



Joint Committee on the National Security Strategy

House of Commons · London · SW1A 0AA

Email JCNSS@parliament.uk



Rt Hon Rishi Sunak MP
Prime Minister
10 Downing Street
London
SW1A 2AA
By email

23 May 2024

Risks and threats to UK democracy before, during and after 4 July 2024

Dear Prime Minister,

On 3 June, our Committee was due to hear from the Minister for Security, Tom Tugendhat MP, and the Secretary of State for Science, Innovation and Technology, Michelle Donelan MP, as part of our Defending Democracy inquiry. Following your announcement yesterday and given the critical nature of our inquiry, we have taken the decision to write to you, to set out our views and concerns in advance of the UK's General Election.

The UK is not alone in holding national elections this year. 2024 is set to be a critical moment in our global history. Record numbers will head to the polls. Although the exact number of elections taking place globally is uncertain, at no point in modern history have so many elections been scheduled to take place in such a short period of time. While this is, in many ways, cause for celebration, the high quantity of elections occurring in quick succession poses a risk to global security.

Foreign Interference

In recent years, the UK has experienced a pattern of attempted foreign interference from countries such as China, Russia, Iran and North Korea.¹ The Intelligence and Security Committee (ISC) explored widespread allegations of Russian interference in the 2016 referendum on UK membership of the European Union.² The National Cyber Security Centre (NCSC) noted in 2023: "The UK government assesses that it is almost certain that Russian actors sought to interfere in the 2019 general election".³ The ISC subsequently pointed to precedent for China seeking to influence democratic processes overseas, in the US and Canada, for example.⁴

¹ National Cyber Security Centre, [Annual Report 2023](#), 14 November 2023, pp 11-12

² Intelligence and Security Committee of Parliament, [Russia](#), HC 632, July 2020, paras 39-48

³ National Cyber Security Centre, [Annual Report 2023](#), 14 November 2023, p 20

⁴ Intelligence and Security Committee of Parliament, [China](#), HC 1605, para 115



Joint Committee on the National Security Strategy

House of Commons · London · SW1A 0AA

Email JCNSS@parliament.uk



Since 2019, there have been significant changes in the geopolitical situation. According to the NCSC, these changes have made the prospect of influencing political discourse in democracies “ever more attractive for state actors”. It describes democratic events such as elections as “attractive targets for malicious actors”.⁵

As such, it is our view that the UK must be prepared for the possibility of foreign interference during the General Election that will take place on the 4 July 2024.

In evidence to our Defending Democracy inquiry, Professor Rory Cormac from the University of Nottingham said, “hostile foreign states feed and exploit our internal divisions and weaknesses. They do not create these divisions. They spot them, they exploit them, they polarise, and they try to crack them open as far as possible”.⁶

We have considered a number of ways hostile actors may seek to exploit divisions and weaknesses during the forthcoming election period. They may seek to:

- Undermine trust in electoral processes through **cyber-attacks targeted at our institutions**, including ransomware attacks. Such attacks could raise questions about their security as well as their ability to facilitate and safeguard UK democracy.⁷
- Target high-profile individuals such as political candidates **to retrieve sensitive information for exploitation through coercion or publication**, thereby undermining trust in politicians.⁸
- **Spread disinformation online about public figures** - including through the use of generative AI to create fake videos and audios - to fuel conspiracy theories and undermine trust in UK leaders and institutions.⁹
- **Sow division and cause chaos where there are already domestic divides** on controversial or politicised topics.¹⁰

Through our inquiry, we also received evidence from the Electoral Commission¹¹ and visited its London office in May 2024. With regards to foreign interference, we note the Commission’s recommendations on the regulation of political finance in the UK and draw all political parties’ attention to it.¹²

⁵ National Cyber Security Centre, [Annual Report 2023](#), p 40

⁶ [Q2](#) [Professor Rory Cormac]

⁷ HMG, [UK holds China state-affiliated organisations and individuals responsible for malicious cyber activity](#), 25 March 2024. Our committee already warned the Government in our 2023 Ransomware Report that “if the UK is to avoid being held hostage to fortune and avoid electoral interference, it is vital that ransomware becomes a more pressing political priority”. Joint Committee on the National Security Strategy, First Report of Session 2023–24, [A hostage to fortune: ransomware and UK national security](#), HC 194 HL Paper 23, para 130

⁸ BBC, [‘UK imposes sanctions after Chinese-backed cyber-attacks’](#), 26 March 2024; HMG, [UK holds China state-affiliated organisations and individuals responsible for malicious cyber activity](#), 25 March 2024

⁹ Unlock Democracy (DED0022), Freedom House, [‘The Repressive Power of artificial Intelligence’](#), 2023, p12

¹⁰ BBC, [Sadiq Khan says fake AI audio of him nearly led to serious disorder](#), February 2024; [Q2](#) [Professor Rory Cormac]

¹¹ [Qq 36-43](#) [Vijay Rangarajan]; [Qq 36-43](#) [Louise Edwards]; Electoral Commission ([DED0016](#))

¹² Electoral Commission ([DED0016](#)) paras 43-50. See also Spotlight on Corruption ([DED0030](#))



Joint Committee on the National Security Strategy

House of Commons · London · SW1A 0AA

Email JCNSS@parliament.uk



Emerging technology and deepfakes

There is nothing new in hostile actors seeking to interfere in elections. Today, however, these actors can reach the British public far more easily than ever before. As a consequence of technological advances, hostile actors – both foreign and domestic – have the ability to influence the information landscape by creating harmful deepfake videos and audios that can rapidly spread. We have seen these tactics being used to sow disinformation in the United States, where a deepfake audio of President Biden discouraged voters from going to the polls during the primary election.¹³ These tactics have also been used in the UK, where a deepfake audio was circulated online before Armistice Day, purportedly showing the London Mayor, Sadiq Khan, making deeply inflammatory remarks.¹⁴ In February 2024, Sadiq Khan told the BBC that the incident almost caused “serious disorder”,¹⁵ yet this did not constitute a criminal offence, according to the Metropolitan Police.¹⁶ Deepfakes continue to have the potential not only to cast doubt over politicians and political parties, but also to mislead the public and cause disorder.

We welcome Government legislation in recent years, which – among other things – has sought to tackle the challenge of foreign interference and strengthen online safety.¹⁷ However, we fear that important legal loopholes remain, partly due to the speed at which technologies are advancing. In particular, the new laws still appear to leave the Government with few powers to combat non-consensual political deepfakes that are produced domestically.¹⁸ For example, we heard that the National Security Act 2023 does not do enough to prevent an ordinary person, who otherwise lacks technological skill, “sitting in their bedroom using a commonly available generative AI tool to create and quickly disseminate convincing political disinformation which social media platforms have no obligation to proactively monitor or take down”.¹⁹

Prosecution is only one potential tool available to the Government in mitigating some of the risks involved in deepfakes. Public education is another. However, the Government’s current Fraud Campaign appears not to educate the public on how to identify deepfakes. And although the Home Secretary has raised the issue of deepfakes posing threats to elections this year,²⁰ this is not the same as a concerted campaign to equip the public in advance of a

¹³ Associated Press News, [‘New Hampshire Investigating fake Biden robocall meant to discourage voters ahead of primary’](#), 23 January 2024

¹⁴ BBC, [‘Sadiq Khan says fake AI audio of him nearly led to serious disorder’](#), 13 February 2024

¹⁵ BBC, [‘Sadiq Khan says fake AI audio of him nearly led to serious disorder’](#), 13 February 2024

¹⁶ BBC, [‘Fake audio of Sadiq Khan is not a crime says Met’](#), 11 November 2023

¹⁷ For example, the 2022 Elections Act, the 2023 National Security Act, the 2023 Online Safety Act.

¹⁸ Logically ([DED0002](#)) para 67; Online Safety Act Network ([DED0033](#)) para 34; Alan Turing Institute ([DED004](#)) paras 2.1, 2.1.1, 2.1.2, 2.1.3

¹⁹ Logically ([DED0002](#)) para 67

²⁰ The Times, [‘James Cleverly: Deepfakes pose ‘perfect’ threat to next election’](#), 25 February 2024



Joint Committee on the National Security Strategy

House of Commons · London · SW1A 0AA

Email JCNSS@parliament.uk



General Election. Although ultimately the public should not be held responsible for detecting harmful online content, we have sought to provide information that may help the public to spot deepfakes and develop their skills to do so. We would encourage the Government and members of the public to watch or read the transcript of the evidence session our committee held on 18 March 2024, where an expert explained a number of ways to spot deepfake images.²¹

We call on the Electoral Commission to issue public guidance on how to spot deepfakes and other types of mis- and disinformation online, as a matter of priority now that an election has been called. We advise any future Government to consider making it illegal to create any kind of harmful political deepfake. We also recommend that any future Government support a whole-of-society approach to combatting these challenges, through further campaigns to share information and to equip the public as technology develops.

Social media and technology companies

As part of our inquiry, we received written evidence from social media and technology companies that operate in the UK. This included evidence from X, Snapchat, TikTok, Meta, YouTube, Google, and Microsoft. We have separately published our concerns about the evidence we received.²² In particular, we were concerned that:

- These companies have taken different, often siloed approaches to tackle the challenge of foreign interference and mis- and disinformation more broadly.
- Social media algorithms continue to create harmful ‘echo chambers’ on sites accessed in the UK. Such echo chambers limit the content and information that users are likely to access and use to inform judgments during an election period.

It is yet to be seen whether Ofcom’s new enforcement powers under the Online Safety Act 2023 can ensure that social media companies adhere to their own policies on mis- and disinformation and take down illegal content swiftly.

Delays to relevant powers and provisions

As mentioned above, the Government has introduced legislation in recent years that is relevant to the challenges we describe. Regrettably, our inquiry has uncovered delays in the implementation of important provisions that means they will not now be enacted before the forthcoming General Election. For example:

- Under the Online Safety Act 2023, Ofcom - the regulatory authority for online safety - is responsible for setting up an Advisory Committee on mis- and disinformation. This

²¹ [Q20](#) [Dr Mhairi Aitken]; [Parliamentlive.tv - National Security Strategy \(Joint Committee\)](#)

²² Joint Committee on the National Security Strategy, [Big tech and social media companies falling short ahead of UK General Election](#), 21 May 2024



Joint Committee on the National Security Strategy

House of Commons · London · SW1A 0AA

Email JCNSS@parliament.uk



committee is intended to provide advice to Ofcom about how services should deal with mis- and disinformation as well as how they use media literacy duties and transparency powers. Despite commitments made by a Minister in October 2023 to support Ofcom in establishing this committee more quickly,²³ we learnt on 18 March 2024 – nearly five months later – that this committee will be put together “probably towards the end of the year.”²⁴

- Ofcom is tasked with ensuring that online service providers are effectively mitigating and managing the risks from foreign interference. However, we heard on 18 March that Ofcom is still considering how to bring this foreign interference offence into force for social media companies after closing their consultation on 23 February 2024.²⁵
- The Foreign Influence Registration Scheme, established under the National Security Act 2023, is expected to come into force in 2024, but the exact timing is not clear.²⁶

We urge the Government to do whatever possible to speed up the delayed areas of work that we have highlighted. Given it will not be possible to complete this work before the General Election, clear public communication about the risks posed by mis- and disinformation and other forms of foreign interference is essential. We refer to this point on public transparency further below.

The safety of Members of Parliament, candidates, and high-risk individuals

During our inquiry, we learnt that the safety of MPs, candidates and other high-risk individuals in the UK is a growing area of risk. Politically motivated abuse and intimidation is high, according to the Electoral Commission.²⁷ We agree with the Electoral Commission that “the way to reduce this threat cannot be for potential victims to take preventative action or self-censor” to ensure their safety, nor should candidates be deterred from entering politics on this basis.²⁸ It is also wholly unacceptable for Members of Parliament to face intimidation when voting or receive death threats as a result of their votes.²⁹

On 28 February 2024, the Home Office announced a new package of support, which included £31 million of funding to support MPs’ safety.³⁰ The Defending Democracy Taskforce, established in November 2022, “takes a broad interpretation of what is needed to defend democracy”, focusing not only on protecting elections and elected officials but also “ensuring that citizens are free and able to debate ideas”.³¹ We call for this work to continue as a priority

²³ HL Deb, 24 October 2023, [col 509](#) [Lords Chamber]

²⁴ [Q21](#) [Jessica Zucker]

²⁵ Ofcom, ‘[Consultation: Protecting people from illegal harms online](#)’, accessed 23 May 2024

²⁶ Home Office, [Foreign Influence Registration factsheet](#), accessed 23 May 2024

²⁷ The Electoral Commission ([DED0016](#)) para 6

²⁸ The Electoral Commission ([DED0016](#)) para 10

²⁹ HC Deb, 22 February 2024, [col 873](#) [Commons Chamber]

³⁰ HMG, [31m committed to protect democratic process](#), accessed 23 May 2024

³¹ Home Office ([DED0047](#)) para 4



Joint Committee on the National Security Strategy

House of Commons · London · SW1A 0AA

Email JCNSS@parliament.uk



in the start of the new Parliament, so that new and returning MPs are briefed quickly and able to take up the support available.

Transparency with the public

Conflict in the Middle East and Russia's renewed illegal invasion of Ukraine has contributed to a sense that the world is becoming more dangerous than at any time since the Cold War, as you yourself have said.³²

Despite public Government statements on the threat from hostile foreign actors such as China, Russia, Iran and North Korea,³³ it is not clear if members of the public fully understand how these threats will manifest and what this means for the UK, its democracy and for them as individuals. For this reason, we have taken the decision to write and publish this letter. Through this correspondence, our Committee hopes to contribute to a vital public conversation in the lead-up to the UK General Election.

We must all be part of the effort to defend the UK's democracy and to remember that, as Jo Cox MP said in her maiden speech, "we are far more united and have far more in common with each other than things that divide us."³⁴ The forthcoming General Election is a crucial test of that spirit and of the Government's preparations to safeguard the electoral processes that epitomise our democratic ideals. We therefore call on you as Prime Minister to use the last few days of this Parliament to bring Government, political parties, and electoral and security agencies together to identify any last actions that can be taken collectively in the national interest.

Yours sincerely,

Dame Margaret Beckett DBE MP

Chair

³² Prime Minister's Office, 10 Downing Street and The Rt Hon Rishi Sunak MP, [Prime Minister's defence speech in Warsaw: 23 April 2024](#), 23 April 2024

³³ Debate, [Cyber Security and UK Democracy](#), 25 March 2024; Oral Statement, [Russia](#), 8 May 2024

³⁴ [Official Report](#), 3 June 2015; Vol. 596, c. 675.