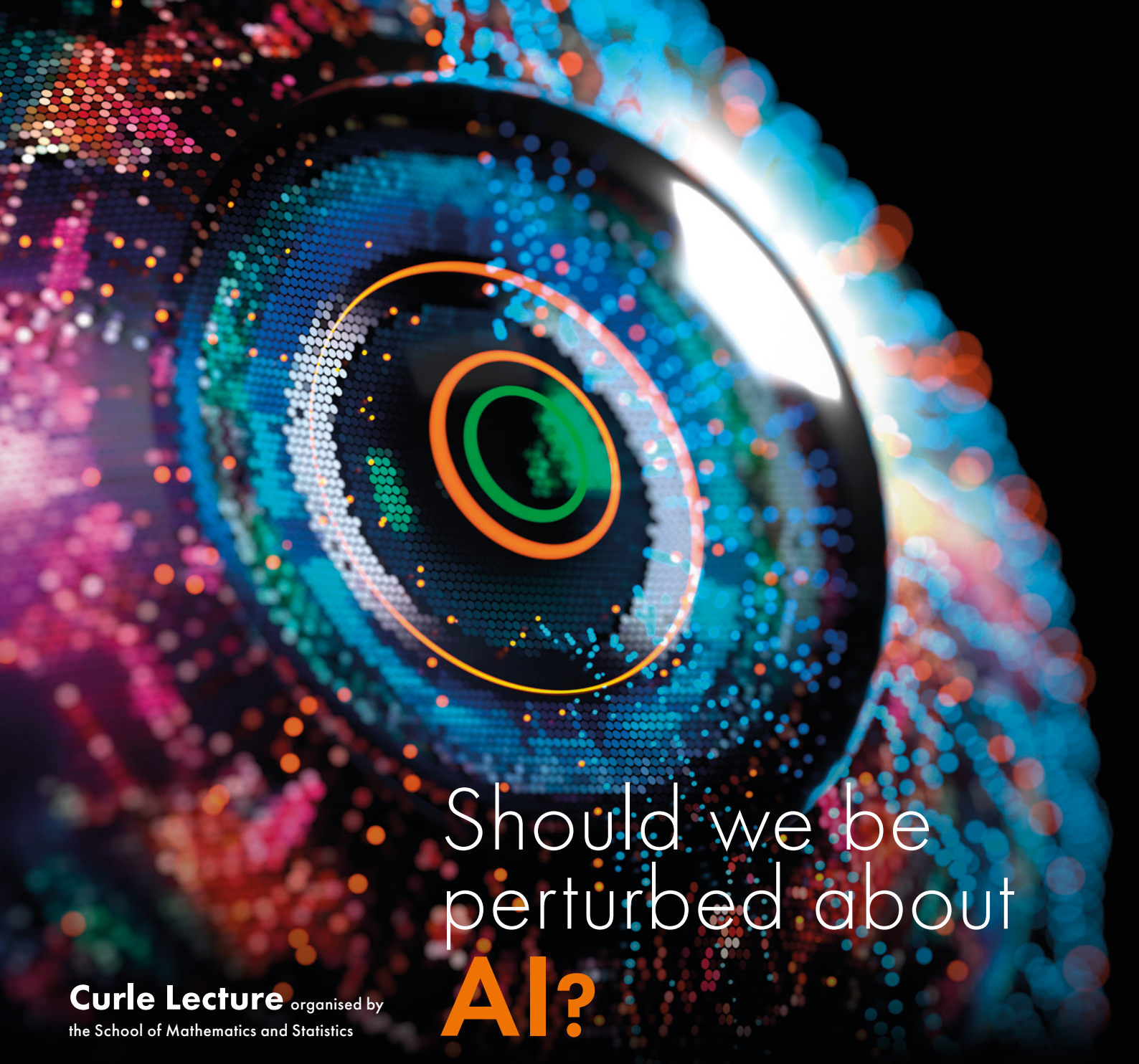

Should we be perturbed about AI?

Curle Lecture organised by the School of Mathematics and Statistics

Speaker:

Professor Des Higham
University of Edinburgh

Monday 2 October, 2023
17.15

Physics Lecture Theatre A,
University of St Andrews

No cost for entry

A traffic "Stop" sign on the roadside can be misinterpreted by a driverless vehicle as a speed limit sign when minimal graffiti is added. Wearing a pair of adversarial spectacles can fool facial recognition software into thinking that we are Brad Pitt. The vulnerability of artificial intelligence (AI) systems to such adversarial perturbations raises questions around security and ethics, and many governments are now considering proposals for their regulation. Mathematics is at the heart of this landscape. It fuels the conflict escalation issue, where new defence strategies are needed to counter an increasingly sophisticated range of attacks. Perhaps more importantly, mathematics allows us to address big picture questions, such as: What is the trade-off between robustness and accuracy? Can any AI system be fooled? Do proposed regulations make sense? Focusing on deep learning algorithms, I will describe in simple terms how mathematical concepts can help us to understand and, where possible, ameliorate current limitations in AI technology.

University of St Andrews | FOUNDED 1413

The University of St Andrews is a charity registered in Scotland, No: SC013532