AI-Enabled Influence Operations:
The Threat to the UK General Election

The Alan Turing Institute

Centre for Emerging Technology and Security

12+ MONTHS BEFORE ELECTION | ONE MONTH BEFORE | 72 HOURS BEFORE | POLLING PERIOD | ONE TO 12+MONTHS POST-ELECTION

AI THREAT TIMELINE
THREAT MOTIVATIONS

= AI ELECTION THREATS

= RECOMMENDATION

01 DISTRUST

Undermining the reputation of targeted political candidates, or shaping voter attitudes on specific campaign issues.

02 DISRUPT

Polluting and congesting the information space, to confuse voters over specific elements of the election campaign or voting process.

03 DISCREDIT

Erode confidence in the integrity of the election outcome, for instance via allegations of electoral fraud.

This also undermines longer-term public trust in democratic processes.

AI BOT ACCOUNTS CIRCULATING VOTER FRAUD CLAIMS

VOTER TARGETING EFFORTS

CANDIDATES BEING DECLARED VICTORIOUS BEFORE OFFICIAL RESULTS

DECEPTIVE POLITICAL ADS

DEEPFAKE ACCUSATIONS AGAINST POLITICAL CANDIDATES

DEEPFAKES OF CANDIDATES WITHDRAWING FROM ELECTIONS OR ATTEMPTING TO RIG BALLOTS

POLLING DISINFORMATION

AI-GENERATED FAKE NEWS SOURCES

R1, R2, R3, R4, R6, R8

R5, R7

01 INFORM

Setting out clear expectations for political parties and the media on AI, as well as informing voters of AI threats.

02 INTERCEPT

Prior evidence gathering and simulation of threat scenarios enhance mitigation strategies to deal with incidents.

03 INSULATE

Reinforcing red lines and expectations around AI incidents and usage to protect against efforts to undermine electoral integrity.

Sam Stockwell, Megan Hughes, Phil Swatton and Katie Bishop, "AI-Enabled Influence Operations: The Threat to the UK General Election," *CETaS Briefing Papers* (May 2024).

cetas.turing.ac.uk

PROTECTION MOTIVATIONS
COUNTERMEASURES TIMELINE