TECHNOLOGY FEATURE Industrial News / Technology Report / Research Communication

Autonomous AI to Autonomous Threats: Why Cybersecurity Is the next Big Battlefield

Artificial Intelligence is transforming industries—but it is also reshaping cyber threats into faster, smarter, and more dangerous adversaries.

Abdul Moez Bin Mansoor | Information Technology Student | Published: 26th April 2026
moezmansoor44@gmail.com | Position: Researcher / Student

Abstract

Artificial Intelligence systems can do things on their own without people helping them. This is making things better and more efficient in areas. However it is also creating kinds of cyber dangers that are smart and hard to stop. Artificial Intelligence systems that can harm us like malware and hacking tools are changing the way cyber risks work. They are making old security methods less effective. This research looks at how Artificial Intelligence systemsre turning into threats. It explains why cybersecurity is a challenge in todays world.

Introduction

Artificial Intelligence is a part of our lives now. Artificial Intelligence systems can make decisions on their own without people helping them. This has changed industries. Artificial Intelligence is also a problem for people who try to keep our information safe. Cybersecurity is not about having passwords and good firewalls anymore. It is like a fight between computers. When bad people make code that can think and work on its own it is very hard to stop. We need to have Artificial Intelligence systems that can fight against the ones. Artificial Intelligence is a deal and it is making the world of cybersecurity very different. This paper is about how Artificial Intelligence's changing the way people attack computers and how we can defend against these attacks. It is about the kinds of threats that Artificial Intelligence systems can make and how we can stop them. The fight against Artificial Intelligence systems is a challenge. Artificial Intelligence systems that can think and work on their own are a problem. Artificial Intelligence is the issue here. We need to focus on Artificial Intelligence to solve the problem.

> ***"This is not just a technological shift it is a transformation of cybersecurity into an algorithmic war"***

Literature Review

The development of intelligence that works on its own is changing technology really fast. This is creating opportunities that we have never seen before but it is also making things more complicated when it comes to security. Artificial intelligence systems that can make decisions without people telling them what to do are being used more and more in important areas like healthcare and finance.

Studies have shown that using intelligence in these areas can make things more efficient but it also makes it easier for hackers to get in. When artificial intelligence systems get better and can learn on their

own they become more vulnerable to attacks. These attacks can make the artificial intelligence system do what the hackers want or they can steal information.

Some experts think that the use of intelligence in cyber warfare is changing the way we think about security. Artificial intelligence systems can be used to launch cyberattacks with very little help from people. These attacks can be hard to detect and stop. They are getting faster and smarter all the time. Artificial intelligence is also being used to defend against cyberattacks. This is creating a kind of competition between the hackers and the people who are trying to stop them.

Artificial intelligence and cybersecurity are closely related to each other. There are concerns about who's responsible when something goes wrong with an artificial intelligence system. We need to have rules and laws in place to make sure that artificial intelligence systems are safe and secure. We also need to work internationally to deal with cyber threats that can come from anywhere in the world.

Overall artificial intelligence has the potential to change things for the better but it also creates new risks that we need to be aware of. Cybersecurity is an issue that affects us all and we need to be careful and smart, about how we use artificial intelligence. Artificial intelligence systems are being used in areas, including healthcare, finance and transportation and we need to make sure that they are safe and secure. Artificial intelligence is a tool and we need to use it wisely.

From Static to Dynamic Threats

To really understand how big this problem is, we need to look at how the people who make threats have changed over time and what they are doing. In the ten years the way people do cyberattacks has been pretty much the same and straightforward. A hacker would slowly look at a network find a weakness make a script or payload and then do the attack by hand. This took time. People made mistakes. The bigger problem was that the bad software used in these attacks was not flexible. If the people in charge of security found out what the bad file looked like they could update their antivirus programs. Stop the threat from happening on the whole network.

Now cyberattacks are becoming more of a problem because they can change and adapt on their own. The old way of stopping cyberattacks is not working well as it used to. We need to find ways to deal with these kinds of threats. Cyberattacks are a problem. The new way that cyberattacks work is with threats that can change and adapt on their own. This is different from the way things used to be where people were in charge and things happened slowly. Artificial Intelligence is the key to understanding these threats.

Methodology

This study uses a method to look into how autonomous Artificial Intelligence systemsre turning into autonomous cyber threats and what this means for global cybersecurity. An exploratory design is used to understand trends, challenges and risks linked to Artificial Intelligence powered cyber threats. Information was gathered from databases like Google Scholar, IEEE Xplore and ScienceDirect using keywords such as " Artificial Intelligence," "cybersecurity threats," "Artificial Intelligence driven attacks," "machine learning in security " and "adaptive malware." Artificial Intelligence is the focus of this research.



Figure 1:Autonomous AI to Autonomous Threats in Cybersecurity *Credit: CyberSec Visuals*

Key Findings & Impact

AUTONOMOUS EVASION

Threats Mechanism

The aspect of a threat is its ability to make decisions based on its environment at any given time. Traditional security solutions, such as Endpoint Detection and Response systems are insufficient for dealing with threats. This is because these systems rely on known threats. An autonomous threat differs as it can alter itself making it difficult for Endpoint Detection and Response systems to detect. Therefore traditional security systems like Endpoint Detection and Response are unable to prevent these threats. Artificial Intelligence systems are the ones that can make these threats.

Adaptive Evasion

One of the dangers of computer programs is that they can change and hide from the security tools that are supposed to stop them. When a bad program does an attack the main bad part of the program stays the same. The rest of the program gets all mixed up. Changed every time it spreads to another computer. When these bad programs figure out that someone is looking for them they can stop doing things blend in with the things the computer is doing or change how they appear on the computer. Artificial Intelligence is used to make these programs.

Lateral Movement

When a computer program that can work on its own gets into a network it usually doesn't cause problems away. The program moves around the network slowly. It uses tools to look at the network and find out where important information is stored. It looks for databases, servers and main controllers. It also checks which user accounts have privileges and quietly tries to get their passwords. Since the program does all this work by itself it doesn't create any activity on the network. This makes it very hard for security people to notice what is happening until the program finishes causing damage. Artificial Intelligence systems are good at this kind of movement.

Attack life cycle

Autonomous Attack

To really understand how fast and serious this battlefield is you need to look at each step of the attack process one by one. An Artificial Intelligence powered attack is different. This is because the autonomous attack process, for Artificial Intelligence driven attacks happens quickly. Artificial Intelligence is the key to understanding these attacks.

Phase 1: Reconnaissance

The attack starts with a computer program that searches the internet for spots. This program looks for gaps in the system or flaws in apps that are connected to the internet. The program was trained to target industries or system designs. Artificial Intelligence is used to train these programs.

Phase 2: Evasion and Infiltration

When the program finds what it is looking for it starts working. If it hits a firewall or something designed to catch intruders the program changes its code. Artificial Intelligence systems are good at this kind of evasion.

Phase 3: Exploitation

Inside the program looks for weaknesses in the software. The program uses these problems to make itself part of the computers operating system. It does this by taking advantage of these weaknesses. Artificial Intelligence is used to find these weaknesses.

Phase 4: Privilege Escalation

The malware secretly watches the network to see what users are doing. Using this information the malware learns how to create login details or change who has access to what on the network. This makes the malware stronger. Allows it to take control moving from just a regular user to becoming the full administrator of the malware itself. Artificial Intelligence systems are good, at this kind of escalation.

Phase 5: Propagation

The program replicates itself.

Tricking people into doing something they should not do is not what it used to be. In the past tricking people was about sending emails to fool them. Tricking people uses intelligence to influence peoples thinking. Computers can look at a persons media, old hacked data and company information to create a custom attack on the company. For example a computer can make a message that sounds like a companys boss telling the person in charge of money to send a lot of money to a bank account in another country. The problem is that artificial intelligence can speak to people in a way that sounds very real and it can do this with people at once. This means that the old methods of teaching employees to be careful are not effective anymore. Tricking people into doing something they should not do is becoming better at tricking people.

Defence Shift

Algorithmic Defense

You cannot defend against a computer attack with a reaction. The truth is, in this kind of battle humans just cannot react enough. When a security expert receives an alert examines the data and figures out what is wrong the computer threat has already locked up the companys data. To stay safe companies have to change how they defend themselves: they need to use computers to fight computers. They have to use intelligence to fight against artificial intelligence threats. This is the way to keep up with the speed of computer attacks. Companies must adopt this way of defending themselves to survive.

AI-Driven SOCs

The modern Security Operations Center needs to use intelligence to help it. This defensive artificial intelligence keeps watching the network all the time to figure out what is usual for the company. It does not just look for things it already knows about the company. Instead it looks for things that're not normal for the company. For example if a server usually only talks to a database inside the company but then tries to send files to a computer it does not recognize outside the company at 3:00 AM the defensive artificial intelligence notices this as something. A Security Operations Center with intelligence is a good thing for the company. Defensive artificial intelligence is important for the Security Operations Center to keep the company safe.

Self-Healing Networks

When defensive artificial intelligence sees a threat coming from somewhere it acts quickly to protect the company. In a matter of milliseconds the defensive algorithm changes the firewall settings to keep the company safe. The bad code is separated from the system to keep the company safe. Advanced systems are moving towards a "self-healing" setup to keep the company safe. This means if a key system file is damaged by malware the defensive artificial intelligence can quickly find a backup to restore the system. This all happens without any delay to keep the company safe. The defensive artificial intelligence and the autonomous threat are important here. The defensive artificial intelligence fights against the threat to keep the company safe. It keeps the system safe from the threat to protect the company.

Zero Trust

The way of doing network security, where everything inside the firewall is considered safe is gone. Now we have something called Zero Trust Architecture. In a Zero Trust setup no device, no user and no application is automatically trusted, whether it is inside or outside the company network. Every time someone or something tries to access the network it has to be checked and approved to keep the company safe. This is done using computer programs to verify the identity. This helps stop things from moving around the network so even if something bad gets into one part of the network it cannot just go into another part of the Zero Trust Architecture network to harm the company.

What's Next?

FUTURE OUTLOOK

An Algorithmic Arms Race

We have made a world that is really connected through technology, which means we have a space where we can be attacked. The problems that come from this fight with algorithms like disruptions in data transfer, financial issues and national security threats are already happening. If we only rely on humans to protect our systems we will have problems. In this time the winner will not be the one with the defenses. The one with the advanced and efficient artificial intelligence algorithms will win. The fight to secure our computers and information has become a battle of the century. Both artificial intelligence and cybersecurity are now very important to keep us safe.

Cybersecurity is like a war and artificial intelligence plays a role in it.

Conclusion

The change from Artificial Intelligence to threats is a big deal in the history of keeping our computers and information safe. We have made a world that is really connected through technology, which means we have a space where we can be attacked and we do not even see it. The problems that come from fighting with algorithms like when our data does not transfer or we have financial issues or our national security is threatened are already happening. If we only use people to protect our systems we will have problems. We are not just protecting our technology we are also protecting our society. In this time the person who wins will not be the one with the protection but the one with the best and most efficient Artificial Intelligence algorithms. The fight to keep our computers and information is a very important battle of the 21st century. Both Artificial Intelligence and cybersecurity are very important now. Cybersecurity is like a war and Artificial Intelligence plays a role in this war. We are using Artificial Intelligence to fight against threats. This is a big part of cybersecurity. The battle to secure our computers and information is a fight between Artificial Intelligence and cybersecurity and Artificial Intelligence is a player, in this battle.

About the Author

Abdul Moez Bin Mansoor is a Data Automation Specialist and Full Stack Web Engineer based in Faisalabad, Pakistan, currently pursuing a Bachelor's degree in Information Technology. His work focuses on building scalable, data-driven applications, with research interests in data analytics, artificial intelligence, and innovative digital solutions for real-world challenges]. They can be reached at moezmansoor44@gmail.com

Keywords: Artificial Intelligence; Cybersecurity; IoT; Pakistan Tech

References

1. The National Institute of Standards and Technology (NIST). (2024). *NIST cybersecurity framework (CSF) 2.0.* https://www.nist.gov.
2. The European Union Agency for Cybersecurity (ENISA). (2023). *ENISA threat landscape 2023*. https://www.enisa.europa.eu.
3. IBM Security.(2023). *Cost of a data breach report 2023*. https://www.ibm.com.
4. McKinsey & Company. (2023). *The cybersecurity implications of artificial intelligence*. https://www.mckinsey.com.

5. Microsoft Security. (2024). *Artificial intelligence and cybersecurity threat landscape report* https://www.microsoft.com/
6. Cisco. (2023). *Cybersecurity readiness index 2023*. https://www.cisco.com.
7. Kaspersky. (2023). *Global cybersecurity threat report.* https://www.kaspersky.com/
8. OpenAI. (2023). *GPT-4 technical report*. https://arxiv.org/abs/2303.08774.
9. European Commission. (2024). *Artificial intelligence and cybersecurity risks*. https://digital-strategy.ec.europa.eu.
10. World Economic Forum. (2024). *Global cybersecurity outlook 2024*. https://www.weforum.org.
11. European Union Agency for Cybersecurity (ENISA). (2024). *Artificial intelligence and cybersecurity: Opportunities*. https://www.enisa.europa.eu
12. Palo Alto Networks. (2023). *Unit 42 threat intelligence report*. https://www.paloaltonetworks.com
13. IBM. (2024). *Artificial intelligence in cybersecurity: Threats and defenses.*
14. https://www.ibm.com.
15. Google Cloud. (2023). *Google Cloud security*. https://cloud.google.com/security.
16. MIT Technology Review. (2023). *How artificial intelligence is transforming cyberattacks.* https://www.technologyreview.com.
17. CrowdStrike. (2024). *Global threat report*. https://www.crowdstrike.com.
18. Verizon. (2024). *Data breach investigations report (DBIR).* https://www.verizon.com/business/resources/reports/dbir/
19. Darktrace. (2023). *Artificial intelligence-driven cyber defense systems report* https://www.darktrace.com.
20. Russell, S. J., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.
21. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). *Generative adversarial nets. Advances in Neural Information Processing Systems, 27.*