

We're in a cyber cold war but data science brings new hope

Submitted by: BlueSky Education

Wednesday, 9 December 2020

Cyber threats are constantly evolving, meaning attackers are always one step ahead. However new research from Nyenrode Business University brings hope to the fight against online crime.

The research, conducted by PhD candidate Scott Mongeau, reveals that cybersecurity data science can fight cyber threats, but that we can only utilize the benefits of these methods with investment.

“My research observes that hostile countries and criminal networks are already utilizing machine learning to stage attacks. We will need to apply these same methods to defend. Detecting and counteracting threats through analytics and machine learning requires focused research.”

“To realize effective data-driven defence, organizations must invest in the orchestration of people, processes, and technology. This trinity cannot be treated in isolation. If we wish to arm ourselves against the risks of increasingly sophisticated cyberthreats, we must accept and commit the costs involved.” Says Mongeau

Mongeau's advice is to start by examining where data-driven cyber defence already works well. He explains that a simple example is filtering for phishing emails. Popular email platforms already use machine learning to detect and filter-out dangerous emails from your inbox. The same methods can be used to identify suspicious network traffic and device behaviour.

The research emphasizes the urgency of embracing data-driven security. While data science is a popular topic, best practices for realizing the benefits are lagging. The field of cybersecurity data science has emerged in the last three years. However, the methods are already being adopted by adversaries. We are already seeing the effects, for instance, in the automation of fake news and misinformation campaigns. The researcher believes that we can expect to see increasingly sophisticated attacks utilizing machine learning and AI in the coming years.

According to Mongeau “cyber risks will evolve and expand. The risks relate not only to digital infrastructure, but physical infrastructure, health, and safety. Consider, for example, water management, healthcare, and traffic control. As the digital world increasingly manages the physical world, we must be increasingly cautious concerning digital defence. By investing in research and development for cybersecurity data science we can defend national interests and improve preventative measures.”

The research is particularly important for policy makers as it reveals that structured planning is required in order to provide the best data-driven defence.

The research is published in: "Cybersecurity Data Science: Best Practices in an Emerging Profession".

ENDS/

For more information, a copy of the research paper, or to speak with the researchers, contact Kate Mowbray at BlueSky PR on Kate@bluesky-pr.com or call +44 710022871