CAPITOL Technology University

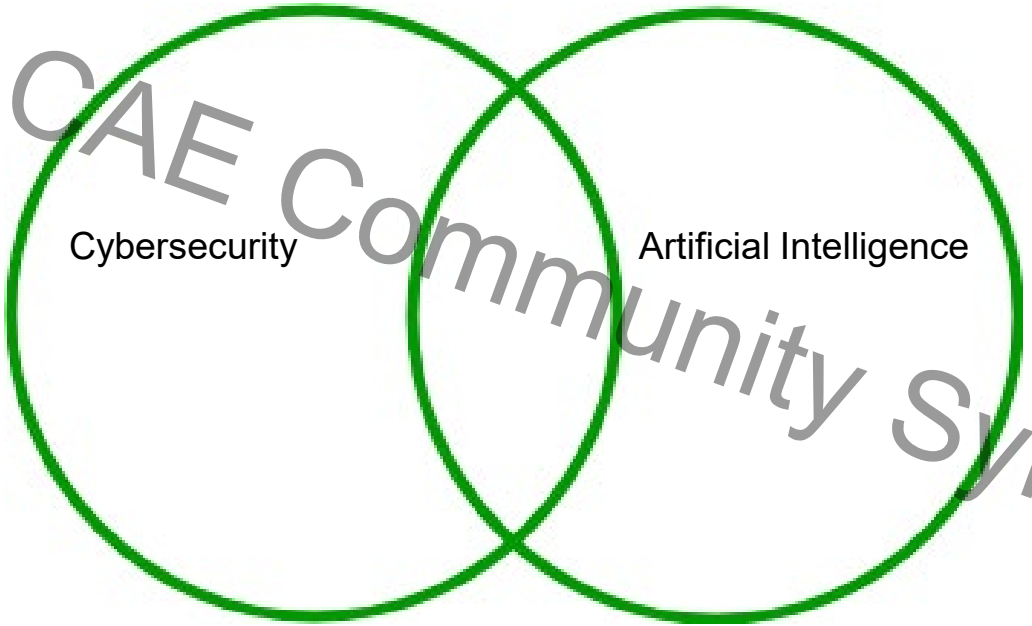
CAE IN CYBERSECURITY COMMUNITY

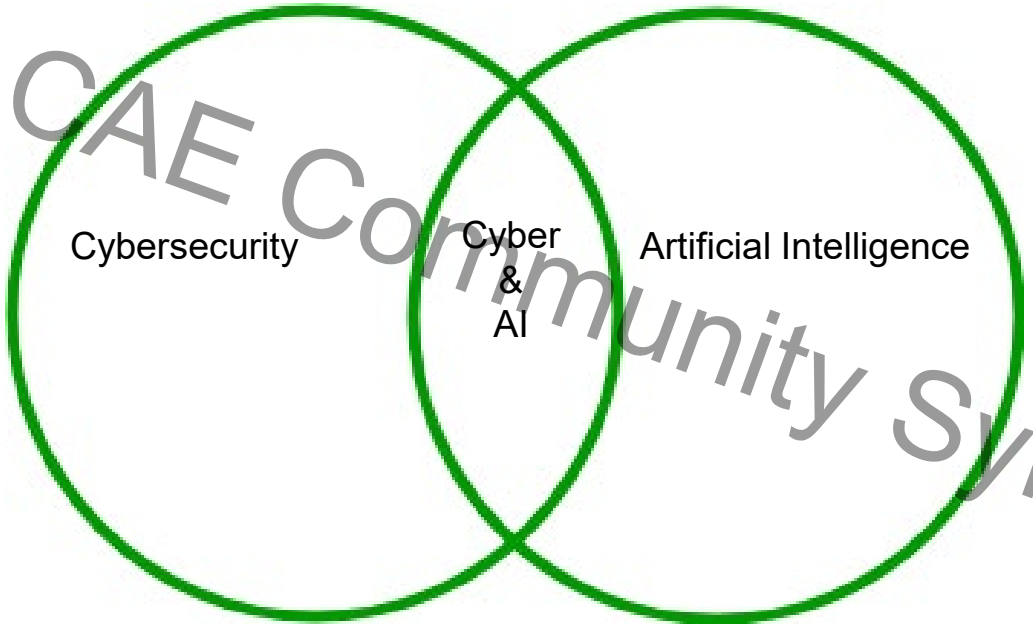
2024 CAE Community Symposium

Exploring the Intersection of Cybersecurity and Artificial Intelligence

Dr. Kellep A. Charles, CISSP
Cybersecurity Chair
Capitol Technology University

2024 CAE Community Symposium





AI

- The Concept is not new
  - Alan Turning and the Turing Test – 1950
  - 1956, at the Dartmouth Conference, that the term "Artificial Intelligence" was first coined by John McCarthy (often regarded as the birth of AI.)
  - the first AI laboratory at MIT in 1959

- So, why has it suddenly surged in prominence today?
  - the exponential growth in computational power
  - the abundance of available data (147 zettabytes daily)
  - The continuous refinement in algorithms

AI

AI is divided into three different evolutionary stages, or there are three stages:

- Artificial narrow intelligence (Weak AI) – Current State
  - no genuine intelligence or there is no self awareness
- Artificial general intelligence (Strong AI)
  - Involves machines that posses the ability to perform any intelligent task that a human being can.
- Artificial super intelligence - ~2040
  - Capabilities of a computer will surpass that of a human being - hypothetical situation

AI-Based Cybersecurity

- $15 billion dollars currently
- Projected to surge to $135 billion in 2030
- To address this challenge, we need to employ force multipliers to enhance our effectiveness.
- Two key strategies for implementing force multipliers are:
    - leveraging automation for increased efficiency
    - Incorporating AI to work more intelligently.

So, how exactly does AI benefit cybersecurity?

- **Enhanced Threat Detection** - AI-driven systems can detect actual cyberattacks more accurately than humans, minimizing false positives and prioritizing responses based on real-world risks. This enables faster and more effective threat mitigation.
- **Phishing Detection** - AI is proficient at identifying and flagging suspicious emails and messages, a common weapon in the cybercriminal arsenal. It helps to thwart phishing campaigns and safeguard sensitive data.
- **Social Engineering Simulation** - AI can simulate social engineering attacks, enabling security teams to identify potential vulnerabilities before cybercriminals can exploit them. This proactive approach is crucial in staying one step ahead of malicious actors.
- **Rapid Incident Analysis** - AI's ability to analyze vast amounts of incident-related data quickly empowers security teams to take swift actions to contain threats, reducing the potential impact of cyberattacks.
- **Access Control Strengthening** -Machine learning algorithms can flag suspicious login attempts and improve password management, enhancing security.

Dark Side of AI in Cyber

- **Social Engineering Schemes** - AI enables cybercriminals to automate processes and create more personalized and convincing messages, leading to a higher success rate in social engineering attacks.
- **Password Hacking** - Enhanced AI algorithms are being used to decipher passwords more quickly and accurately, making password hacking more efficient and profitable.
- **Deepfakes** - AI's manipulation of audio and visual content enables the creation of convincing deepfake content for fraudulent purposes.
- **Data Poisoning** - Hackers can manipulate AI algorithms by poisoning training data, influencing their decisions and leading to potentially severe consequences.

Conclusion

The intersection of cybersecurity and AI is a dynamic and evolving landscape.

It is incumbent upon us, as cybersecurity leaders, educators and professionals, to embrace AI's potential, understand its risks, and continue adapting to ensure a secure and resilient digital world.