Artificial intelligence in Cyber Security

Individual Assignment

Contents

1) Abstract

Advances in data technology will create computers that act and behave the same as humans. AI is a related and unique aspect of data technology that requires a machine to react and act because of the human mind. Major non-true intelligence options embody the analogy of human senses. The system is capable of recognizing bits and speech as options placed at intervals in the system to implement potential activities in traditional life situations without the help of humans. However, computing is the study of intelligent agents that take the state of their environment into account and achieve their goals. Most of the systems in the computer world are designed to meet the needs of the situation with the application of the unique characteristics of the human aspects. Computing is typically an association of related humans with problem-solving techniques for understanding activities and human-inspired components for learning, decision-making, and higher levels of emotional cycle functioning. As opposed to human intelligence, computing is machine-based intelligence.

In the field of cyber security, the last few years have seen an evolution from cybercrime to cyber warfare. Although security devices have become fashionable and powerful, cyber-attacks and threats are increasing daily. The main reason for this cyber attack is our outdated threat detection strategies to detect the threat or malware breakout. Cybercriminals are increasingly coming up with clever ways to infect networks and computer systems with various types of malware, bypassing computer security devices or programs. Computing changed every space it was introduced to. MasterCard anomaly detection and malware scanning are made possible using MIL and AI algorithms. AI algorithms are ready to work more efficiently than humans once they incorporate processing speed. Also, AI algorithms will determine the top annoying hidden fraud clues that one simply cannot observe. AI facilitates cutting down on the number of false positives that arise with the use of non-artificial fraud detection strategies. Computational strategies have often found this to be equally cost-effective for all phases of cyber security.

2) Introduction

Applying AI in cyber security is the method of analyzing giant amounts of risk information and, therefore, the relationship between threats in your enterprise data systems to identify new types of attacks. The resulting new levels of intelligence feed human teams across multiple classes of cybersecurity with improved IT quality inventory, threat exposure, management efficiency, risk prediction, incident response, and improved communication around cybersecurity within the organization. With their ability to quickly analyze countless incidents and pinpoint different types of threats, AI technologies facilitate security teams to reduce the risk of a breach and improve their security posture with efficiency and effectiveness.

Wherever network security arrangements incorporate computer science and machine learning to strengthen security, it is called artificial intelligence (AI).

AI cybersecurity addresses the need to change threat assessment in complex environments. Specifically, the quadrant here measures a pair of use cases for AI in AI cybersecurity: [1]

- Anomaly detection: AI can typically find anomalies in the day-to-day operation of a network. This helps you see once and wherever your users are accessing the network. Entry devices even have AI integration for analytics. In surprising behavior, some solutions block users. Different solutions simply send alerts.

- Classification of information: AI is effectively a classification utility. This speeds up the screening process for malware or dangerous actors. This often provides organizations with tons of knowledge.

Attack surfaces for cyber threats are rapidly increasing, fueled by the explosion of remote operations and the associated increase in the use of Internet-connected services. Ancient signature-based methods of combating these threats are proving increasingly ineffective. Detecting a threat or expecting notification from users after developing a signature to recognize and counter it is too slow to make organizations responsible for attacking.[2]

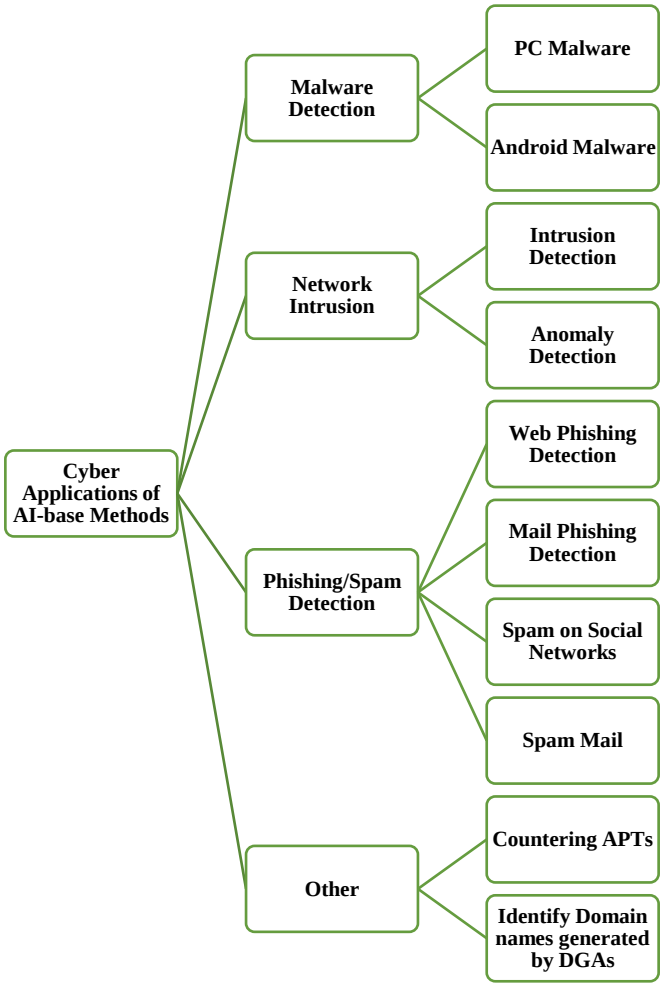
This is where AI comes in. The only way to combat the various emerging threats is for security systems to proactively detect them as they appear and adapt accordingly. This method can even work on terminal bites.

Cutting out humans at this level makes the system compete because of AI, which will analyze countless sets of information to look for all kinds of threats. Instead of looking for specific software package signatures for well-known attacks, it will detect malware, phishing, or "crypto-jacking," which occurs when infected systems are routed to mine cryptocurrency for hackers. If any of those behaviors are encountered, the AI learns and improves its defenses, providing more effective cyber protection.[3]

The cyber attack surface in modern enterprise computing environments is large and growing rapidly. This suggests that analyzing, improving, and enhancing an organization's cyber security posture simply requires human intervention.

An AI-powered Risk Management Approach to Cybersecurity

- The right collection of data
- Application for Representation Learning.
- Machine Learning Customization
- Cyber Threat Analysis
- A Model Security Problem



AI and machine learning are rapidly becoming essential to data security because they can rapidly analyze massive data sets and track a wide range of cyber threats, from malware threats to shady behavior that can lead to a phishing attack.[4]

These technologies enable constant learning and improvement by extracting information from past experiences and identifying new types of attacks that may occur today or tomorrow.

Malware is constantly evolving. AI can detect new malware by comparing its behavior to that of "normal" software without requiring a specific code signature. AI can prevent new risks rather than reacting to old ones. AI is also good at avoiding threats from bots trying to take over or

create accounts. AI can distinguish between helpful automated behavior and dangerous activity by evaluating large amounts of data. Another area where AI can help with cyber security is the early detection of threats. The enormous volume of data that AI analyzes enables it to detect breach threats before they can be used against it. The devices used by most remote workers can be kept safe with the use of AI in cybersecurity, which is the most critical benefit. Even if threat signature changes are not made, it can still provide protection. [5]

Intrusion detection systems can compare an AI-derived model of "normal" network activity to detect anomalies that point to malicious traffic from a perimeter breach.

Endpoint security solutions can incorporate AI at the hardware level to protect devices from new attacks before encrypting their vectors as signatures in security software.

Systems using artificial intelligence for IT operations (AIOps) can gather vast amounts of data from various sources, enabling them to identify hostile actors even when their behavior is not visible in individual situations.

Advanced malware analysis tools can be built using machine learning to keep up with the more sophisticated hacks and spoofing that hackers are constantly coming up with. [6]

Benefits of using artificial intelligence in cyber security

- Technology improves over time: As AI and machine learning learn the behavior of a business network and recognize patterns in the network over time, it becomes harder for hackers to penetrate a business's network.

- Artificial intelligence detects unknown threats: a human may not be able to determine all the threats a corporation faces. Every year, hackers launch countless attacks with completely different motives. Unknown threats cause massive damage to a network. Before you find, recognize, and prevent them, the impact they have is worse.

- As attackers try new techniques, from sophisticated social engineering to malware attacks, modern solutions need to be used to prevent them. AI is established as one of the simplest technologies to map and stop unknown threats from destroying a corporation.

- Better risk management: risk management is critical to securing a company's network. As mentioned earlier, the average company deals with several threats daily. They must be found, established, and avoided to stay safe. Analyzing and assessing existing security measures through AI analysis facilitates risk management.

  AI helps you assess systems faster than cybersecurity personnel, thereby multiplying your ability to determine vulnerabilities. It detects weak spots in PC systems and business networks and helps businesses specialize in the security tasks they need. It enables risk management and the timely securing of business systems.

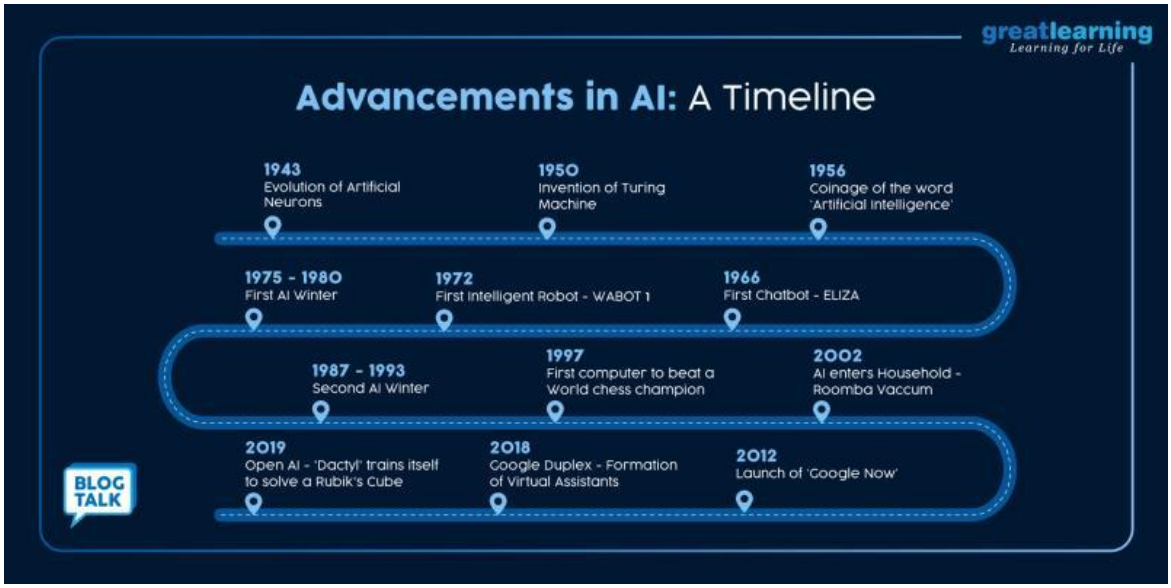
- AI and ML will handle a lot of data: the NGFW firewall scans thousands of files daily without degrading service to network users.

- Reduction of Duplicate Processes: The company deals with several threats every day. They must be found, established, and avoided to stay safe. Analyzing and assessing existing security measures through AI analysis facilitates risk management.

- Faster detection and response time: Vulnerability to AI and ML software systems within a highly firewalled and anti-malware software environment on a laptop or desktop is simple and alert to threats, limiting the need for human intervention.

- Security authentication: Most websites have a user account feature wherever one logs in to access services or purchase products. Some have contact forms that require visitors to fill in sensitive data. As a corporation, an extra layer of security is required to run such a website, which includes personal information and sensitive data. The additional layer of security can ensure that your visitors are safe while browsing your network.

  Hackers use credential stuffing and brute force attacks to gain access to company networks. Once a nursing-related offender gets into a user account, your entire network can be compromised.



- Better overall security: AI/ML protects the macro and small levels, creating it tough for malware to penetrate a business network. This frees up IT groups to wear down additional complicated threats, and up overall security posture. [7]

Impacts of Artificial Intelligence on Cyber Security

- Threat to hunting

  Traditional security methods use signatures or indicators of compromise to detect threats. This system may work well for previously detected threats; however, it is not effective for undetected threats.

  Signature-based techniques will track ninety threats. Replacing ancient techniques with AI increases detection rates up to 95 percent, however, and you can get a flurry of false positives. The simplest answer would be to mix each of the old strategies with AI. This can result in a 100% detection rate and minimize false positives. Corporate AI can be used to augment threat-hunting methods with disaggregated activity analysis. For example, you will be able to use AI models to develop profiles of individual applications within an organization's network by processing high-end information.

- Risk management

  Traditional security methods use signatures or indicators of compromise to detect threats. This system may work well for previously detected threats; however, it is not effective for undetected threats.

  Signature-based techniques will track ninety threats. Replacing ancient techniques with AI increases detection rates up to 95 percent, however, and you can get a flurry of false positives. The simplest answer would be to mix each of the old strategies with AI. This can result in a 100% detection rate and minimize false positives. Corporate AI can be used to augment threat-hunting methods with disaggregated activity analysis.

- Data centers

  AI will optimize and monitor several essential knowledge center processes, such as backup power, cooling filters, power consumption, internal temperature, and information measurement usage. Insightful powers and AI's continuous monitoring capabilities provide

insight into what values improve the effectiveness and security of hardware and infrastructure.

In addition, AI reduces hardware maintenance costs by alerting you once you are forced to fix the device. These alerts encourage you to repair your device before it breaks too badly. In 2016, Google reported a forty percent reduction in facility cooling costs and a fifteen percent reduction in energy consumption when implementing AI technology in knowledge centers.

- Network security

  The two most time-consuming parts of traditional network security are developing security policies and understanding the organization's network topography.

  Policies: Security policies define which network connections are legitimate and which you should inspect more closely for malicious activity. These rules can be used to successfully impose a zero-confidence model. Considering multiple networks, developing and maintaining policies presents the greatest challenge.

  Topography: Many businesses do not use the same naming patterns for their applications and workloads. So security teams have to spend a lot of time figuring out which workload group is associated with a particular application. [8]

  AI is deployed in cybersecurity to quickly analyze multiple incidents and establish different types of threats, from zero-day vulnerabilities used by malware to distinguishing risky behaviors that could lead to a phishing attack or the transfer of malicious code. This technology can be a self-learning system that automatically and endlessly gathers knowledge across your enterprise information systems. This knowledge is then analyzed for uncorrelated patterns among the millions to billions of signals related to the enterprise attack surface to identify new types of attacks.

However, as in all arms races, the development of offensive and defensive capabilities usually occurs simultaneously. As companies strengthen their data and sharpen detection, protection, and response skills, cybercriminals are developing their own tactics and bringing their big guns of machine learning into the fray. [9]

AI enables hackers to launch more sophisticated attacks and uses machine learning techniques to build more powerful attack models. Defenders have the same ability to check their targets.

A hacker who corrupts or manipulates the AI's data stores can trick the AI into ignoring danger, or vice versa.

Biometric authentication is vulnerable to theft and copying, a crime known in cybersecurity as "spoofing." Despite what some celebrities say, one cannot change their fingerprint, eye color, or even face.

Hugh Thompson, CTO of Symatec, described at the latest RSA conference how a hacker used deep forgery technology to impersonate the voice of a company CEO and steal millions of dollars from under the noses of employees. In a remote workplace, a hacker may need to make a short call with an authorized tone to make a significant profit.

This is only the tip of the iceberg in terms of hacking techniques. Others use automated attacks, AI-driven phishing schemes, and widespread ransomware attacks. [10]

Perhaps this is what the future of artificial intelligence in cyber security will look like.

Perhaps two giant artificial brains fighting until they lose their bank accounts represent the future of artificial intelligence in cyber security. Given the size and importance of everything, a world with both good and terrible AI is scary.

The future of our species is undoubtedly AI. Imagine all the riches we'll experience when humanity's relationship with AI grows into a symbiotic relationship like that between a bee and a flower. Until then, hold on to your hats because the robots are in the fray. [11]

A lot of the tough security demands of today's area units are satisfied by AI. AI is expanding what can be accomplished in presidential contexts that demand the best cybersecurity protections—defense and national security organizations.

Through automation, AI provides a competitive advantage. In government and Department of Defense cybersecurity positions, where AI is common, supplementing human capabilities will become easier as efficiency and potential increase.

Applying AI functions can reduce human errors. Integrating AI capabilities into manual and semi-manual processes minimizes errors and inconsistencies.

Professionals in the cybersecurity field may like new skill sets. Rather than looking for antiquated cyber skills, organizations can hire AI professionals to leverage their expertise in AI and machine learning technologies for cybersecurity. [12]

The impact of this new space may yet grow across sectors. Cybersecurity and AI-related deals have more than quadrupled over the past four years, a trend that shows AI's ability to support cybersecurity can still expand. The variability of AI use cases and their potential applicability to government The operation should be investigated by cybersecurity professionals.

3) Evolution of the topic

Constant technological evolution pushes cybersecurity to evolve at an equal pace. Every new technology gets used in the wrong hands and becomes a web security threat in some capacity. To begin with, offensive-defensive methods and schools of innovation have, as a measure of mutuality, increased in complexity in the nature of cyber-attacks and therefore in the volume of attacks. Information security is more necessary than ever, and simply modifying existing security solutions and redefining security protocols is not enough to protect your virtual assets. Instead, bolstering your information security with advanced technologies will make your security team's job easier. [13]

Over the past few years, AI has evolved into a powerful tool that allows machines to assume and act like humans. Moreover, it has caught the attention of educational institutions worldwide and is seen as the next important technological shift after the evolution of mobile and cloud platforms. Some even decide that it is the fourth technological revolution.

Artificial intelligence and machine learning technologies have proven to be huge advances across many industries, and cyber security is no different. In terms of cyber security, AI will drastically and instantly reduce response times and security prices, providing next-level precision to police breaches and making cyber security extra economical. In step with reports, more than seventy corporations believe that AI is essential to cyber security. Investments in AI should advance the application and theory of safe construction and ready AI-enabled systems. significant efforts in managing the AI-type measurement needed to produce safe training items; protecting models from probes and resistive inputs; and confirming the model's passion, individuality, and fairness. [14]

This includes safe strategies and decision-making supported by AI for the environment and the routine use of AI-human systems. Integrating AI into cyber-physical and process strategies that include validation, distribution, and collection of an artificial intelligence corpus that includes systems, datasets, and models for research will require collaborators in nursing engineering disciplines, practice, science, and education. Analytics investments in cybersecurity must deploy AI systems in critical infrastructure to help segment the persistent challenges of cybersecurity. Existing techniques include network watching for software package analysis techniques, policing anomalies to detect code vulnerabilities, and cyber logic nursing systems for synthesizing security patches at the initial warning of an attack. AI systems will perform these analyses in seconds instead of weeks or days. In theory, cyberattacks can be protected and discovered after they are published. However, there are implications on many dimensions and a desire to be safely prepared when understanding these AI actions.

AI systems need innovative cybersecurity strategies and tools to increase their resilience and reliability. AI is used by cybersecurity in an increasingly conscious way, reacts in real time, and increases its effectiveness overall. This includes adjusting and self-adapting against continuous attacks that change today's attacker-versus-defender disparities. AI will be used to classify many types of attacks, for example, in order to quickly find and know about inconsistencies on the side of informing the adaptive response at scale and using methods that help identify weaknesses in the defense, monitor mistreatment strategies, and collect lessons learned. how to repair them. Professional small teams of cyber defenders will effectively protect networks. that the same level of system protection can be extended by providing essential domain information to address AI misbehavior, design it densely, and address, for example, system degradation behavior and quality-of-service limitations.

While security experts believe AI is the way forward for businesses, it will come with seemingly intractable problems. While maximum computing adds a layer of security to your organization, cybercriminals can constantly use technology to their advantage. [15]

With AI, we efficiently analyze user behavior, deduce a pattern, and determine any irregularities in the network. This level of data makes it easier to quickly identify cyber risks. Conversely, entities that are currently excited about human intelligence may later become vulnerable to malicious cyber programs that mimic legitimate AI-based algorithms. Many organizations rush to sell AI and ML-based security solutions, completely ignoring the fact that these algorithms create a false sense of security.

"Supervised learning" is another concept that is not entirely safe. Under this, security algorithms label information sets (malware, safe or clean information, redundancies, etc.) according to their results and consider the information in those sets as results. Cybercriminals will modify these tags if they gain access to them. Also, routine tasks that depend on AI are handled by advanced hacking campaigns through the deployment of machine learning. Although AI poses a security threat to companies, AI automation can transform organizations' ability to detect and remediate remedial incidents. It can also handle corporate executive threats and device management in some cases. [16]

4) Future development in the area

Today, businesses specialize in the security of their systems. They know the huge impact of every small and large scale cyberattack. To secure their organizations, organizations use different types of security. This multi-layered security device usually starts with a generally acceptable firewall capable of controlling and filtering incoming network traffic. After this layer, the second line of defense consists of an anti-virus encryption system. These antivirus applications scan through the system to look for and find suspicious codes and malicious files. Due to their protection against cyber-attack, businesses often acquire data backups as part of a disaster recovery policy.

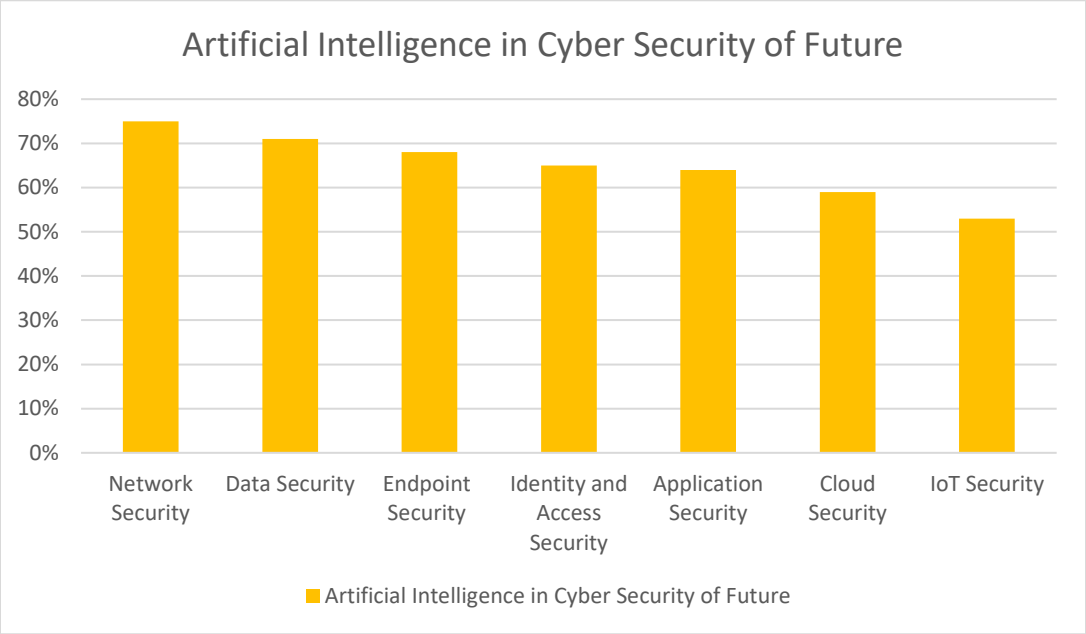
Artificial intelligence is dynamic in the landscape of various industries, and cyber security is no exception. Apart from incident response, malware detection, and more, AI is used to improve various aspects of cyber security. Throughout this blog post, we discuss how AI is dynamic within the cybersecurity sector and what the long term holds for this exciting technology! [17]

AI in cyber security can look like the nursing assistant at the beginning of a speech. However, it is a long-term wave that can be changed, but it thinks that you are connected to the world forever.

There is little question that AI has a promising future in cyber security. Here are a few reasons why:

- Identify threats further quickly and accurately than humans can.
- Prevent attacks by automatically obstructing suspicious activity.
- Improve the resilience of networks against attack.
- Speed up the strategy of recovery from a cyber-attack.
- Improve the protection of digital systems. [18]

AI is already starting to play a role in cyber security. Its role will be even more important in the future. Organizations that want to stay ahead of the curve should be forced to start financing AI-based security solutions right now.



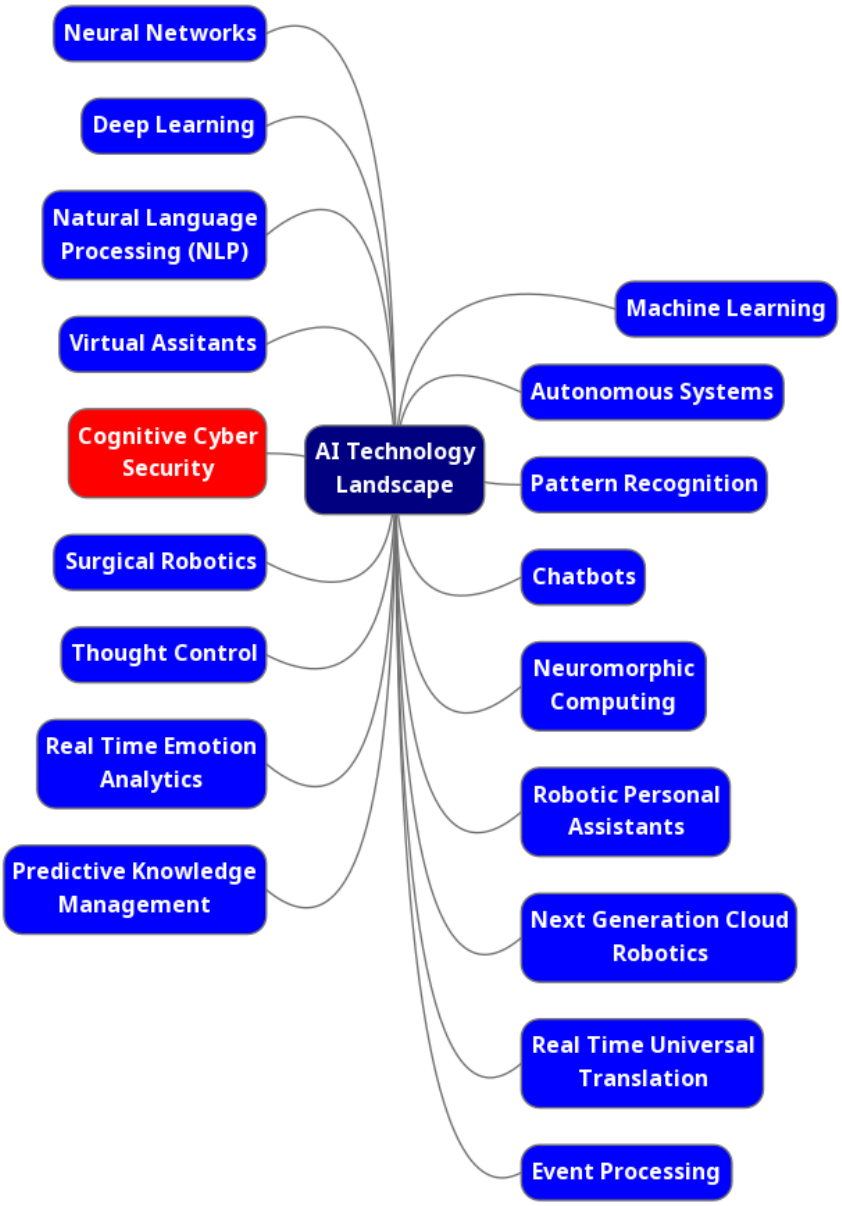
By the way, AI is going to play a big role in cyber security in the future. The amount of additional information generated, and the ever-growing variety of cyber threats reflect the increasing importance of cybersecurity. Thanks to this, it is gradually becoming more annoying for people to stay awake.

Today, human analysts perform several tasks themselves. With the help of computing, the method is done mechanically and completed without much delay. It includes characteristic patterns of knowledge and malware detection. AI can even facilitate higher defenses against cyber-attacks by anticipating them and responding faster than humans. [19]

Businesses are under constant threat from cyber-attacks, so the stakes are high. A triple-crown attack can result in the loss of sensitive information, financial loss, and reputational damage.

AI-powered tools facilitate protection against characteristic and intrusive threats before they harm businesses.

They can provide additional facilities for businesses to respond to attacks quickly and effectively. By leveraging AI, businesses stay one step ahead of cybercriminals and keep their information safe. [20]



5) Conclusion

In history, technology has evolved to some extent. Machine learning and computing are advancing far too quickly relative to society's flexibility to grasp and understand them. Computer systems that use machine learning and computing simultaneously are becoming increasingly important and pervasive. This analysis paper reflects data collected from various engineering and scientific experts, suggesting that the future of AI depends on the ability of the United States to balance the challenges and frontiers of AI, mainly in the cyber security space. It should be noted that the discussion is described above in more than one time frame. With rapid technological advances, new application domains, and cyber security, the interaction between AI and ML may introduce new challenges and opportunities. National and international thinking related to these issues is predicted to change over time, and these insights and inquiries will force review and periodic updating. The country's focus has long been on creating high efforts in sterilization computing, as its technology has advanced since the previous years. Artificial intelligence is helping to support various industries from time to time. Investments in AI should advance the practice and theory of safe construction and AI-enabled systems. Producing safe training requires significant effort in managing AI, protecting models from probes and resistive inputs, and affirming the passion, individuality, and fairness of the model. Through technology, AI will assist in capturing and processing the vast amount of information that is happening in the current era of technology systems. Unlike various effective applications of AI, AI is expected to be used by both defenders and attackers in cyber security scenarios.

6) References

[1] S. &. N. S. Abraham, "A predictive framework for cybersecurity analytics using," *arXiv preprint arXiv:1502.01240.,* 2015.

[2] O. Barden, "New approaches for new media: Moving towards a connected methodology. Qualitative Research Journal, 13," pp. 6-24, 2013.

[3] B. Bland, "China's robot revolution. Financial Times," p. 6, 2016.

[4] N. Bostrom, " Superintelligence: Paths, Dangers, Strategies, Reprinted.," 2016.

[5] A. P. Buckley, "Using sequential mixed methods in enterprise policy evaluation: A pragmatic design choice?: EJBRM EJBRM. Electronic Journal of Business Research Methods," pp. 13(1), 16-26., 2015.

[6] S. &. Z. M. Farajpour, "DEFINING THE PLACE OF EXPERT SYSTEMS IN THE OPERATION OF ORGANIZATIONS.," *Kuwait Chapter of the Arabian Journal of Business and Management Review,* pp. 122-134, 2013.

[7] X. Huang, "Technology, service, and collaboration in retail supply chains: Three essays," *The University of Minnesota.,* 2004.

[8] B. W. Jackson, "Artificial Intelligence and The Fog Of Innovation: A Deep-Dive On Governance And The Liability Of Autonomous SYSTEMS.," *Santa Clara High Technology Law Journal,* p. 35, 2019.

[9] H. S. M. S. K. S. Y. A.-R. R. &. I. I. Kolivand, " Photorealistic rendering: A survey on evaluation," *Multimedia Tools and Applications,* 2018.

[10] S. Makridakis, "High tech advances in artificial intelligence (AI) and intelligence augmentation (IA) and Cyprus," *The Cyprus Review,* 2018.

[11] B. Shneiderman, "Human-centered artificial intelligence: Reliable, safe & trustworthy," *International Journal of Human-Computer Interaction,* 2020.

[12] J. Thornhill, " AI: Thinking machines: Stories," *Financial Times ,* 2016.

[13] F. &. F. K. Wortmann, "Internet of things," *Business & Information Systems Engineering,* 2015.

[14] A. D. P. &. M. S. Leylavi Shoushtari, " A review of the evolvement trend of robotic interaction control," *The Industrial Robot,* 2016.

[15] S. A. Oke, "A literature review of artificial intelligence," *International journal of information and management sciences,* 2008.

[16] W. M. Schuster, "Artificial intelligence and patent ownership.," *Washington and Lee Law Review,* 2018.

[17] A. U. A. Shidawa Baba Atiku, "Survey on The Applications of Artificial Intelligence in Cyber Security, ITU, and WCIT," *International Conference on Cyber Conflict: Architectures in Cyberspace,* 2019.

[18] A. S. L. R. a. Y. E. E. Menahem, "Improving malware detection by applying multi-inducer ensemble," *Comput. Statist. Data Analysis,* 2013.

[19] J. P. M. M. T. B. L. S. P. H. J. &. S. N. Drmola, "Perspectives on Cybersecurity," *MASARYKOVA UNIVERZITA,* 2015.

[20] M. H. Jarrahi, "Artificial intelligence and the future of work: human-AI symbiosis in organizational decision making," *Business Horizons,* 2018.