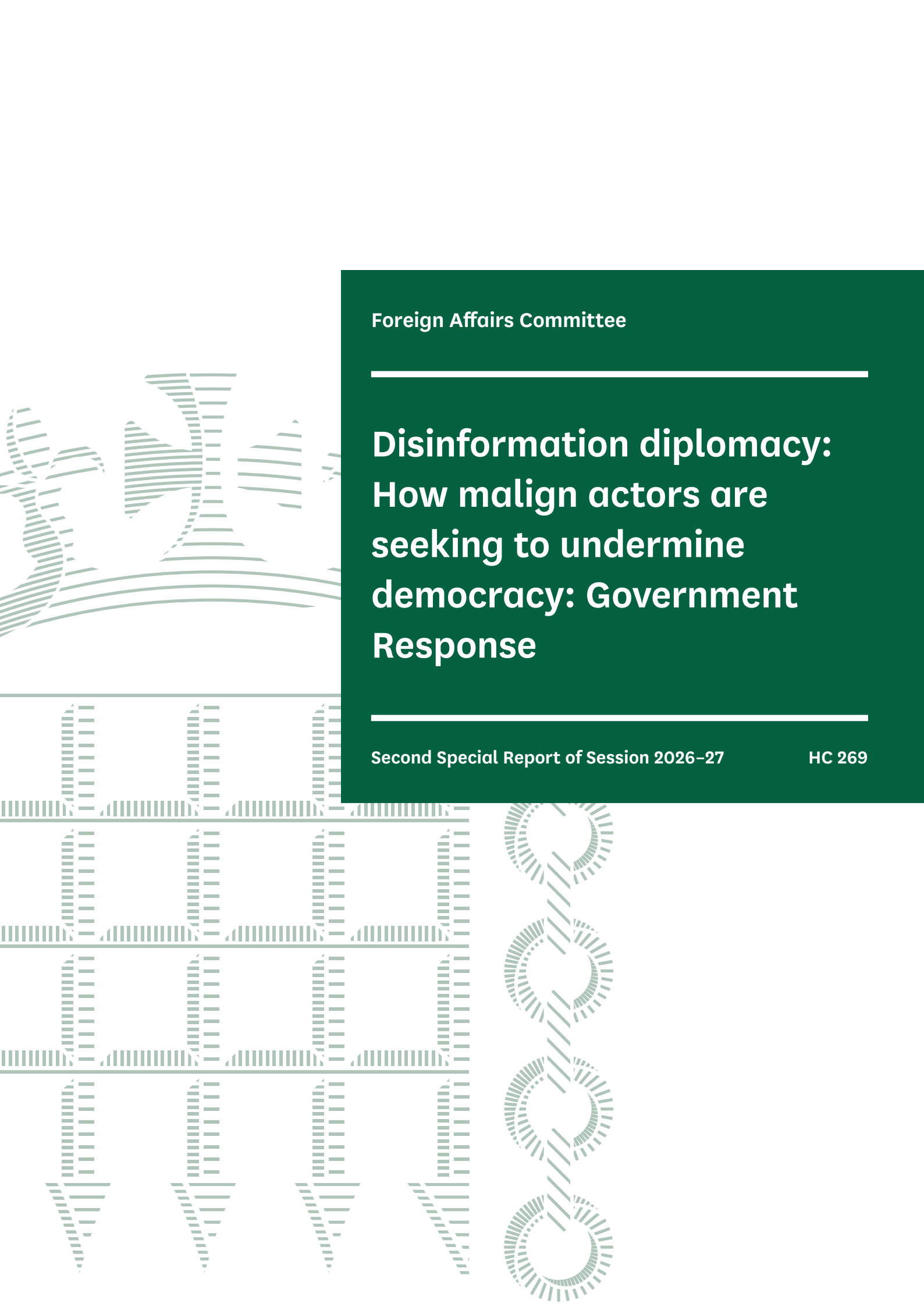




Foreign Affairs Committee

Disinformation diplomacy: How malign actors are seeking to undermine democracy: Government Response

Second Special Report of Session 2026–27

HC 269

Foreign Affairs Committee

The Foreign Affairs Committee is appointed by the House of Commons to examine the expenditure, administration, and policy of the Foreign and Commonwealth Office and its associated public bodies.

Current membership

[Emily Thornberry](#) (Labour; Islington South and Finsbury) (Chair)

[Fleur Anderson](#) (Labour; Putney)

[Alex Ballinger](#) (Labour; Halesowen)

[Aphra Brandreth](#) (Conservative; Chester South and Eddisbury)

[Dan Carden](#) (Labour; Liverpool Walton)

[Richard Foord](#) (Liberal Democrat; Honiton and Sidmouth)

[Alan Gemmell](#) (Labour; Central Ayrshire)

[Uma Kumaran](#) (Labour; Stratford and Bow)

[Abtisam Mohamed](#) (Labour; Sheffield Central)

[Edward Morello](#) (Liberal Democrat; West Dorset)

[Sir John Whittingdale](#) (Conservative; Maldon)

Powers

The Committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No. 152. These are available on the internet via www.parliament.uk.

Publication

This Report was Ordered by the House of Commons, on 2 June 2026, to be printed. It was published on 8 June 2026 by authority of the House of Commons. © Parliamentary Copyright House of Commons 2026.

This publication may be reproduced under the terms of the Open Parliament Licence, which is published at www.parliament.uk/copyright.

Committee Reports are published on the Committee's website at www.parliament.uk/facom and in print by Order of the House.

Contacts

All correspondence should be addressed to the Clerk of the Foreign Affairs Committee, House of Commons, London SW1A 0AA. The Committee's email address is fac@parliament.uk. You can follow the Committee on X (formerly Twitter) using [@CommonsForeign](https://twitter.com/CommonsForeign).

Second Special Report

The Foreign Affairs Committee published its fourth Report of Session 2024–26 on 27 March 2026, [Disinformation diplomacy: How malign actors are seeking to undermine democracy](#) (HC 703). The Government Response was received on 22 May 2026 and is appended below.

Appendix: Government Response

Introduction

1. The UK Government is grateful to the Foreign Affairs Committee for its report published on 27 March 2026. We welcome the Committee's reflections on the Government's approach to countering Foreign Information Manipulation and Interference (FIMI) across the international and domestic agenda and we have carefully considered the Committee's recommendations. This is a response on behalf of the Government and has been drafted by FCDO in consultation with relevant departments. This response addresses the Committee's recommendations in two parts: the first focuses on the Government's international response and the second, the domestic response.
2. We share the Committee's view of the nature of the threats we face; the seriousness of the threat posed by FIMI to the UK and our international partners; and the need for greater coordination across Government. As the Foreign Secretary outlined in her December Locarno speech, we are confronting an industrial-scale attack on the UK's and our allies' information environment, aimed at undermining our security and democratic systems, with Russia engaged in information warfare against the UK and Ukraine.

3. Combating the threat of information warfare requires effective coordination of all tools and levers available to us, across all parts of government, both domestically and internationally. The FCDO's Spending Review settlement demands that the department target its financial allocations in a more concentrated way on FCDO Priorities. This includes activity that delivers our Security priorities and contributes to the UK's wider defence spending uplift. The Department has ensured that the allocations we have received are targeting the threats and challenges we face, including a key focus on countering hybrid threats including cyber attacks, election interference, FIMI and other threats to stability.
4. We recognise the Committee's points about the need for strong join up across Government on this agenda. Ministers and officials are therefore working to strongly cohere our efforts across the whole of government, including as we join up domestic and international activity. The Government also recognises the need to place our response to foreign information threats in the context of our response to wider state threat activity given these actors often operate across multiple vectors to achieve their aims and will continue to adapt our approaches as the threat evolves.
5. Since Stephen Doughty MP, Minister of State (Europe, North America and Overseas Territories), gave evidence to the Committee in January, we have continued to strengthen our cooperation with key international partners. For example, in March, the UK, together with countries in the Nordic and Baltic regions, noted growing cooperation to detect and counter FIMI and agreed to further strengthen this cooperation at the Aurora Forum.
6. We have also continued to take specific action to disrupt information threat networks and actors upstream, at source. In May, the UK imposed sanctions on another 56 individuals and entities involved in activity to undermine Ukraine.¹ This action is testament to the government's commitment to combatting Russian malign interference worldwide. The May sanctions include employees of the Social Design Agency and ANO Dialog, FIMI entities designated by the UK in October 2024 which continue to be used by the Kremlin to run large-scale interference campaigns. We have also exposed for the first time the use of these organisations by the Kremlin to interfere in the Armenian elections in favour of pro-Russian figures.

1 <https://www.gov.uk/government/news/uk-targets-hostile-and-heinous-russian-activity-with-latest-sanctions>

7. The UK is determined to go further and faster to increase its capabilities and tools to illuminate and counter hybrid threats, including FIMI. We welcome the Committee continuing to share its insights and expertise as we work urgently to strengthen the Government's system for countering FIMI.
8. The Government recognises the Committee's concerns regarding reductions in UK ODA. As the Foreign Secretary set out in her statement to Parliament on 19 March, announcing ODA allocations for the period through to 2028–29, the reduction in the UK's international development budget was not an ideological choice but a difficult decision, required to support critical additional investment in defence, in light of an increasingly challenging global security environment.
9. The UK is not alone in having taken such a step. A number of our closest allies, including France, Germany and Sweden, have made similar decisions. The Prime Minister has also confirmed that the Government's intention remains to return to spending 0.7% of GNI on development assistance when fiscal circumstances allow. In the meantime, around 70% of the UK's still substantial development spending will be directed towards the most fragile and conflict-affected states, including Ukraine.
10. In addition, funding through the Integrated Security Fund (ISF) – a government-wide fund that addresses the highest priority threats to UK national security, at home and abroad – will continue. This includes support for efforts to counter FIMI, with multiyear funding profiles published for each region. While ISF allocations are published at portfolio level, the Government does not provide a more detailed breakdown to preserve operational flexibility and protect staff and delivery partners.
11. Finally, recognising the exceptional soft power value of the BBC World Service, Grant-in-Aid funding for the BBC World Service for the next three years has increased to £148 million a year. This means we have increased our contribution to World Service funding by 42% – up from £104.4 million in 2024/25 when this Government took office. In an era of widespread disinformation, this investment will support the BBC World Service to continue delivering impartial, accurate and trusted journalism around the world.

International

Ukraine

Recommendation 5: The Government should provide greater clarity on the progress made in implementing the One Hundred Year Partnership Agreement between the UK and Ukraine, including specific information on the operation and intent of Article 7, combatting foreign information

manipulation and interference. It should also set out what discussions, if any, have taken place with Ukraine regarding potential amendments to the Agreement in the event that a peace settlement with Russia is reached.

Agree.

12. We are committed to continuing to support Ukraine to counter Russian information operations and disinformation, including developing improved capabilities to respond to information manipulation. The UK's operational activity aimed at disrupting Russian FIMI networks and reducing their ability to generate and disseminate malign narratives at source forms a key part of this effort.
13. We have a strategic partnership with Ukraine through the UK-Ukraine 100 Year Partnership. In November, the first UK-Ukraine dialogue on FIMI took place to assess progress against our committed support and to explore opportunities for deeper co-operation. The Government will update the House as these dialogues continue.
14. All future discussions between the UK and Ukraine will be rightly guided by the commitments made in the 100 Year Partnership, part of the focus of which is UK programmatic support to strengthen Ukraine's ability to identify and disrupt hostile information operations.
15. The Government is committed to working with Ukraine to ensure that the 100 Year Partnership Agreement maintains its relevance in relation to discussions on security assurances, any potential ceasefire and any other issues relevant to Ukraine's future.

Eastern Europe, West Balkans and Caucasus

Recommendation 6: We call on the Government to implement new targeted financial and travel sanctions on Georgian Dream officials supporting the Foreign Agents Registration Act, Georgian kleptocrats and Georgian media organisation spreading disinformation. These additional designations would significantly increase the cost on those who are seeking to undermine the Georgian people's desire for a European alignment and signify the UK's support for Georgian democracy, not autocracy.

Partially agree.

16. The UK stands with the Georgian people's Euro-Atlantic aspirations, shares the Committee's serious concerns about democratic backsliding in Georgia and strongly condemns efforts to undermine fundamental freedoms, including through disinformation and repression of legitimate protest.
17. The UK has imposed sanctions on Georgian officials responsible for serious human rights violations, demonstrating that those who undermine democracy and repress peaceful dissent will be held to account.
18. In February, the UK sanctioned two Georgian-based television channels, Imedi TV and POSTV, for their prominent and sustained role in disseminating Kremlin aligned disinformation about Russia's invasion of Ukraine, assessed as undermining Ukraine's sovereignty and stability.² This demonstrates our firm commitment to combating FIMI in Georgia and FIMI targeting the Georgian diaspora.
19. The Government will continue to work closely with our international partners to support democratic resilience in Georgia, and to counter the FIMI threat, making use of the full range of tools at our disposal, including sanctions, in line with our values and relevant legal frameworks. However, we will not speculate on or comment on future sanctions designations as to do so could reduce their impact. Nevertheless, all sanctions decisions are taken based on robust evidence and kept under regular review.

Recommendation 7: The UK Government must support Moldova in its investigations into those actors which sought to undermine electoral integrity through cyber-attacks, fake bomb threats at polling stations and foreign information manipulation and interference campaigns. This includes the UK sanctioning individuals and organisations responsible. The UK must make clear that there are consequences for those who sought to deliberately interfere in Moldova's democracy.

Agree.

20. This Government recognises that Moldova remains on the front-line of Russian hybrid threats, particularly hostile information operations. As such, Russia's attempts to influence, subvert, and undermine Moldova's democratic processes during last year's elections were not unexpected.

2 https://assets.publishing.service.gov.uk/media/699c9dd4882eb23165f1277f/Sanctions_Notice__Russia__24_February_2026.pdf

21. We are proud of the support that we provided to support Moldova's efforts to safeguard its electoral integrity in the face of this interference – this included the UK imposing sanctions in April 2025 on Evrazia, a pro-Russia network of actors operated by exiled Moldovan oligarch Ilan Shor, that was seeking to destabilise Moldova's democracy and spread Russia's malign influence.³ In August 2025, the UK also imposed sanctions on a Russian cryptocurrency network, again connected to Shor and his company A7, both of which had been involved in information interference activities.⁴ We are pleased that this work was acknowledged by the Moldovan government and the Committee as valuable. We will endeavour to support the Moldovan government where possible with their investigations into those actors which seek to undermine the country's democracy.
22. The UK-Moldova Defence and Security Partnership, agreed in November 2024, contains specific joint actions to counter FIMI and to improve Moldova's resilience to hostile cyber activity. We are proud to support CyberCor, Moldova's national institute of cybersecurity innovations, to develop emerging talent and bolster Moldova's national cyber security. We look forward to continuing our work with the new Moldovan Government in support of our shared priorities in this area. Moreover, as set out in our response to recommendation 1, this Government recognises that a truly independent media and vibrant civil society are crucial to a functioning democracy. In Moldova the UK will continue to provide broader 'whole of society' support to increase institutional and societal resilience to hybrid threats.

Recommendation 8: Working with the European Union, the UK Government should scale-up assistance for independent media, civil society organisations and media literacy whilst continuing to monitor and expose foreign influence operations in these regions.

Partially agree.

23. The Government remains committed to working with the European Union to support the efforts of independent media and civil society organisations to combat state-sponsored information manipulation and interference in Armenia and the Western Balkans.

3 <https://www.gov.uk/government/news/campaign-to-tackle-dirty-money-steps-up-with-new-sanctions>

4 <https://www.gov.uk/government/news/uk-targets-sanctions-circumvention-and-crypto-networks-exploited-by-russia>

24. The Government strongly supports Armenia's desire to deepen its relations with the West. The UK, along with our international partners, including in the European Union, is supporting the Armenian Government to protect its democratic resilience and ensure elections that are free from malign interference. This includes work on how Armenia can protect itself against anticipated Russian attempts at information manipulation or interference that threaten the national security of both Armenia and the UK.
25. The Government is investing to counter FIMI in the Western Balkans and Armenia with support for independent media and civil society mechanisms. Please refer to our response to recommendation 1 for further information.

Cooperation with Europe

Recommendation 17: The Government should initiate the first UK-EU dialogue under the Security and Defence Partnership on foreign information manipulation and interference. The Government should also outline how it is using the Security and Defence Partnership and other bilateral agreements with EU partners to strengthen cooperation in detecting and responding to foreign information manipulation and interference to increase the cost for malign actors seeking to interfere in democracies.

Agree.

26. The Government has increased coordination with the European Union (EU) and EU member states to strengthen cooperation on hybrid threats, including FIMI, through the UK-EU Security and Defence Partnership.
27. The FCDO Minister for Europe, Stephen Doughty, represented the UK at a dedicated UK-EU consultation on hybrid threats with the European External Action Service (EEAS) and European Commission in Brussels on 15 September 2025 which sought to address shared security challenges, including information threats. Prior to this, on 4 September 2025, Minister Doughty, held the first formal UK-EU Consultation with the EEAS under the Partnership, focusing on Ukraine and the Western Balkans.
28. Through the UK-EU Security and Defence Partnership and bilateral agreements with our EU partners—including the Lancaster House Declaration signed with France at the UK-France Summit in July 2025, and the UK-Germany Kensington Treaty signed the same month—the UK will continue to strengthen collaboration with our European partners, recognising that FIMI is a global threat requiring a

global response. It is for this reason that we also intend to step up our ability to counter threats to our national security, including FIMI, as part of the new UK-Poland Defence and Security Treaty.

29. In responding to information operations, joint action with our European partners includes, but is not limited to, sharing information and analysis on the threat and potential responses, as well as coordinating sanctions and activities to deter and constrain FIMI actors, including by increasing the costs of engaging in such activity.

FCDO overseas network

Recommendation 19: The Government should in response to this report provide evidence to the Committee on how it utilises its overseas network to detect, defend and deter foreign information manipulation and interference and how these insights are informing policy responses.

Agree.

30. The FCDO is investing in upskilling its staff to work on FIMI, including through a dedicated training offer which has been rolled out at priority overseas Posts in FY25–26. This has included delivery in Europe, Africa and Latin America.
31. The FCDO leverages a network of more than 100 political officers across priority UK diplomatic missions to engage with host governments on the threat from FIMI, response options and opportunities to collaborate. In turn, reporting from our overseas network enables us to build a comprehensive picture of the global nature of the FIMI threat and seek further opportunities for cooperation with and learning from international partners.
32. We also leverage our overseas network to deepen dialogue with host governments and civil society actors on FIMI and develop initiatives to detect, defend against and deter FIMI in line with UK policy objectives. Having a skilled workforce, able to engage effectively in this evolving policy area in different geopolitical contexts, is critical to the success of the UK's international engagement and reach on FIMI.

US

Recommendation 11: These tensions underscore the need for continued diplomatic dialogue with the United States. Without such efforts, divergent approaches risk weakening collective work on combatting foreign

information manipulation and interference. In principle, the government should stand up for those countering disinformation, wherever in the world it occurs.

Agree.

- 33. The US remains the UK's closest security and defence partner. For this reason, we will continue to coordinate closely with them on shared national security threats.
- 34. The UK and US share a deep commitment to upholding freedom of speech and defending open democratic debate. The UK views information manipulation as a form of deception rather than legitimate discourse. We are focused on stopping hostile actors from misleading the public, not on regulating political views or lawful disagreement.
- 35. Decisions regarding the closure or funding of US institutions are matters for the US Government. It would not be appropriate for us to comment on these.

China

Recommendation 2: The Government must treat China the same as it treats any other state. It is therefore vital that the Government is transparent with Parliament and the public and outlines their strategy for engagement and the red lines for countering Chinese state influence, including the use of cyber-attacks and disinformation.

Agree.

- 36. We will not sacrifice our national security for economic growth. This red line was reiterated by the Prime Minister during his visit to China in January. The Government takes all threats to our national security seriously. Where we identify attempts to threaten our national security or democratic way of life, we will act; information threats are no exception to this.
- 37. We recognise the importance of raising public awareness of threats to the UK across the information, cyber, and physical domains. The Government is committed to being open about the nature of these threats, as well as responding proportionately. On 4 March, in his statement to Parliament, the Security Minister set out the Government's assessment of Chinese covert activity, and commitments to tackle this through the Counter-Political Interference and Espionage Action Plan.

38. Our approach to China remains consistent, we will co-operate where we can and challenge where we must. Refusing to engage with China would be a dereliction of duty, leaving British interests on the sidelines.

Recommendation 10: The Government must use all its diplomatic powers, alongside that of allies, to deter Chinese disinformation targeting Taiwan. The Government should expand its bilateral relations with Taiwanese officials and civil society groups to better understand the information environment within the Indo Pacific and sharing of best practice on countering foreign information manipulation and interference threats.

Partially agree.

39. As was acknowledged by Minister Doughty, in his oral evidence to the Committee, the Government is aware and concerned about reports from Taiwan's National Security Bureau that misinformation from China into the country increased 60% last year.
40. The Government engages with the Taiwanese authorities on a range of issues, and the UK will continue to support democratic values and media freedom in Taiwan, including through engagement with Taiwan's vibrant network of civil society organisations.
41. The UK considers the Taiwan issue one to be settled by the people on both sides of the Taiwan Strait through constructive dialogue and firmly opposes any activity – including information manipulation or misinformation – that undermines peace and stability in the Taiwan Strait and the free and fair operation of democratic processes. We are supportive of work that strengthens key democratic actors and that contributes to societies that are better equipped to address emerging threats, build public trust and uphold democratic values.

Iran

Recommendation 3: The Foreign, Commonwealth and Development Office Hybrid Threats Directorate should draw upon capabilities within the Department's Iranian regional teams to develop programming to counter foreign information manipulation interference campaigns emanating from Iran.

Agree.

- 42. This Government is committed to protecting the UK against hostile activity from Iran. The UK has an established toolkit to deter and respond to a range of threats, including through the National Security Act and the Foreign Influence Registration Scheme (FIRS), under which Iran is designated in the ‘Enhanced Tier’.
- 43. The UK continues to take action to hold the Iranian regime to account; we have sanctioned 36 individuals and entities in relation to malign and destabilising Iranian activity.
- 44. The Government supports the Committee’s recommendation to draw on our existing capabilities as part of our response and recognises the well-established regional expertise within the FCDO Iran Unit. The Unit’s deep experience in Iranian tactics, techniques and procedures continues to prove vital in informing the Government’s wider approach to countering state threats. Indeed, close joint working between the thematic and geographic teams within the FCDO is central to the range of work and delivery across the Department.

Non-state actors

Recommendation 4: The Government should review its work through the Counter Daesh Communications Cell to ensure it is producing messaging that appeals to potential recruits. It should also increase efforts to identify credible partners on the ground who are best placed to deliver counter-Daesh narratives.

Disagree.

- 45. We remain confident that the CounterDaesh Communications Cell (CDCC) continues to make a meaningful contribution through its coordination role within the Global Coalition against Daesh.
- 46. The FCDO’s CDCC delivers crucial strategic communications campaigns to challenge Daesh and al-Shabaab disinformation narratives. A core objective of the Cell’s work is to reduce vulnerabilities to Daesh radicalisation and recruitment, delivered through a combination of online and on-the-ground interventions.
- 47. Through this, the CDCC’s strategic communications have successfully supported wider efforts to reduce Daesh’s influence, including as part of the Global Coalition against Daesh. The CDCC has reached audiences in the tens of millions, contributing to a sustained reduction among local communities in support for Daesh, and increasing public trust in legitimate authorities.

48. We are confident that we have established an extensive network of credible partners, enabling us to reach vulnerable communities and deliver targeted communications to strengthen local resilience to Daesh's disinformation. We will continue to review programme effectiveness and delivery, consistent with FCDO-wide spending frameworks and processes. Further detail on the CDCC's work with partners can be provided privately to the Committee through appropriate classified channels. This assessment is based on our own monitoring and evaluation of delivery and reflects sustained feedback from external partners who have a high degree of visibility of the CDCC.

Recommendation 13: Given the importance of combatting foreign information manipulation and interference, it is unacceptable that the Foreign, Commonwealth and Development Office is presently under-resourced. The Government should immediately rectify this by utilising the funds associated with the defence uplift to increase funding and staffing within the newly formed Hybrid Threats Directorate. The Foreign, Commonwealth and Development Office must have the necessary resources to ensure their critical work can be conducted across all regions of interest and take forward this ministerial priority.

Partially agree.

49. This Government shares the Committee's concerns about the scale and severity of the challenge to the democracy and security of the UK and that of our international partners. We are committed to going further and faster to defend ourselves and our allies by limiting the impact of information threats.
50. The Department has ensured that the allocations we have received are targeting the threats and challenges we face, including a key focus on countering hybrid threats including cyber attacks, election interference, and FIMI. This demonstrates the Government's firm commitment to countering the growing scale and sophistication of FIMI. It also underlines the FCDO's commitment to continue modernising its capabilities through to 2030 and beyond.
51. We will continue to prioritise our resources on targeting information networks propagating FIMI activity at source, as well as driving concerted international action with our closest partners. Hybrid Threats Directorate has been allocated a non-ODA budget for this spending review period that enables sustained and more effective action to counter hybrid threats.

Recommendation 9: The Government should set out how it will ensure that reductions in overseas development aid and integrated security fund programming do not facilitate a vacuum that can be exploited by malign

actors seeking advantage in Africa. We urge the Government to ensure appropriate funding is available to ensure resilient and sustainable independent media organisations are able to thrive across the African continent.

Partially Agree.

52. This Government remains steadfast in its commitment to media freedom in Africa and around the world, and we recognise the vital role that journalists play in upholding human rights, supporting accountable governance, and protecting democracy. We have already taken significant steps to protect and promote media freedom globally.
53. In March, the UK took on the co-chair role of the Media Freedom Coalition (MFC). The MFC has an important role to play in strengthening independent journalism, protecting journalists at risk, and addressing emerging digital threats, including in Africa. At a time when independent public interest media is facing multiple threats, from intimidation and censorship to disinformation and financial pressures, we will use our role as co-chair to help the Coalition step up its response.
54. Recognising that influence is not determined by the scale of aid alone, the Government has also committed to a new approach to Africa centred on building modern partnerships that bring mutual benefit. There have been 32 visits by FCDO ministers to Africa since July 2024, including five visits already this year across Mozambique, Somalia, Ethiopia, the DRC, and Chad; our programmes reflect the UK's role as a partner, investor and champion of reform, demonstrating this new approach in practice.
55. Working with our African partners to support and protect independent media and wider media freedoms in their countries will form part of this new approach, with funding decisions kept under regular review. In recognition of the increasingly dangerous and volatile world we face, and given budgetary constraints, the ISF will focus its resources on delivering the top priorities within the National Security Strategy. In line with this approach, though the ISF has streamlined delivery and consolidated programming in Africa, it will continue to directly counter malign state and hybrid threat activity and bolster the resilience of our African partners.
56. In addition to support for independent media, we also want to highlight government action to disrupt information networks identified as operating in Africa. For example, in July 2025, we imposed sanctions on the African

Initiative, a social media content mill established and funded by Russia and employing Russian intelligence officers to conduct information operations in West Africa.⁵

Recommendation 12: The Government must work with regional partners in Latin America to support independent media and strengthen cooperation with trusted civil society organisations recognising that instability in Latin America directly affects UK diplomatic, trade and security interests and should not be treated as peripheral to the Government's counter-FIMI strategy. The Government should ensure it has the required capacity to monitor the growing threat of foreign information manipulation and interference in the region. The Government should report to this Committee within six months on how it will strengthen UK monitoring, diplomatic engagement and democratic resilience partnerships in Africa, the Indo-Pacific, Europe and the Americas.

Partially Agree.

- 57. The global information environment is becoming increasingly contested. The information threats we face do not respect borders – the same malign actors employ similar tactics to target the UK and our international partners alike.
- 58. Responding to this challenge requires close coordination with partners across regions to identify malign information activity, tackle the networks responsible for this activity at source, and to strengthen our collective resilience. The FCDO has therefore been scaling up our response across geographies most affected by this activity.
- 59. The Government has so far prioritised action to tackle Russian FIMI targeting the UK and our European partners, in particular Ukraine, given the acuteness of the threat of Russian information warfare. However, the FCDO is also engaged in strengthening resilience to hostile information activity in Latin America. This includes utilising our internal analytical capabilities to monitor and identify FIMI activity in the region, alongside engagement with regional partners to strengthen their resilience to information threats. For example, the UK has funded civil society initiatives to strengthen media literacy and fact-checking skills, so organisations can spot false narratives and support democratic debate. The UK has likewise engaged directly with governments in the region to raise awareness of the threat.

5 <https://www.gov.uk/government/news/uk-sanctions-russian-spies-at-the-heart-of-putins-malicious-regime>

60. This Government remains steadfast in our commitment to countering and reducing the impact of hostile information activity affecting our partners. We agree to update the Committee through a verbal briefing session on our international approach to monitoring, diplomatic engagement, and resilience building efforts in response to FIMI.

Recommendation 14: To show its continued commitment to media freedoms, the Government should again provide to the Committee six-monthly updates, including an assessment of threats to media freedom and the UK's response to foreign information manipulation and interference in priority regions.

Partially agree.

61. The FCDO has a longstanding commitment to protecting media freedoms globally. Media Freedom, in the form of a strong, robust, independent, local media, with a variety of voices, remains a priority for this Government.
62. We recognise the importance of keeping the Committee updated regarding this Government's work on media freedoms. While we review options for written reporting, we will provide periodic verbal briefing sessions for Committee members.

Recommendation 15: The Government must recognise that accurate, impartial news is essential to the UK's national security and overseas interests and should be treated by Government as a strategic national asset in an era of information warfare. At a time when the UK is reducing its Official Development Assistance and disinformation is spreading globally, the BBC World Service, is widely regarded as the world's most trusted international broadcaster. Whilst we welcome the additional funding being provided by the Government over the next three years, this is nominal increase but due to inflation is likely to be a flat settlement. Therefore, the Government should provide the BBC World Service with a further increased funding settlement, drawn in part from the defence budget, so it can plan, invest, and deliver its services effectively. It should also be made clear that funding from the Ministry of Defence would be provided with appropriate safeguards and commitments to ensure that the BBC World Service is able to continue to operate independent of Government. If the BBC World Service does not receive the funding it needs, it will continue to contract with a diminishing influence. Its loss would significantly diminish the UK's soft power and undermine our ability to counter information warfare.

Partially agree.

63. This Government agrees with the Committee's view on the vital role that accurate and impartial news plays in healthy and resilient media environments, including through the BBC World Service. As the Foreign Secretary made clear this March, "in a world of rising disinformation, the BBC World Service provides hundreds of millions with journalism they can trust and rely on. It offers clarity, accuracy and an independent voice where reliable information is increasingly difficult to access."
64. This is why the FCDO has increased funding for the BBC World Service to £148 million per annum. This is a real terms uplift over the period. This is a positive settlement in challenging fiscal circumstances and reflects the importance we attach to the World Service – as mentioned, this Government has increased its contribution to World Service funding by 42% since taking office.
65. The BBC has welcomed this settlement, which will enable the BBC World Service to grow its audience reach over the period of the Spending Review.
66. This Government is confident that the agreed funding allocation – which was informed by a comprehensive assessment of strategic priorities, affordability, and value for money – will enable the BBC World Service to continue to operate effectively and efficiently, and to provide trusted, impartial news to increased global audiences.
67. We note the Committee's recommendation for further additional funding to the BBC World Service over the next three years, drawing from the defence budget. We also note that the rules around what constitutes defence spending for the NATO target are very stringent. The BBC Charter Review is considering potential World Service funding mechanisms for the longer-term, and we cannot get ahead of that process.
68. Respecting BBC editorial and operational independence, the Government will continue to engage with the BBC on World Service priorities and performance, including on innovation and adaptation to evolving information threats. The Government highly values the work the BBC World Service does as an independent and trusted broadcaster, showcasing the UK, our culture, and our values around the globe.

Russia

Recommendation 1: The UK must prioritise existing funds for civil society organisations and independent media to enhance their resilience and capacity across Europe, but especially around the Black Sea Region and the Western Balkans, to stem the flow of Russian influence and aggression.

It should also step-up its counter foreign information manipulation and interference offering to allies in the Black Sea Region to ensure Russia cannot succeed in its attempts to influence election results. Failure to do so risks the potential for breaches of human rights and limits democracy. This would further threaten direct confrontation with NATO and European security.

Agree.

- 69. We are acutely aware that countries in the Black Sea Region and the Western Balkans are a target for Russian FIMI, including disinformation, aimed at undermining democratic progress and Euro-Atlantic integration.
- 70. Given the nature of the threat, the UK is investing to counter FIMI, including disinformation, in both these regions. For example, the UK is supporting civil society and independent media in Bosnia and Herzegovina (BiH), to build resilience against disinformation and malign foreign influence and enable alternative narratives. We are working in partnership against FIMI through support to investigative media in BiH and Armenia to provide objective, factual information regarding foreign interference.
- 71. The UK provided the Moldovan government with significant support ahead of their elections last year, to help secure these against Russian interference. This included funding to support cyber resilience, increase media literacy and institutional resilience to hybrid threats, and to identify and counter information manipulation and interference that threatened to undermine Moldova's democratic processes. We look forward to continuing our work with the new Moldovan Government in support of our shared priorities in this area under the UK-Moldova Defence and Security Partnership which includes specific joint actions to counter hybrid threats and FIMI.
- 72. As underscored throughout this response, this Government recognises that a truly independent media and vibrant civil society are crucial to a functioning democracy. We will continue to provide support to independent media organisations and civil society groups operating in countries in the Black Sea Region and the Western Balkans. In this vein, the UK, along with our international partners, are engaging on how to support the Armenian government to safeguard their upcoming elections and democratic resilience, including on how Armenia can protect themselves against anticipated Russian attempts at information manipulation or interference, in the forthcoming elections and democratic processes.

Domestic

Governance

Recommendation 18: To ensure a whole-of-society approach, the Government should establish a public-facing National Counter Disinformation Centre. The UK's National Counter Disinformation Centre should be placed on a statutory footing, be subject to oversight by Parliament, and be directed to understand, identify and combat foreign information manipulation and interference campaigns being directed against the UK and its interests. The National Counter Disinformation Centre should be similar to Sweden's Psychological Defence Agency, Ukraine's Center for Countering Disinformation, and France's Vigilance and Protection against Foreign Digital Interference service (VIGINUM).

Partially agree.

- 73.** The Rycroft Review has reported on the barriers facing the Government when it comes to adopting a fully joined-up approach to countering foreign information threats.
- 74.** We recognise these conclusions and have been working across Government to strongly cohere the government's approach to address this pressing national security challenge.
- 75.** We note the Committee's suggestion, and will take it into account alongside the conclusions of the Rycroft Review, and the lessons we can learn from our allies, including those highlighted by the Committee.

Public awareness of threat

Recommendation 20: The government should launch a public awareness campaign to educate citizens about the risk of foreign information manipulation and interference. This should include the measures taken and mechanisms in place to protect democratic institutions. Additionally, the Foreign, Commonwealth and Development Office should launch a publicly accessible information portal to document the scale and aims of disinformation campaigns, similar to the European External Action Services' highly-effective EUvsDisinfo resource.

Partially agree.

76. We agree that increasing public understanding and awareness of the nature of the threats plays an important role in building societal understanding of and resilience to the threat of FIMI, including disinformation. We will continue to highlight the nature of the threat, including through the publication of information on the gov.uk website about UK action to counter FIMI. To date, FCDO has published on gov.uk its action to counter FIMI including exposing the threat from Russia, Russian attempts to subvert democratic processes in Moldova, and the activity, and sanctioning, of several individuals and entities conducting FIMI in the UK and Europe. Alongside awareness raising on the risks of foreign information manipulation and interference we are pursuing media literacy initiatives as these are also critical to building societal resilience to mis- and disinformation. The government's 'You Won't Know Until You Ask' campaign promotes the core media literacy skills and behaviours which are effective regardless of whether content is foreign-backed or domestically generated. We are considering options to extend or adapt the campaign, including whether it could address FIMI.

Recommendation 21: Where examples would resonate with the public, the Government and the National Security Community should declassify information relating to foreign information manipulation and interference. In addition, the Government should provide Parliamentarians and other key stakeholders (e.g., civil society organisations and media organisations) with regular briefings on their work to combat foreign information manipulation and interference as well as training to identify and report disinformation campaigns. This should mirror the offerings provided by the National Cyber Security Centre for cyber security and resilience.

Partially agree.

77. We share the Committee's objective of improving awareness of FIMI and support greater resilience and public literacy.
78. The UK has a track record of publicly exposing actors propagating FIMI and their tactics, techniques and procedures. Since October 2024, the UK has exposed and sanctioned 96 actors engaged in FIMI.
79. In December 2025, during her Locarno Speech, the Foreign Secretary exposed Russia for engaging in information warfare against the UK and Ukraine and announced action to counter this. This May, the UK went even

further to sanction and expose 56 additional interference actors for delivering Russia's information warfare. As part of this, the FCDO published details of this destabilising activity and the actors responsible on gov.uk.⁶

80. We recognise the importance of regular engagement with key stakeholders including Parliamentarians, the private sector and civil society organisations, in strengthening collective awareness of and resilience to FIMI. Building on existing engagement and outreach, the FCDO will continue to work across Government to enhance information sharing and stakeholder engagement on hybrid threats, including through briefings and media freedom initiatives. We will continue to make judgements on correct way to provide briefings ensuring we are protecting sensitive information and handling appropriately.
81. The FCDO will continue engagement with the National Cyber Security Centre to understand best practice and consider how relevant lessons can be applied, including on providing briefings where appropriate, on efforts to counter FIMI, while recognising that approaches to countering FIMI must reflect the distinct nature of information threats.

Media Literacy

Recommendation 22: The Government must not overlook media literacy as part of its all-of society approach to strengthening and securing the UK's national security, including foreign information manipulation and interference from malign actors. The Government should seek to learn best practice from Baltic and Nordic countries and apply them to the UK, ensuring its approach focuses on all ages, not just the under-16s.

Agree.

82. The Government recognises that media literacy is an important part of building societal resilience to FIMI, where foreign influence is spread through mis- and disinformation. We know that while foreign interference differs in its source, it often takes the same recognisable forms of misleading or manipulative content. As a result, the core media literacy skills and behaviours, such as questioning the origin of information, assessing credibility, recognising emotional or identitybased manipulation, and verifying information before sharing, remain effective regardless of whether content is foreignbacked or domestically generated.

6 <https://www.gov.uk/government/news/uk-targets-hostile-and-heinous-russian-activity-with-latest-sanctions>

- 83. DSIT's 'You Won't Know Until You Ask' campaign promotes these core media literacy skills and behaviours by advising parents to teach their children to pause, check facts, check who posted the content, and consider if the content is AI generated.
- 84. This campaign is now being evaluated to assess its impact and to inform next steps. As part of this, we are considering options to extend or adapt the campaign, including whether this could address specific risks, such as FIMI, whilst remaining focused on the techniques of actors engaged in this activity, and not attribution of this.
- 85. Given that FIMI is a global challenge, and the FCDO's extensive overseas network, referenced in our response to recommendation 19, we recognise the value of both sharing best practice and learning from our allies, which of course includes our Baltic and Nordic partners.
- 86. We agree that social media platforms have a critical role to play in promoting media literacy. DSIT engages directly with platforms on media literacy where appropriate, with Ofcom playing an important coordinating role under its Online Safety Act duties.

UK Domestic Legislation

Recommendation 23: The Government should require social media companies to publish algorithmic transparency data (logic and biases), provide legitimate data access to researchers free of charge and without cumbersome restrictions, and oblige platforms to publish an annual report on the detection of artificial amplification and foreign interference and the subsequent actions taken to remove such content.

Partially agree.

- 87. We acknowledge concerns about the role of algorithms in amplifying harmful content, as set out in the Government's response to the Science, Innovation and Technology Committee's report on social media, misinformation and algorithms in September 2025. With this in mind, the Online Safety Act already gives Ofcom the power to request information on algorithm design, including as it relates to illegal mis- and disinformation.
- 88. We also agree that social media companies should provide legitimate data to researchers. This government has legislated to allow for a Researcher Access to Data Scheme, allowing for the first time independent researchers to have access to what has previously been private company data. We will be

consulting on how to operationalise this scheme later this year before bringing forward regulations for both Houses to approve. This is in addition to Ofcom's existing extensive powers on information gathering and transparency.

Recommendation 24: The Government should conduct an urgent review of the National Security Act 2023 Foreign Interference Offence, a priority offence under the Online Safety Act 2023, to ensure it is fit for purpose given the difficulties in meeting the foreign power condition.

Disagree.

89. The National Security Act 2023 provides law enforcement and the intelligence agencies with the tools they need to deter, detect and disrupt modern day state threats, including foreign interference.
90. The Foreign Interference Offence which the Act introduced has been carefully designed to target malign activity carried out for, on behalf of, or intended to benefit a foreign power that seeks to undermine the interests of the UK, our institutions, political systems, or rights and freedoms.
91. As the Act was introduced in 2023, it is still relatively new. Consequently, the powers it contains, including the Foreign Interference Offence, have not yet been robustly tested. There is a live case currently before the courts which should help clarify how these operate in practice, enabling evidence-based judgements on their efficacy.
92. The Government keeps all legislation under review and will carefully consider how the Online Safety Act and National Security Act interact as they are enforced. This includes working closely with Ofcom on the implementation of platform duties on Foreign Interference Offence content under the Online Safety Act, where we continue to explore how relevant information could be shared to support Ofcom in ensuring its codes are iterative and reflective of the evolving evidence base.
93. It is also important to note that platforms' responsibilities under the Online Safety Act only require them to have "reasonable grounds to infer" content is Foreign Interference in order to tackle it, which is a lower standard than the criminal threshold required for the offence under the National Security Act.

Recommendation 25: We welcome the Government's proposals to explore options to address potential digital replica harms including whether a new statutory regime of personality rights may be appropriate to

protect individuals against the threat of deepfakes. At a minimum, the Government should ensure these personality rights cover a person's likeness, voice and body.

Partially agree.

94. We acknowledge the Committee's concerns about the potential harms created by digital replicas. We simultaneously recognise that digital replicas can be a powerful tool, including for the creative industries, but real-world harm can be caused by someone's likeness being replicated without their permission.
95. We agree with the Committee that this is an important area of work requiring further investigation. It is for this reason that in March 2026, the Secretary of State for Science, Innovation and Technology, Liz Kendall MP, announced that the Government will launch a consultation in the summer. The consultation will seek views on how we address potential harms from digital replicas, while protecting legitimate innovation and freedom of expression. We would encourage the Committee to share their expertise as part of this consultation once it launches.

Recommendation 26: The Government should amend the Online Safety Act to oblige social media companies to provide transparency of user location. This should include publicly available information about 1) the region an account was created; 2) the region the account is based; and 3) whether the connection to the platform was via a Virtual Private Network (VPN). Social media companies should also be obliged to provide an opt-out function to safeguard users under the threat of transnational repression.

Disagree.

96. The Online Safety Act provides one of the strongest online safety frameworks in the world, placing clear duties on platforms to tackle illegal content, including electoral offences, harassment and abuse, and related harms, including where it is AI-generated.
97. There are legitimate reasons for people to use VPNs, including protecting their privacy and keeping personal data secure. The use of a VPN does not automatically indicate malicious activity, nor does the lack of a VPN connection guarantee confidence in an account's declared location. The Government continues to monitor the use of VPNs on the effectiveness of the Online Safety Act and will consider other options if necessary. Any intervention must be proportionate and evidence based.

98. We recognise and are concerned about the threat of transnational repression online but are confident that the Online Safety Act strikes the right balance in requiring platforms to mitigate against online behaviours, including threats to kill, harassment and stalking, controlling or coercive behaviour and communications offences (threatening or false communications), commonly associated with transnational repression. Nevertheless, the Government will continue to keep the Online Safety Act under review to ensure it is fit for purpose.

Recommendation 27: The Government should include provisions in the Representation of the People Bill that tackle AI-generated content, the creation and dissemination of disinformation, limits on the potential abuse of social media algorithmic biasing for political advantage, and a ban on cryptoasset donations to political parties.

Partially agree.

99. The Representation of the People Bill is a landmark piece of legislation which will ensure everyone has a voice in our democracy. It is the boldest and most ambitious change to our democracy for decades.
100. As set out in our response to recommendation 25, recognising the importance of addressing this and related risks, the Government will launch a consultation in the summer to seek views on how we address potential harms from digital replicas, while protecting legitimate innovation and freedom of expression.
101. DSIT will also establish a Taskforce to put forward proposals for government on best practice for labelling AI-generated content, with an interim report to be published in Autumn.
102. We acknowledge concerns about the role of algorithms in amplifying harmful content. That is why the Online Safety Act gives Ofcom the power to request information on algorithm design, including as it relates to illegal mis- and disinformation. While the OSA provides one of the strongest online safety frameworks anywhere in the world, including protections against illegal content, such as illegal election-related disinformation, we must ensure that protections keep pace with evolving threats, including to UK democracy. The Government will continue to actively review the framework to understand where the Act can be strengthened through evidence-based measures.
103. Finally, we have accepted the recommendation in the independent Rycroft Review, published in March, to impose a moratorium on the use of crypto assets as political donations, to safeguard the integrity of our political finance system from foreign interference. We will implement this measure

through the Representation of the People Bill and apply it retrospectively so that any political donations made in crypto assets from 25 March must be returned. With this policy, we are taking decisive action to defend the legitimacy and integrity of our democratic system from foreign interference.

Artificial Intelligence (AI)

Recommendation 16: The Government should establish an AI counter disinformation sandbox to test the boundaries of regulation and technology. The sandbox should facilitate experimentation of AI tools across Whitehall, the intelligence community and trusted international partners.

Partially agree.

- 104. We know that Artificial Intelligence (AI) is already being used by states as a tool to conduct information manipulation and interference. This includes the generation of AI deepfakes of politicians and other high-profile figures, including around elections, to spread disinformation and distort the truth.
- 105. As well as the potential for AI to be harnessed by our adversaries for malign activity, we also recognise that AI has great potential to be used positively, including in the detection, monitoring and disruption of FIMI. The FCDO continues to keep its capabilities under close review.
- 106. The Government has already established AI sandboxes, such as the AI Growth Lab, which has been designed as a safe space for regulators and businesses to test AI products and identify where current rules might hinder innovation. In response to the AI Action Plan, the Government committed to work with regulators to boost their capabilities. The Government has been clear that we will legislate where necessary, guided by evidence and where there are demonstrable gaps.
- 107. In line with the Committee's recommendation, we will assess the existing AI sandboxes and their utility and use this to scope whether a bespoke AI counter disinformation sandbox would be useful rather than duplicative.