Can AI and Big Data Methods Really Help in Cyber Security?

The terminology of "Big Data" has been used in many areas. The Cyber Security problem is a great example of a Big Data problem. The amount of data that is necessary to find malicious actors within mixed corporate environments continues to expand. Finding the "dumb" or "lazy" attackers that use known attack vectors is fairly straight forward. But how do you find the more advanced technically savvy bad guys? AI is starting to play a bigger role in detection methods within cyber solutions. But how do you mix the two? It is exceeding hard to accomplish AI over truly large ever changing data sets. Training AI to find something it is seen before is a more traditional approach. However, in the cyber problem you are looking for an attacker using a new approach you don't have in your data to get around controls. In this talk we will discuss the Cyber Security detection problem and the issues around speed and size of the data combined with the ever changing attack vectors.