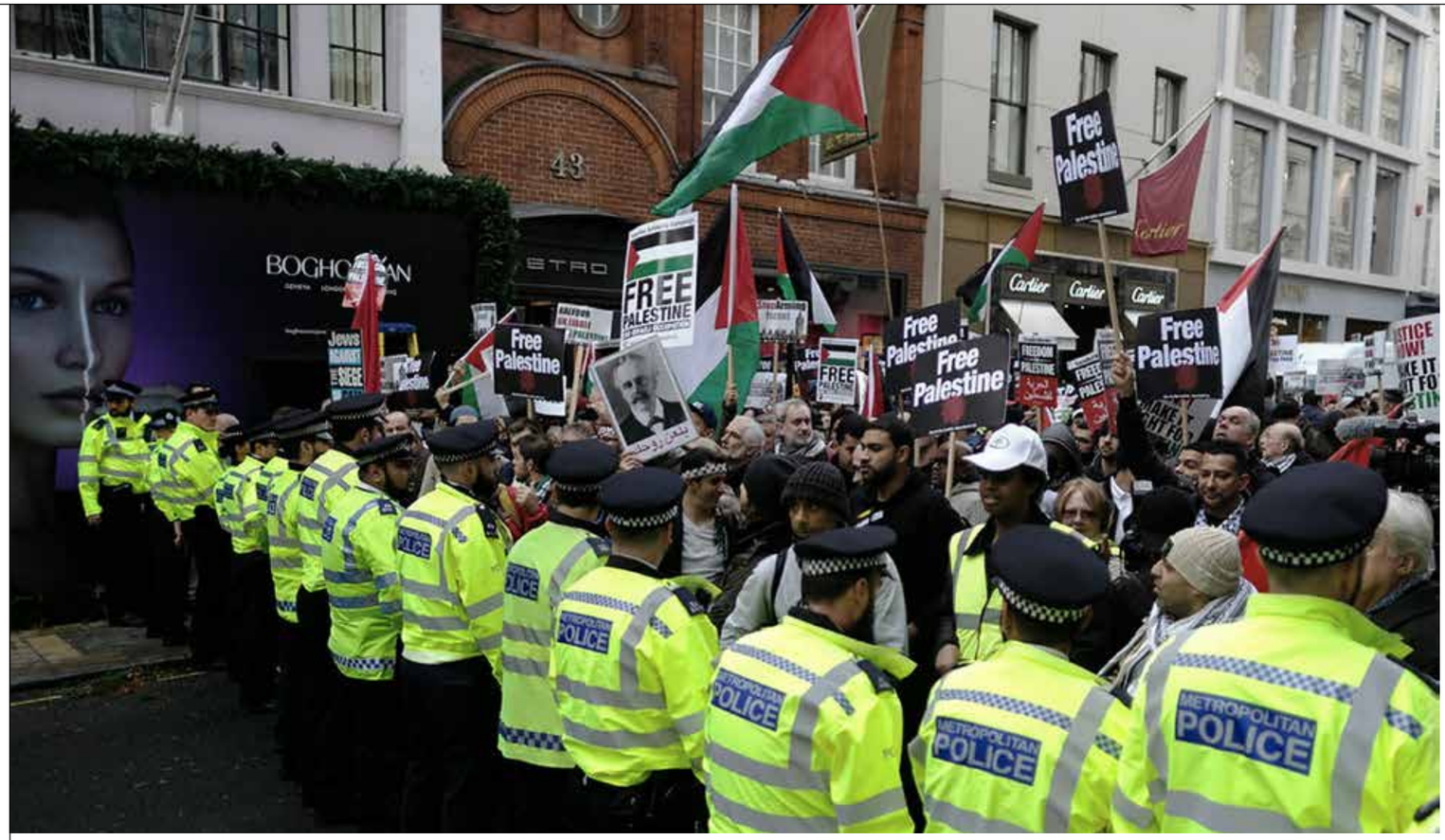

Picture credit: Alisdare Hickson

DEMOCRACY UNDER FIRE

Beth Hepworth *considers a big year for global elections in this digital threat forecast*

2024 is set to be a monumental year for democracy; with over two billion people across 50 countries going to the polls to elect representatives at local, national and intra-continental levels. This includes elections in some of the world's most populous countries, such as India, Brazil, Indonesia and the US.

While this year will certainly be a milestone in the long evolution of democracy, many of these elections take place amid a backdrop of increasing divisions in international relations, an uptick in populist politics and a widespread disenchantment with political representation in some of the world's most developed democracies.

All these issues transcend real-world and online spaces, creating distorted and muddied political landscapes prime for exploitation. This will likely manifest in diverse online adversarial threat behaviours and narratives aiming to both manipulate public opinion and capitalise on volatile information environments to cause harm. In view of this, we have outlined the primary digital threats posing significant risks to elections across the world in 2024.

MISINFORMATION AND DISINFORMATION

Electoral misinformation and disinformation will likely remain highly prevalent in elections across the world in 2024. Online threat actors, such as partisan pseudo-media entities and amateur political commentators will likely continue sharing content designed to sow distrust in the electoral process through both authentic and inauthentic means, while attempting to generate engagement for both ideological and commercial gain. Across geographies, false narratives are likely to target voting systems and the integrity of electoral institutions, particularly in countries with heightened polarisation and in the aftermath of closely contested elections.

This type of disinformation at scale will have a significant impact on highly volatile political environments and countries with a history of contentious fraud claims in previous elections. Electoral disinformation narratives played a significant role in elections across the world in 2023, including in Nigeria, Spain, and Turkey, and has already had an impact on elections in Taiwan and Indonesia in the first two months of 2024. These narratives often emanate from discourse pushed by politicians and candidates, before being amplified by both organic and inauthentic users – a behaviour which is likely to continue over the coming year.

Disinformation targeting the integrity of elections can influence dangerous real-world behaviours, including disrupting democratic processes and triggering post-election violence. This has been witnessed over the past year in countries such as Brazil – where supporters of former President Jair Bolsonaro stormed Congress in January 2023 alleging institutional election fraud.

HATE SPEECH

Hate speech perpetrated by extremist organisations and political parties in online spaces will likely pose a significant risk to elections across the world, particularly in the US, Europe, South Africa and India.

These entities will likely exploit polarised information environments and target wedge issues – such as immigration and religion – to seed hateful discourse towards minority groups, as well as to recruit and mobilise users in less-monitored digital spaces. These behaviours are often perpetrated by extremist organisations and are amplified organically by their online supporters. These actions will likely be seen during the campaigning period ahead of the June European Union elections, particularly in light of the growing popularity of ultra-nationalist ideologies and politicians across the continent in 2023.

There is also a significant risk of ideologically motivated real-world violence around election periods. Ahead of the February Indonesia general election, heightened levels of anti-Rohingya discourse online triggered violent confrontations between protesters and refugees. Similarly, in India, the Hindutva ideology – which has millions of supporters and has incited hatred against civilians and political candidates belonging to minority religious communities both online and offline – will likely impact the April-May general election.

Hate speech does not usually manifest in an isolated environment and is normally embedded with other behaviours including misinformation, harassment and violent extremism. Around the October US election in particular, we are likely to see an increased presence of extremist groups and armed militias who claim to protect electoral integrity while sharing ultranationalist viewpoints and encouraging civilians to take up arms.

FOREIGN INFLUENCE

Foreign state-backed influence operations (IOs) targeting elections are highly likely to be a persistent and significant threat in 2024. The aim of foreign IOs targeting elections is to create a divisive and distorted information environment. This in turn triggers confusion and fuels voter polarisation, while instilling public distrust in leaders and the electoral process.

The US and EU elections will likely be primary targets for foreign IO campaigns originating from hostile states such as Russia, Iran, and China. These operations often use inauthentic online assets to amplify content, as well as co-opting domestic media entities and journalists, who either authentically launder narratives from the hostile state or are explicitly directed to do so. Recent reports have outlined how Russia and China linked IOs have targeted the US to exploit domestic socio-political divisions. Similar state-linked campaigns will likely increase in prevalence in the coming year, capitalising on wedge issues, such as US spending on Ukraine, to sow discord ahead of the October US election.

AI-GENERATED CONTENT HAS HAD LIMITED NEGATIVE INFLUENCE ON ELECTIONS UP TO NOW

Foreign IOs will also likely target governments with an overlapping ideological alignment in an attempt to strengthen bilateral relations. For example, Russia will likely build on the popularity of the regional branches of RT and Sputnik in Latin America to spread narratives aimed at destabilising politics in elections in Mexico and Brazil. Similarly, there is an increased risk of Russian interference targeting the upcoming May elections in South Africa. Covert influence operations have already been found to inflame inter-racial and intra-African National Congress tensions, as well as promote pro-Russian propaganda in relation to the war in Ukraine.

AI-GENERATED CONTENT

AI-generated content will likely play a greater role in elections in 2024 as threat actors and political campaigners continue to embed AI techniques within their content-producing toolkits. AI-manipulated and generated media will likely be used by inauthentic entities to deceive voters, as well as by official election campaigns as promotional material.

Threat actors certainly have the ability to weaponise AI effectively and convincingly, which has been demonstrated on numerous occasions over the past year. For example, in April 2023, the Republican Party in the US released an ad with AI-generated images visualising a 'dystopian world' with a re-elected President Joe Biden. Similarly, in December 2023, Moldovan President Maia Sandu was forced to refute claims made in a Russia-made deepfake video of herself.

However, the successful use of sophisticated AI-generated content and technically manipulated media in sowing distrust in candidates and electoral processes will likely be limited; the majority of such content

Some actors will exploit polarised information environments and target wedge issues to seed hateful discourse

being low quality and easily discernible by ordinary online users. In Indonesia, for example, while many media reports highlighted the proliferation of AI-generated media during the 2024 election campaigning period, this content was merely an extension of official political campaigning and did not have nefarious intentions.

THERE IS A SIGNIFICANT RISK OF IDEOLOGICALLY MOTIVATED REAL-WORLD ELECTION VIOLENCE

As a result, the risk of AI to elections in the medium term is often overstated. The vast majority of elections in 2023 saw AI-generated content have a limited influence and current disinformation campaigns are succeeding organically by exploiting societal rifts. As such, the present risk of AI to elections is centred more on the intrinsic uncertainty of its potential, rather than on its current impact.

HARASSMENT AND DOXXING

Heightened levels of targeted harassment and doxxing are likely in 2024, following a spike in threats against election workers and politicians over the past year in countries including New Zealand, Sweden, the US and Japan. Going forward, targets of online harassment campaigns are likely to include political candidates, election workers, journalists, activists and members of the judiciary. This is most likely to manifest in highly polarised political environments.

These threats will likely entail the dissemination of Personally Identifiable Information (PII) online – such as targets' home addresses, family members and phone numbers – as well as online harassment campaigns designed to undermine their legitimacy. In the US, this has manifested in a phenomenon known as 'swatting' – a form of harassment where false calls to law enforcement trigger an armed police raid on the target's house. A recent example of this saw Secretary of State for Maine, Shenna Bellows, targeted in December 2023.

Digital forms of harassment can also be a precursor to inciting physical violence against journalists and civil society members. These behaviours are often instigated by high-level politicians who legitimise the harassment. We have already seen this in the recent 7 January 2024 election in Bangladesh, where Awami League supporters attacked reporters at voting stations. Similarly, in Mexico, high-profile politicians and criminal groups frequently attack and harass media workers, making it one of the most violent countries in the world for journalists.

As we navigate the 2024 election landscape, it is important to acknowledge the digital activities that threaten our democracies in the real-world. From misinformation and disinformation to hate speech, doxxing and foreign influence operations, threat actors are seeking to exploit vulnerabilities and sow discord. The proliferation of AI-generated content also adds another layer of complexity, albeit with limitations that may not yet match the anxieties surrounding its potential impact.

However, by understanding the multifaceted nature of these threats and facilitating a reasoned, rational and fact-based conversation, we are able to begin countering their influence. Collaboration between governments, tech companies, civil society and individuals is essential in fortifying our digital defences and preserving the integrity of our democratic institutions ●

Beth Hepworth is Director of Protection Group International.

False narratives are likely to target voting systems and the integrity of electoral institutions globally