NJESR/June-2026/Volume-8/Issue-6 E-ISSN-2582-5836
DOI-10.53571/NJESR.2026.8.6. 33-42

Artificial Intelligence in Cyber Warfare: A Primer

Shikha verma

Assistant professor

Hari Sahay Law College Gorakhpur

(Received-15 May2026/Revised-28May2026/Accepted-10June2026/Published-16June 2026)

Abstract

Artificial Intelligence (AI) has become a major change in the world of cyber warfare, changing how countries, military groups, and other groups carry out their online activities.AI helps speed up and improve cyber operations by automatically finding threats, checking for weaknesses, analyzing harmful software, and responding to security incidents. At the same time, enemies can use AI to create more advanced attacks, spread false information, and target important systems. Adding AI to the cyber world brings both new chances and new problems, and it raises questions about safety, who is responsible, moral issues, and global peace. This paper looks at how AI is used in cyber warfare, covering both attacking and protecting strategies, the bigger picture of how it affects strategy, the legal and moral issues it brings, and what the future might hold. The paper ends by saying that although AI can greatly help with cybersecurity, if it is used wrongfully, it can make cyber conflicts worse and increase global risks. So, strong rules, teamwork between countries, and careful use of AI are needed to make sure it is used safely and well in cyber warfare.

Keywords:-Artificial Intelligence, Cyber Warfare, Cybersecurity, Machine Learning, Autonomous Systems, Information Warfare, National Security

Introduction

Cyber warfare has become a big part of how countries protect themselves. At the same time, new advances in artificial intelligence have changed the way organizations and governments handle information, make decisions, and carry out complex tasks. The mix of AI and cyber warfare is one of the biggest changes in security today.AI can help defend against cyber attacks by spotting threats faster and responding better. But it can also help attackers by making smarter malware and running influence campaigns. The 21st century has brought huge changes to the world's security because of fast improvements in how we communicate and share information. More and more, governments, military groups, businesses, and people rely on digital systems. This has made

cyberspace just as important as land, sea, air, and space in terms of national power. As societies get more connected through the internet, cyber threats have gone from small crimes to big tools of state power and warfare.In this context, cyber warfare is now one of the biggest challenges for national and international security.Cyber warfare uses digital tools to mess up an enemy's information systems, communication networks, and key infrastructure.

Unlike regular wars, cyber attacks can happen anywhere and without anyone knowing who did it.Cyber operations can target military systems, government offices, financial networks, hospitals, transportation, and energy systems.The number and smartness of cyberattacks have shown that cyberspace is now a place where countries compete for power, influence, and safety.

At the same time, AI has become one of the most important technologies in today's world.AI covers many ways computers can do things that usually take human intelligence, like learning, thinking, solving problems, seeing things, and making decisions.New improvements in machine learning, deep learning, natural language processing, and neural networks have made AI systems much better.These technologies can handle large amounts of data, find hidden patterns, make predictions, and do complex tasks quickly and accurately.

The coming together of AI and cyber warfare means a big change in technology with big effects on security and defense.AI can change both attacking and defending in cyber operations by making them more efficient, faster to decide, and better at understanding the situation.In cybersecurity, AI systems can check network activity as it happens, find unusual things, spot harmful actions, and automatically respond to threats.These abilities are more important now because organizations face too many cyberattacks and security alerts for humans to handle properly.

On the attack side, AI can help automate finding weaknesses, planning better attacks, and creating smart malware that avoids traditional security systems.

AI can also make realistic phishing emails, fake documents, synthetic voices, and deepfake videos that help in tricking people and spreading false information.Because of this, AI makes cyber attacks more effective and lowers the skill needed to carry out complex ones, which could hurt both governments and non-government groups.

Using AI in cyber warfare also brings up important questions about strategy, ethics, and laws.AI systems can work so fast that human leaders might not be able to control or understand their actions, leading to accidents or worse during conflicts.The fact that some AI systems can act on

their own brings up issues about who is responsible, how clear their actions are, and who is in charge.Also, using AI for surveillance, misinformation, and influencing people raises concerns about privacy, lies, and controlling public opinion.These changes have made governments, international groups, and researchers look into the impact of AI on global security and try to create good rules for it.

From a military point of view, AI is seen as something that can greatly boost the power of cyber operations.Big countries like the United States, China, Russia, and NATO members are spending a lot on AI to improve their cyber abilities.The push to win in AI has led to worries about a cyber arms race, where countries develop more advanced AI tools and systems to attack.Because of this, it's important for leaders, military experts, cybersecurity workers, and scholars to understand how AI is used in cyber warfare.This paper gives a full picture of how AI is used in cyber warfare by looking at its basics, both offensive and defensive uses, the big picture of how it affects security, the ethical problems, and what the future might look like.

It tries to show both the good and bad sides of using AI in cyber operations.It also emphasizes the need for smart innovation, cooperation between countries, and good laws to manage AI use.By looking at how AI and cyber warfare connect, this study helps everyone understand how new technology is changing how we fight in the digital age.

Literature Review

Existing literature shows more attention is being paid to AI in cyber operations.Researchers have focused on machine learning for detecting intrusions, assessing security risks, classifying malware, gathering threat intelligence, and creating defensive systems that work on their own.Scholars studying strategy have looked at how AI might affect deterrence, the chance of conflicts escalating, and military competition.Yet, there are still big gaps when it comes to rules and regulations, who is responsible when things go wrong, and what international standards should be in place.

Adding AI to cyber warfare has grabbed a lot of interest from researchers, government officials, military planners, and cybersecurity experts.The existing studies show AI can greatly improve both attacking and defending in cyberspace, but it also brings new problems in security, ethics, and how things are controlled.More research shows AI is changing the way cyber threats happen by making them faster, bigger, and more advanced.

Early studies looked at using machine learning in cybersecurity.Goodfellow, Bengio, and Courville (2016) said machine learning can find patterns in large sets of data and get better over time.Their work set the stage for many cybersecurity uses, like spotting intrusions, identifying malware, catching unusual activity, and analyzing threats.Researchers say traditional methods that rely on known threats are not enough anymore, so AI-based systems are needed for better security.

Several studies have looked at AI in cyber defense. Sommer and Paxson (2010) said machine learning can help detect intrusions by spotting strange network behaviors.Buczak and Guven (2016) reviewed using data mining and machine learning in cybersecurity and found AI makes it easier to find and predict threats.These studies suggest AI can process a lot of security data faster than people can, helping catch and stop attacks more quickly.

Research has also covered using AI in threat intelligence.Husák et al.(2018) said AI can automatically collect, process, and analyze threat info from various sources.This helps organizations spot future threats and build better defenses.AI-based threat tools are getting more important as cyberattacks become more complex and happen more often.

Besides defense, scholars have looked at AI's offensive use in cyberspace. Brundage et al.(2018) said AI can be used by bad actors to run attacks automatically, make better phishing attempts, and create malware that can slip past regular detection.Their report, The Malicious Use of Artificial Intelligence, warned that AI makes it easier for both countries and non-state groups to carry out advanced cyber operations.They said AI could change the security landscape by allowing attacks that are larger and more targeted.

The idea of using AI in autonomous cyber weapons has been studied a lot. Scharre (2018) said these systems can perform complex tasks without human help.While most discussions started with military use, now the same concerns are being looked at in cyber warfare.These systems can find targets, use weaknesses, and attack quickly without human input.Although they could make operations more effective, people are worried about who is responsible, the unexpected effects, and how well these systems follow international laws. Another big topic is how AI affects information warfare and influence campaigns. Rid (2020) studied how disinformation has changed over time and how new tech makes it more powerful.Recent studies show AI tools like natural language processing, generative AI, and deepfakes are changing how information warfare is done.Chesney and Citron (2019) said

deepfake tech can create very realistic audio and video, making it hard to tell real from fake information.This poses a danger to democratic institutions, public trust, and national security. The strategic effects of AI in cyber warfare have also been widely talked about. Buchanan (2020) said cyber operations are now a key part of competition between major powers.AI is seen as a tool that makes intelligence, defense, and attacks better.Scholars think AI might change the balance between attack and defense in cyberspace by making decisions faster and allowing quick attacks.However, there are worries that AI systems might act too fast for humans to respond, increasing the chance of conflict.

Ethical and legal issues are another important area.Taddeo and Floridi (2018) said using AI in security needs to be careful about fairness, transparency, and who is held responsible.Researchers are concerned about biased algorithms, privacy violations, and the bad use of AI.Also, the fact that some AI systems work on their own makes it tricky to figure out who is accountable when something goes wrong.Existing international laws, like the rules of necessity, proportionality, and distinguishing between civilian and military targets, might struggle when applied to AI in warfare.

Even though a lot of research has been done, there are still gaps.First, there's not much agreement on how to govern AI in cyber warfare.Studies know the risks, but real plans for international rules are still missing.Second, there's not much real-world data on how effective AI-powered attacks really are, because military cyber activities are secret.Third, the long-term impact of using AI heavily in cyber warfare needs more study, especially on how it affects deterrence, the chances of conflict, and global stability.

Overall, the research shows AI is a big part of how cyber warfare is changing. The studies give useful insights on how AI is used technically, its role in strategy, and its ethical issues.But since AI is growing fast, more research is needed to handle the new problems and create good rules.Understanding these changes is key to making sure AI helps cybersecurity and international peace instead of making things worse.

Foundations of Artificial Intelligence

AI is about computer systems that can do things that usually need human intelligence.These systems use technologies like machine learning, deep learning, reinforcement learning, natural language processing, and computer vision.In cybersecurity, AI can look at huge amounts of data, find patterns, and help with making important decisions.These abilities make AI very useful in cyber operations where quick action and the ability to handle large tasks are important.Artificial

Intelligence, or AI, is the ability of computer systems to perform tasks that normally require human thinking, like learning, reasoning, solving problems, making decisions, understanding what is seen or heard, and using language.The idea of AI was first clearly explained by John McCarthy in 1956, who called it the science and engineering of making intelligent machines.In recent years, improvements in computer power, the amount of available data, and better algorithms have turned AI from just an idea into a real technology used in many areas, such as healthcare, finance, transportation, defense, and cybersecurity.Basically, AI is designed to create systems that can look at information, learn from it, adjust to new situations, and carry out tasks on their own.Unlike regular software that follows fixed instructions, AI systems can get better by using data and learning over time.This ability to change and improve makes AI especially helpful in places like cyberspace, where threats and methods used by attackers are always changing.

Types of Artificial Intelligence

Artificial Intelligence can be broadly categorized into three levels based on capability:

Artificial Narrow Intelligence (ANI)

Artificial Narrow Intelligence, also known as Weak AI, is designed to perform specific tasks within a limited domain. Examples include virtual assistants, recommendation systems, facial recognition software, and cybersecurity threat detection systems. Most AI applications currently deployed in cybersecurity and cyber warfare belong to this category.

Artificial General Intelligence (AGI)

Artificial General Intelligence refers to systems capable of performing any intellectual task that a human can perform. AGI remains largely theoretical and has not yet been achieved. However, researchers continue to explore technologies that may eventually lead to human-level intelligence.

Artificial Superintelligence (ASI)

Artificial Superintelligence represents a hypothetical stage where machines surpass human intelligence in virtually all cognitive functions. Although ASI remains speculative, discussions regarding its potential implications have become increasingly important within security and defense communities.

AI in Offensive Cyber Operations

AI allows for automatic gathering of information, spotting targets, finding weaknesses, creating personalized phishing attempts, adjusting malware, and improving attacks.Machine learning can look at networks, find vulnerabilities, and decide which weaknesses to exploit first.Bad actors

might use AI to make realistic fake messages for phishing and social engineering attacks.Smart cyber tools can speed up attacks and make the whole process more efficient.

Relevance of AI to Cyber Warfare

AI has special qualities that make it very useful for cyber warfare.Today's cyber world creates huge amounts of data that humans can't process quickly enough.AI can handle this data fast, spot unusual activity, find dangers, and help with decision-making as it happens.In attacks, AI can help with finding targets, discovering weaknesses, choosing who to attack, and launching attacks automatically.For protection, AI helps detect intrusions, study harmful software, look for threats, and manage security incidents.AI can learn from past attacks and change how it works to deal with new threats, which gives a big advantage in the cyber world.Also, AI helps speed up cyber activities, letting organizations react to threats quicker than they could with old, manual methods.As cyber attacks get more complex, AI acts as a powerful tool that improves both defense and attack capabilities.

AI in Defensive Cyber Operations

Artificial Intelligence (AI) is now a key part of how modern organizations protect themselves from cyber threats.It helps detect, understand, and deal with these threats faster and more accurately than old security methods.As cyberattacks get more complex, companies struggle with the huge amounts of security data coming from their networks, devices, and software.AI-powered security operations offer better tools to find threats, act quicker, and make systems more secure.Using techniques like machine learning, deep learning, and data analysis, AI helps shift cybersecurity from just reacting to threats to being able to predict and stop them before they happen.

Role of AI in Cyber Defense

The main goal of defensive cyber operations is to keep information systems, networks, and important facilities safe from unwanted access, problems, and harmful actions.Many traditional cybersecurity tools use signature-based methods to find threats by matching them to known patterns.These tools work well for attacks that have been seen before, but they can't always catch new or changing threats.AI helps fix this by looking at a lot of data and spotting strange patterns that could mean something is wrong. Unlike regular systems, AI-based security tools keep learning from new information and adjust to new dangers.This allows companies to find attacks

that happen for the first time, long-term threats, and complex malware that might otherwise go unnoticed.

Intrusion Detection and Prevention Systems

AI plays a big role in making cyber defense better, especially in improving Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).These systems keep an eye on network traffic and what's happening with computer systems to spot possible security problems.Using machine learning, these systems can study how networks usually work and create a normal pattern.If something happens that doesn't fit this pattern, the system can send warnings or take action to stop the issue.AI helps detect new threats that haven't been seen before because it looks at how things behave instead of just checking for known bad things.Also, deep learning can handle complicated data from networks and find small signs of danger that regular tools might miss.Because of this, AI-powered IDS and IPS systems are better at finding threats and make fewer false alarms.

Malware Detection and Analysis

Malware is still one of the most common and harmful types of cyberattacks.Most traditional antivirus programs use signature databases to spot bad software, but newer malware uses tricks like changing its code or structure to avoid being detected.AI-based systems use machine learning to study how files look, how their code is built, and how they behave.These systems can find harmful software even if it's a new type that hasn't been seen before.By looking at how a program uses system resources, AI can tell the difference between good and bad software very accurately.

Also, AI helps speed up malware analysis by doing tasks that used to take a lot of human work.Security experts can use AI tools to group different types of malware, find how attacks happen, and understand the risks better and faster.

Threat Intelligence and Predictive Analytics

Cyber threat intelligence means gathering, organizing, and looking at information about possible cyber dangers.AI makes this process better by automatically gathering data from many places like security records, social media, hidden websites, and databases that track threats. Using machine learning, computers can find patterns and connections in big amounts of data, which helps companies spot new threats before they happen. Predictive analysis lets security experts guess what attacks might come next, check where systems might be weak, and take steps to stop

problems before they start.For instance, AI tools for threat intelligence watch for signs that something harmful might happen across the internet and alert people early if an attack is possible. This helps companies get ready for threats and makes it less likely that hackers can break in successfully.

Automated Incident Response

More cyberattacks are happening and they are getting more complicated, making it harder to handle them by hand.Security teams in Security Operations Centers (SOCs) often get overwhelmed because they receive too many security alerts every day.

AI helps solve this problem by using Security Orchestration, Automation, and Response (SOAR) tools. These systems can automatically check security alerts, connect related events, and carry out set actions. For instance, AI can cut off infected devices, block harmful IP addresses, stop dangerous processes, and start investigations without needing a person to do it.Automating how incidents are handled speeds up the response, lowers the damage done, and lets security experts focus on tougher issues. By making it faster to stop and fix threats, AI improves how well cyber defenses work.

Conclusion

Artificial intelligence is changing how cyber warfare is conducted.It can automatically analyze information, help make better decisions, and carry out cyber operations on a larger scale, which brings both chances and dangers.While AI can help improve defenses, it also makes it easier for attackers to carry out more advanced attacks.It is important to balance the use of AI with security, responsibility, and global stability.Future policies should focus on using AI in a responsible way, making sure there is human control, and working together internationally to ensure AI helps make cybersecurity stronger instead of causing more problems.AI is now a big part of defensive cyber operations, helping organizations find, understand, and deal with cyber threats better than old methods.It is used in areas like finding intrusions, analyzing malware, gathering threat information, predicting attacks, and automatically responding to incidents, which greatly improves cybersecurity.Even though there are challenges like poor data, difficulty in explaining AI decisions, and attacks designed to trick AI, AI is still a key part of modern cyber defense.As cyber threats keep getting more complex, the role of AI in making cybersecurity stronger and protecting important systems will become even more vital.

References

Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of geopolitics*. Harvard University Press.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., hÉigeartaigh, S. Ó., Beard, S., Belfield, H., Farquhar, S., ... Amodei, D. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*. Future of Humanity Institute, University of Oxford.

Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

Chesney, R., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review, 107*(6), 1753–1820.

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.

Husák, M., Komárková, J., Bou-Harb, E., & Čeleda, P. (2018). Survey of attack projection, prediction, and forecasting in cyber security. *IEEE Communications Surveys & Tutorials, 21*(1), 640–660. https://doi.org/10.1109/COMST.2018.2871866

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.

Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war*. W. W. Norton & Company.

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

Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In *Proceedings of the 2010 IEEE Symposium on Security and Privacy* (pp. 305–316). IEEE. https://doi.org/10.1109/SP.2010.25

Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. *Science, 361*(6404), 751–752. https://doi.org/10.1126/science.aat5991