn, W. J. (2010). Defending a New Domain: The Pentagon's Cyber strategy. Foreign Affairs, 89(5), 97-108.
32. Scharre, P. (2018). Army of None: Autonomous Weapons and the Future of War. W. W. Norton & Company.
33. Endsley, M. R. (2019). Situation Awareness in Aviation Systems. CRC Press.
34. Galliott, J. (2015). Military Robots: Mapping the Moral Landscape. Routledge.
35. Schmitt, M. N., & Thurnher, J. (2013). "Out of the Loop": Autonomous Weapon Systems and the Law of Armed Conflict. Harvard National Security Journal, 4, 231267.
36. Chaltiel, Y. (n.d.). Information systems. EMSOPEDIA. Retrieved July 11, 2024, from https://www.emsopedia.org/entries/informationoperations/#:~:text=One%20of%20the%20key%20transformer
37. Publication. (n.d.). Www.usiofindia.org. Retrieved July 11, 2024, from https://www.usiofindia.org/publication-journal/the-art-of-perception-management-ininformation-warfare-today-2.html
38. Davies, V. (2023, May 4). How does the military protect itself from hackers? Cybermagazine.com. https://cybermagazine.com/articles/getac-expertsreveal
39. Marwala, T. (2023, July 24). Militarization of AI Has Severe Implications for Global Security and Warfare. United Nations University. https://unu.edu/article/militarization-ai-has-severe-implications-global-security-andwarfare
40. Adib Bin Rashid, Ashfakul Karim Kaushik, Hassan, A., & Mehedy Hassan Bappy. (2023). Artificial Intelligence in the Military: An Overview of the Capabilities,
41. Cebrowski et al. 1998. Network-Centric Warfare - Its Origin and Future. U.S. Naval Institute. https://www.usni.org/magazines/proceedings/1998/january/network-centricwarfare-its-origin-and-future