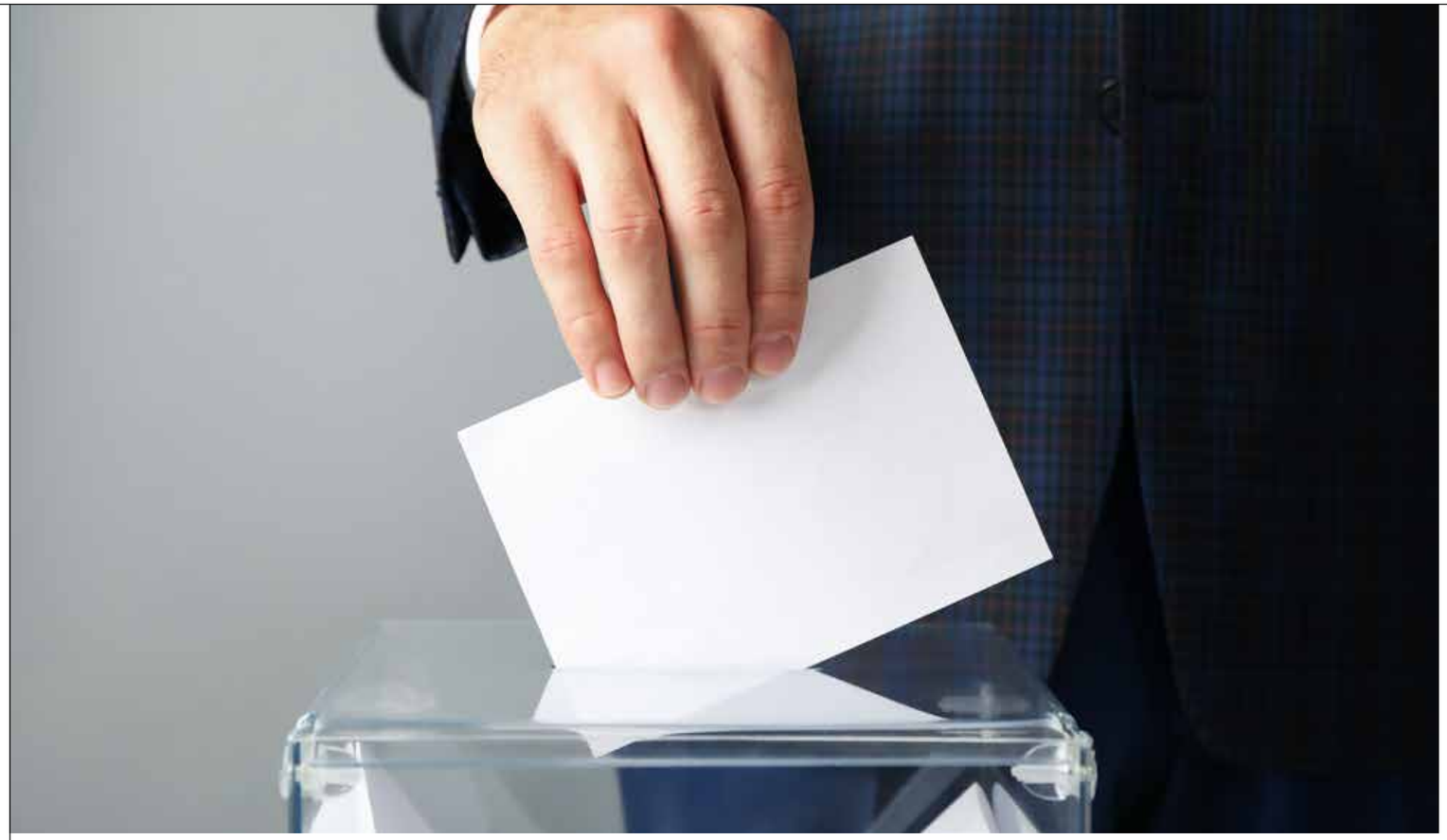

Picture credit: AdobeStock

DEMOCRACY UNDER SIEGE

Lewis Shields *navigates the global threats to democracy in a historic election year*

In this historic year for elections globally, cyber security threats are front and centre of political discourse, with malicious actors – ranging from hostile nation states, to politically motivated cyber criminals and online trolls – likely seeking to influence the outcomes across the globe. As voters prepare to make crucial decisions, political processes are under significant threat from these various cyber activities aimed at manipulating public opinion and eroding trust in democratic institutions.

While direct election interference from hostile state actors against voting mechanisms remains possible, the greatest threat stems from the continuous spread of mis-, dis- and malinformation (MDM), which seeks to undermine public trust and exacerbate polarisation, both of which pose a threat to the preservation of democratic integrity.

MDM is almost certainly the primary danger to the integrity of elections, with threat actors of varying motivations seeking to sway voter opinions of candidates, affect the outcome or undermine public confidence in the democratic process and associated institutions. To date, much of the high-profile instances of disinformation observed around the UK elections has come from competing political parties.

Although adversarial nation state actors had very little impact on the UK election process, there is a higher likelihood that these actors took active measures to influence public opinion to achieve a favoured outcome or sow division in society to weaken a perceived adversary. Social media platforms – due to their wide reach, susceptibility to impersonations of legitimate entities and bot/troll accounts and the speed at which information can be disseminated – are particularly vulnerable to these kinds of influence campaigns.

The proliferation of false narratives requires a concerted effort from both the public and private sectors to identify and counteract disinformation

Similarly, influence campaigns are very likely to be conducted – either at small scale or large scale – by ideologically or politically motivated cyber criminals. The threat of these actors disseminating malinformation surrounding an election – including breaches of voter databases and hacking of confidential party information – also remains high. Often these campaigns are conducted not for personal gain, but for clout among peers or to generate publicity.

Members of the public also contribute to the spread of mis- and disinformation, either knowingly or unwittingly, primarily through the use of social media platforms. While an individual does not have the ability to affect the election outcome, the propensity for inaccurate information and media snippets to become widespread has been demonstrated multiple times in recent months. This often results in truths associated with objective realities being diluted, devalued, and diminished.

The proliferation of false narratives requires a concerted effort from both the public and private sectors to identify and counteract disinformation. Meanwhile, many believe social media companies should have a more significant role to play in monitoring and mitigating the spread of false information, though the speed and scale at which these platforms operate pose considerable challenges.

Big tech and social media companies were accused of falling short ahead of the UK General Election, and recent findings indicate the lack of moderation and regulation regarding algorithms, with the potential for the creation of 'echo chambers' for users on such sites. These echo chambers limit the content and information users are likely to access and possibly use to inform judgments during an election period.

Generative AI has become a powerful tool in the arsenal of those looking to influence elections. While these tools are regularly used for benign purposes, the continued improvement of generative AI technology has allowed for increasingly sophisticated manipulation of audio and video content known as deep fakes. By creating highly realistic, synthetically generated images and deep fakes of politicians, adversaries can fabricate incidents or statements that never occurred, discrediting and undermining opposition candidates. Synthetically generated videos can now exhibit natural expressions, speech and mannerisms that can be difficult to distinguish from reality. The ongoing development of these tools very likely lower the barriers to entry for threat actors, increasing the threat and potential impact of attacks.

AI-driven MDM can also be used to rapidly implement strategies that trick users into disclosing credentials and other sensitive information. The risk of being misled by false information is often increased by attacks on the back end of AI systems, where systems are compromised, making people overly dependent on them without fully understanding their mechanisms. The sophistication of such tools and tactics means that even a well-informed electorate can be misled by seemingly authentic content and practices.

The threat from targeted attacks against election workers, government officials, public servants, political candidates and journalists remains high. In the past six months alone, more than a dozen Westminster insiders have reportedly been targeted, including politicians and government advisers. These attacks often involve social engineering attempts that leverage election-related events as lures, which are designed to encourage interaction and exploit human vulnerabilities.

Threat actors very likely seek to capitalise on contentious policy proposals from political parties that elicit emotional reactions to entice engagement with malicious links, attachments and redirects. The high threat is likely exacerbated by widely available generative tools, which enable more believable social engineering approaches.

CHINA HAS REPORTEDLY DEMONSTRATED BOTH THE INTENT AND CAPABILITY TO INFLUENCE UK POLITICS

At the same time, the rise of synthetic media technology – such as manipulated videos, false social media posts and even fake campaign voicemails – has raised concerns about its potential impact on political campaigns, democratic processes and the overall geopolitical landscape. This widely available and affordable technology has enabled attackers to not only scale their efforts, but also increase their chances of success by making fake personas more convincing and difficult to detect.

To avoid falling victim to such social engineering attacks there must be an increased focus on education, awareness and identification. Voters should always be cautious before opening emails or clicking links related to political campaigns or donations. Staff, from election workers right the way up to politicians, need to be educated and trained to spot the 'tell-tale' signs of a social engineering attack. In today's sophisticated threat landscape awareness training isn't an optional benefit, it is an organisational imperative.

Widely perceived adversarial nation states – including Russia, China, Iran and North Korea – have long been known to interfere in major global events, either for the purposes of espionage, exacerbate social divisions and other forms of competitive advantage. Dame Margaret Beckett, Chair of Westminster's national security committee, said herself in a recent letter to Prime Minister Rishi Sunak that the UK has experienced a "pattern of attempted foreign interference" from these countries in recent years. This year is no different and the fallout from ongoing global geopolitical events coupled with elections occurring around the world have created a febrile environment for these actors to conduct these malicious activities.

Russia is deemed to pose a considerable and consistent threat to the elections of its perceived rivals and are often attributed the most overt influence and interference campaigns. Reporting indicates that In 2016, the UK Brexit vote was targeted by disinformation campaigns peddled on social media platforms, allegedly by Russian state-affiliated groups.

While the Brexit vote was much more consequential to the UK's and EU's global trajectory, these actors have demonstrated both the intent and capability to conduct campaigns that influence UK political outcomes,. US senator Mark Warner, chair of the United States Senate Intelligence Committee, issued a warning to the UK government of a likely ramp up in "egregious" efforts by Moscow to interfere in the election and was expected to continue leading up to the recent UK election.

RUSSIA POSES A CONSIDERABLE AND CONSISTENT THREAT TO ELECTIONS OF ITS RIVALS

Additionally, China-affiliated actors have reportedly demonstrated both the intent and capability to influence UK politics. Earlier this year Chinese state-affiliated hacking group APT 31 allegedly attempted to access UK lawmakers' email accounts, potentially indicating a longer-term strategy to shape overseas political outcomes.

As such, the threats posed against the UK's recent election were being taken seriously by the National Cyber Security Centre (NCSC) as evidenced by increased support ahead of the election, offering an extra layer of security on the personal devices of high-risk individuals. The Personal Internet Protection service was a free service for high-risk individuals warning them if they tried to visit a domain known to be malicious and then blocking outgoing traffic to these domains. Previously used by organisations, NCSC's extension of the service to the individual is telling of the threat level and likely methodologies of nation-state actors. This was an opt-in service, however, meaning that individuals had to take it upon themselves to understand their personal level of risk and understand their responsibility to prioritise their own cyber security. The service underscored the reality that there is an element of personal liability in protecting yourself and the organisations/governments you represent from nation-state cyber attacks.

Challenges posed by disinformation campaigns, targeted attacks on election workers and high-profile officials, and the overall complexity of the digital landscape are significant. However, with heightened awareness, collaboration among stakeholders and the implementation of robust cyber security measures, it is possible to navigate such threats successfully.

Maintaining the integrity of election results is critical as it extends beyond data protection. Ensuring trust in a truly democratic society by identifying and anticipating threats to such results is essential for upholding overall public confidence in its governing institutions. Effective cyber security must be capable of detecting and mitigating both technical threats and those that undermine the perceived security and legitimacy of the elections.

The integrity of the democratic process hinges on the ability to conduct free and fair elections, untainted by external interference or internal sabotage. Following the recent UK general election, the rise of sophisticated cyber threats necessitates a comprehensive and proactive approach to election security.

While the cyber security challenges are daunting, they're not insurmountable. This year's many elections will test the resilience of the electoral processes, but with concerted efforts it should be possible to uphold democracy. With robust security protocols and a proactive stance, we can navigate this minefield and ensure elections remain free, fair and secure ●

Lewis Shields is Director of Dark Ops at ZeroFox.

Social media companies should play a more significant role in monitoring and mitigating the spread of false information