ACICE
ADMM Cybersecurity and
Information Centre of Excellence

UPDATE ON
THE CYBER DOMAIN

Issue 06/23 (June)

How Artificial Intelligence can be used to enhance Cybersecurity Operations

OVERVIEW

AI technology has many uses and is now increasingly employed worldwide in multiple industries such as e-commerce, education, healthcare, robotics, transportation, gaming and cybersecurity. One important use of AI technology in cybersecurity is to provide new and innovative solutions to identify and mitigate potential cyber threats. According to Blackberry's recent research, "the majority (82%) of IT decision-makers plan to invest in AI-driven cybersecurity in the next two years and almost half (48%) plan to invest before the end of 2023."

"What AI enables us to do is to respond in an intelligent way, understanding the relevance and consequences of a breach or a change of behaviour, and in real time develop a proportionate response." – Poppy Gustafsson, co-CEO of Darktrace.

DEFINITION OF AI

AI is a field of computer science that focuses on using machines or systems to perform tasks that typically require human intelligence. AI encompasses various techniques and approaches, which include complex algorithms, statistical models, language processing, and computational power, that enable machines to understand, learn from, and make decisions or predictions based on data. AI algorithms and models are built upon various techniques, including machine learning (ML), machine vision, deep learning, natural language processing (NLP), and robotics. These technologies enable AI systems to process vast amounts of data, identify patterns, make decisions, and continually improve their performance through iterative learning process.

HOW AI IS CHANGING THE CYBER THREAT LANDSCAPE

As the barriers to AI technology lowers, it has become easier for cybercriminals and adversaries to exploit this new technology. In recent years, there has been an increase in malicious actors utilising AI to launch sophisticated cyberattacks. AI-assisted cybersecurity threats such as: (a) generative AI-assisted malware; (b) deepfake AI; (c) phishing; and (d) distributed denial of service (DDoS) attack, have raised concerns amongst organisations around the world.

Generative AI-assisted Malware

Generative AI uses neural networks to identify patterns and structures in existing data to generate new and original content. Threat actors can use generative AI to develop highly effective malware that can continuously evolve and evade cybersecurity measures. Researchers from HYAS Labs have shown proof of concept (PoC) that polymorphic malware can bypass a leading-industry cybersecurity system without the system flagging any alerts or detections.

Deepfake AI

Deepfake AI technology is used to digitally alter existing images, audio and video to create bogus content. Attackers could automate and scale their malicious activities such as generating AI-powered deepfakes to achieve their own interests and agenda. For instance, on 16 Mar 2023, a group of hackers intercepted one of the Ukrainian live broadcasts with AI-fabricated content, showing Ukraine's President Volodymyr Zelenskyy commanding his soldiers to surrender to the Russians.

Phishing

Traditionally, recipients may be able to identify phishing emails as the contents could contain poor grammar, spelling mistakes and suspicious information. However, with the advances in AI, cybercriminals can now use AI tools such as ChatGPT to create highly convincing phishing emails that do not have these obvious key indicators. Increasingly, more individuals are tricked by these phishing emails and lured into clicking malicious links or downloading malware.

DDoS Attacks

Attackers can use AI to collect as much information on the victims' systems to understand the vulnerabilities in the networks. Thereafter, attackers can amplify the scale and impact of the DDoS attacks against Internet and Cloud platforms to disable security measures or cause damage to the victims' systems.

***"AI cyberattacks can be used not just to shut down infrastructure but also to exploit information"* – Alberto Domingo, technical director of cyberspace at NATO Allied Command Transformation.**

HOW AI CAN HELP IN CYBERSECURITY OPERATIONS

Despite the threats posed by the use of AI, AI-assisted tools can bring significant advantages in enhancing cybersecurity. This is because AI-tools are more efficient in processing and analysing massive amounts of data, effectively saving time particularly on processes that are manual in nature. Here are some examples on how AI can help in cybersecurity operations:

Using Generative AI to Identify Vulnerabilities

Generative AI can create predictive models to identify potential vulnerabilities based on historical and present data. Mitigating measures can then be put in place to prevent cyberattacks. The predictive capabilities of generative AI can also detect anomalous activity that could signify a cyberattack using zero-day vulnerabilities. A zero-day vulnerability is an undiscovered flaw in an application or operating system for which there is no mitigation nor patch for it because the software maker does not know it exists. This allows for effective countermeasures to be put in place to mitigate the risks.

***"Generative AI is a complete game-changer. Everyone knows this is the next powerful thing."* – Margrethe Vestage, European Union tech chief.**

Creating AI Simulated Environments to Test and Evaluate Systems

AI can simulate environments by re-creating realistic scenarios that can stress-test and evaluate security systems and responses. For example, generative AI can create learning materials on phishing emails or other attacks that train employees to recognise and avoid similar attacks. Generative AI can also automate stress testing on the cybersecurity systems to reveal potential flaws, and thereby strengthening and hardening the defences. All these measures can help identify cybersecurity risks and improve overall cybersecurity defences.

Using AI in Cyber Threat Intelligence

Threat intelligence is defined as data that is collected, processed and analysed to understand a threat actor's motives, targets and attack behaviours. Generative AI is capable of analysing large volumes of data to identify patterns and indicators of compromise that can be used to identify cybersecurity risks and respond to them quickly. Threat intelligence will allow organisations to make better, data-backed decisions to combat against threat actors.

CONCLUSION

AI technology has been proven to be a useful tool that can strengthen cybersecurity defences. However, there are practical limitations to implementing AI in cybersecurity. The cost of designing, building and maintaining AI-enabled cybersecurity systems may be prohibitive as AI in cybersecurity is a relatively new concept. Besides, the use of AI in cybersecurity may only be available to large organisations given the requirement for large data sets for machine learning (ML).

Separately, malicious actors will continue to use AI for illicit purposes, while cybercriminals will always keep up with the trends in cybersecurity and look for ways to exploit any vulnerabilities. Ultimately, organisations need to always stay vigilant to navigate the rapidly evolving cyber threat landscape.

***"The potential benefits of artificial intelligence are huge, so are the dangers."* – Dave Waters.**

Contact Details

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE, at ACICE@defence.gov.sg.

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

• • • •

ANNEX A

News Articles

1. Cybersecurity Best Practices & Measures to Prevent Cyber Attacks in 2023
   [Link: https://www.ekransystem.com/en/blog/best-cyber-security-practices]

2. Cybersecurity Best Practices for Smart Cities | CISA
   [Link: https://www.cisa.gov/resources-tools/resources/ cybersecurity-best-practices-smart-cities]

3. Top 10 cybersecurity best practices to Prevent Cyber Attacks in 2023
   [Link: https://www.analyticsinsight.net/top-10-cybersecurity-practices-to-prevent-cyber-attacks-in-2023/]

4. Securing The Future: The Most Critical Cybersecurity Trends Of 2023
   [Link: https://www.forbes.com/sites/forbestechcouncil/2023/02/ 28/securing-the-future-the-most-critical-cybersecurity-trends-of-2023/]