Dr. James B. Fraley

ChatGPT Cyber Attacks

Using Artificial Intelligence and Machine Learning Teaming can provide better insight and extend protections for enterprises today. AI/ML for cybersecurity can be valuable in various ways. Unfortunately, the adversaries also know that and use AI/ML tools to test security and protections – the bad. Lastly, the US and other countries are waking up the reality of how powerful AI/ML can be and lawmakers are trying to figure out how to regulate and control the exploding uses for AI/ML (the ugly). Governments around the world are increasingly recognizing the need to regulate artificial intelligence (AI) to ensure its ethical and responsible use while fostering innovation. Regulations can vary significantly from one country to another, but here are some common approaches and regulatory measures that governments are using to regulate AI.

This session will cover various topics that illustrate the Good, Bad and the Ugly.

Ultimately, while AI/ML can be used for good and bad purposes, it can also be a valuable tool for enhancing cybersecurity defenses. Balancing the benefits of AI with the need for robust security measures is crucial in the modern digital landscape. AI/ML in conjunction with other cybersecurity tools and practices can enhance an organization's overall security posture by providing intelligent insights and automating routine tasks. However, it should complement, rather than replace, the expertise of cybersecurity professionals. Lastly, specifics of AI regulation can vary widely from one jurisdiction to another, and the regulatory landscape is still evolving rapidly. Organizations developing and deploying AI systems should closely monitor and comply with relevant regulations in their respective regions and sectors.

Additionally, the organizations should engage with regulatory bodies and industry associations to help shape responsible AI/ML practices and regulations.

Biography

Dr. Fraley was recently promoted at the Director for Cyber Security Education for the College of Technology. He has been teaching at Wilmington University since 2015. Prior to joining Wilmington University, he served as the Senior Director McAfee's Cybersecurity Consulting Practice and also held the position as the Senior Cyber Threat Intelligence Strategist. Dr. Fraley has led the design of complex cyber security operational architectures and advanced threat intelligence solutions for industry and governments worldwide. In that capacity, Dr. Fraley engaged various customers and senior leadership throughout the Fortune 2000 and Governments to propose and implement better cybersecurity detection and prevention of cyber-attacks.

Dr. Fraley has been asked by the Government to present technical issues such as Enterprise Security, Machine Learning for Malware Detection, and Big Data for cyber situational awareness and predictive cyber security defensive measures. Dr. Fraley has several papers published by Institute of Electrical and Electronics Engineers (IEEE). His dissertation and advanced research focuses on leveraging machine learning (specifically cluster algorithms and deep learning) detection of Advanced Persistent Threats (APT) and Polymorphic/Metamorphic malware.

Dr. Fraley has guest lectured at Columbia University, Georgia Institute of Technology, University of Maryland, University of Delaware and George Mason University. Dr. Fraley is also an Assistant Professor at Wilmington University – teaching Information Assurance and Cyber Security.