Artificial Intelligence and Impacts on Cyber Security T&E

Presenter
Donald Lane

35th International Test and Evaluation Symposium Global T&E Environment in 2025 and Beyond

KBRwyle

Introduction

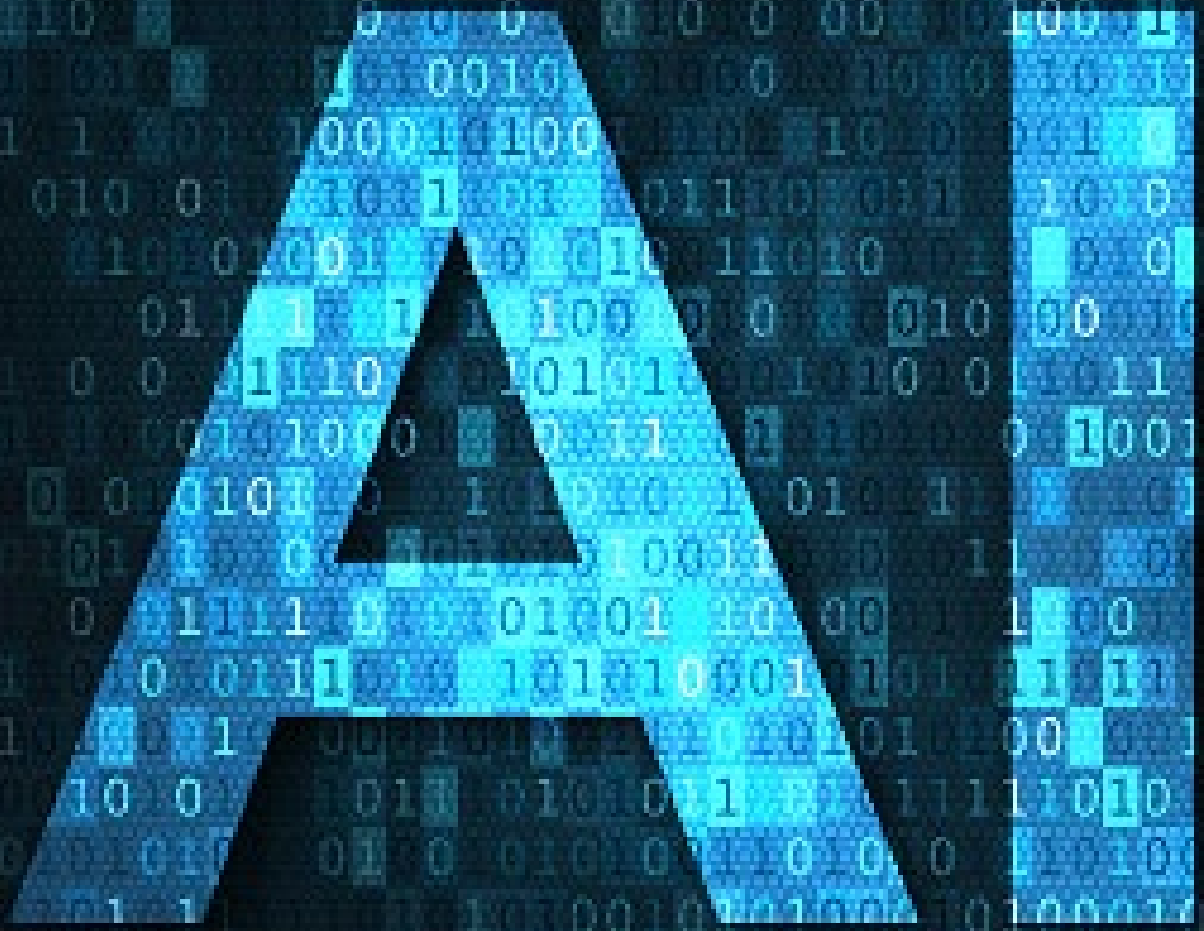
The stage is set. We are in an age of awe and wonder with disruptive technologies that include Artificial Intelligence, Cloud Computing, Quantum Computing.

Where and how does all this technology fit together in T&E, including Cyber Security?

A great question! Lets expand upon relevant disruptive technologies and their future potential impact on the Test and Evaluation community.

“When thinking of A.I. and how it impacts Test and Evaluation don’t think Inside or Outside of the Box. Try thinking that there is no Box!”

Artificial Intelligence (A.I.)



Future development within a Test and Evaluation environment for software will be hosted in the cloud. This allows unlimited access to Cloud CPU resources enabling machine learning of A.I. algorithms. Once A.I. is utilized through an application programming interface (API), it will enable Cyber Security staff to work with the A.I. improving the efficiency to detect errors within software code and potential vulnerabilities.

Artificial Intelligence (A.I.)

- Academia and software company's are researching ways to implement A.I. as a tool to automate Test and Evaluation processes normally done through proprietary tools or developers.
- One example of automation currently used today is taking raw test data results and utilizing A.I. to assist the test engineer in analyzing results in less time and ensuring Quality Assurance of the test results. This teaming of A.I. working with the human factor allows them to accomplish something must faster than they could do alone separately.

Artificial Intelligence (A.I.)

- Cyber Security Testing will be impacted once a common A.I. framework and industry standard is adopted within the Commercial and Department of Defense (DoD) industry.
- This presents new challenges to the Test and Evaluation community. As data hosting requirements change, methodologies for testing vulnerabilities and software will have to be introduced as well, working with A.I. solutions.

Cloud Computing

- Classic computing technology (software and hardware) is but the first layer in the foundation for Artificial Intelligence. With current classic computing it will not be long before the Cloud CPU platform will be leveraged as an environment that will allow the machine learning environment of A.I. and autonomous application development.

Cloud Computing

- Cloud Computing presents a unique opportunity to implement A.I. solutions or software tools for the T&E environment. This includes the following benefits:
  - Low cost maintenance and transfer of risk to the Cloud host or provider
  - Cloud infrastructure allows scaling and performance increases to analyze test results much faster
- Cloud vendors are now offering hosting for A.I. solutions and machine learning within Cloud Environments.
- Customers are now subscribing to Cloud CPU services that will allow them to leverage Cloud CPU resources for machine learning capabilities of A.I. solutions.

Cloud Computing

- Impact to the T&E community will be trying to integrate these new Cloud capabilities and CPU services within their processes and training staff how to use them.
- With the great advantages it promises, it also introduces new risks and engineering complexities associated with introducing new functionality and algorithmic data that will need protection.

Quantum Computing

Testing and Evaluation of software will also be enhanced by Quantum algorithms combined with A.I. solutions that will be able to automate a large portion of the tedious test data aggregation, and perform data analysis at an unparalleled scale.

Quantum Computing

- Quantum Computing is being researched around the world by countries, agencies, military, academia, and commercial companies due to the potential unlimited CPU capability it may provide.
- Current Quantum Computers have been utilized already and proven effective by two of the computer industry giants for Fuzz testing of software code and analysis utilizing a Quantum Computer and Neural Artificial Intelligence algorithms.
- As Quantum Computing technology matures, it will enable A.I. algorithms to machine learn in a parallel state versus classic computing methods.

Quantum Computing

- Impact to the T&E community will be the availability to process large amounts of test data and analyze it on a scale unheard of before.
- Complexity of preparing test data for Quantum Analysis will remain the hardest challenge for Data Scientists, and Test Engineers.
- Impact to Cyber Security T&E will include all the above, but the most profound impact will be the ability for A.I. to take an evolutionary leap forward, providing assistance in identifying cyber adversaries and attack patterns, and analyzing potential vulnerabilities.

Quantum Cloud Computing (QCC)

- Specific Cloud vendors are now offering QCC services for customer access to their Neural networks and Quantum Computer that will enable machine learning of A.I. algorithms as part of their Cloud Computing platform.
- Depending on the customer's Cloud provider and T&E environment, this could pave the way for standardization of an A.I. Test and Evaluation framework that utilizes Quantum Computers or Simulation. This will allow customers to easily prepare for T&E events and easier integration within an organization.

Cyber Range Testing

A.I. will automate Cyber Range testing and allow faster response times for the customer and data analysis of cyber threats utilizing A.I. tools and algorithms.

Cyber Range Testing

- Artificial Intelligence will play a major role within the Cyber Range environment during adversarial testing. A.I. is already being utilized for intrusion detection using automated tools for real-time analysis.
- A.I. will impact T&E processes that utilize software tools such as vulnerability detection methods, automated internal code tools, application penetration, fuzz/robustness testing, and database scanning tools.

Conclusion:

Where and how does all this technology fit together in T&E, including Cyber Security?

Conclusion:

- The future Cyber Security T&E environment can be implemented today and could include a Cyber Range hosted within a Cloud environment.
- This allows easy integration of tools and services that would include hosting the A.I. algorithms, customer test data, and machine learning (Bot) within the same cloud environment.
- This would provide signification scaling and performance increases utilizing the Cloud CPU resources and access to Quantum Computer Cloud services.
- Benefits can be applied when analyzing test results and improving the performance of A.I. solutions that will be working with the Test Engineers, Data Scientists, and Cyber Security Analyst's.

Questions?