House of Commons

Foreign Affairs Committee

Encoding values: Putting tech at the heart of UK foreign policy

Third Report of Session 2022–23

Report, together with formal minutes relating to the report

Ordered by the House of Commons
to be printed 5 July 2022

HC 170
Published on 8 July 2022
by authority of the House of Commons

Foreign Affairs Committee

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

Current membership

Tom Tugendhat MP (*Conservative, Tonbridge and Malling*) (Chair)

Chris Bryant MP (*Labour, Rhondda*)

Liam Byrne MP (*Labour, Birmingham, Hodge Hill*)

Neil Coyle MP (*Labour, Bermondsey and Old Southwark*)

Alicia Kearns MP (*Conservative, Rutland and Melton*)

Stewart Malcolm McDonald MP (*Scottish National Party, Glasgow South*)

Andrew Rosindell MP (*Conservative, Romford*)

Bob Seely MP (*Conservative, Isle of Wight*)

Henry Smith MP (*Conservative, Crawley*)

Royston Smith MP (*Conservative, Southampton, Itchen*)

Graham Stringer MP (*Labour, Blackley and Broughton*)

Claudia Webbe MP (*Independent, Leicester East*) was also a Member of the Committee during this inquiry.

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

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

Committee staff

The current staff of the Committee are Medha Bhasin (Second Clerk), Hannah Finer (Committee Specialist), Ken Davies (Committee Specialist), Clare Genis (Committee Operations Manager), Jonathan Hingston (Committee Specialist), Alice Lynch (Committee Specialist), Antonia McAndrew-Noon (Senior Media and Communications Officer), Chris Shaw (Clerk), Daniela Sindrestean (Committee Operations Officer).

Contacts

All correspondence should be addressed to the Clerk of the Foreign Affairs Committee, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 6106; the Committee's email address is fac@parliament.uk.

You can follow the Committee on Twitter using @CommonsForeign.

Contents

Summary

New and emerging technologies are fundamentally altering the nature of international relations and the role of the nation-state, as well as forming new arenas in which battles for global influence play out. The growing influence of private technology companies is challenging traditional levers of state influence and channels of diplomatic engagement. In addition, global technology standards are increasingly a tool for geopolitical competition as authoritarian governments seek to gain technological dominance and to shape global standards based on their preferred governance models.

The UK Government has explicitly stated its intention to position the UK as a "science and technology superpower". The developments outlined above require the Foreign, Commonwealth and Development Office (FCDO) to fundamentally reassess the ways in which it projects the UK's influence, builds alliances, engages with our competitors, and works with allies to control the firms and technologies that pose a risk of exporting data and technology to our adversaries. Failure to adapt will have devastating consequences for our security, prosperity and global influence, as well as threatening the privacy and liberties of people in the UK and across the world.

There is an opportunity for the FCDO to exemplify the values articulated in the Integrated Review by leading on collaboration with the private sector and civil society, both in the UK and overseas, in the pursuit of its objectives. It is now vital that the FCDO works across Government to ensure there is a single picture of those firms and adversaries who pose a risk to the UK, and that the Government is using the appropriate controls to disrupt the efforts of those who wish us harm. This should include engaging with local product teams and technologists to understand the localised impact of technologies in communities across the world. The Government can also influence global best practice, for example by sharing knowledge of the National Cyber Security Centre (NCSC) and drawing upon the expertise of our world-class research organisations, companies and institutes.

The UK's position on technology standards vis-à-vis the US and EU remains unclear and the UK is being left out of important technology cooperation initiatives. The UK therefore risks becoming a rule-taker rather than a rule-maker on technology standards. We also cannot meaningfully influence the global order without the cooperation and support of our partners. While there is an opportunity for the UK to exercise thought leadership, we cannot go it alone and should not seek to carve out a "fourth way" for the UK in global technology governance. The Government's continued focus on bilateral technology agreements is creating incoherence and fragmentation, thus failing to provide a strong and cohesive alternative to authoritarian technology governance models. There is an opportunity for the FCDO to leverage its diplomatic influence and wider relationships to promote mutual understanding among the world's different regulatory blocs, in order to facilitate a cohesive international approach to technology governance, based on the shared values of democracy, openness and human rights.

"Digital deciders" such as India, Singapore and Brazil are yet to fully align themselves with rights-based or authoritarian technology governance models. This is recognised and reflected in the diplomacy of the Chinese government. Together with our allies, creating deeper partnerships with these countries will be crucial to shaping the

future of the global technology landscape. The UK Government should increase its diplomatic efforts with countries who might otherwise align with models of digital authoritarianism, including by offering trade and investment opportunities in support of technologies that support democratic values and human rights.

The integration of technology within UK foreign policy should reflect the intrinsic links between the UK's domestic capabilities and its global influence. The Government's previous reticence to review and intervene in foreign investments that move strategically important UK businesses overseas has slowly eroded our domestic capabilities, with implications for our ability to project influence internationally. Better integration of work between departments, to support greater coherence between the UK's domestic industrial and economic policy and its foreign policy, will be crucial if the UK is to realise the Government's international ambitions.

Introduction

1. New and emerging technologies are fundamentally altering the nature of international relations and the conduct of diplomacy. The growing influence of private technology companies and the backing some nation-states can give them, increases the number of actors governments must engage with, challenging traditional levers of influence and channels of diplomatic engagement. Global technology standards and regulations are increasingly an arena for geopolitical competition: democracies are faced with increasingly assertive authoritarian governments seeking to gain technological dominance and to shape global standards based on their preferred governance models.

2. These developments present significant challenges to the UK's security, prosperity, diplomatic relationships and global influence. They also offer new opportunities for innovation in the way that the Foreign, Commonwealth and Development Office (FCDO) projects the UK's influence, builds alliances and engages with our competitors. The UK Government has explicitly stated its intention to be a world leader in shaping international rules and behavioural norms relating to new technologies and has prioritised investment in cutting-edge technologies and positioning the UK as a "science and technology superpower".[1]

3. In this context, in March 2021, we launched an inquiry into technology and the future of UK foreign policy. Our aim was to examine the implications of new and emerging technologies for the practice of foreign policy and what the FCDO is and should be doing to adapt to these opportunities and challenges.

4. During this inquiry, we took oral evidence from foreign policy and technology experts, technology companies and industry associations, civil society organisations, diplomats from the foreign ministries of other nations, and FCDO ministers. We also received 41 submissions of written evidence. We thank all these contributors for their engagement.

5. This report sets out our recommendations for how the FCDO can adapt to, and maximise its influence within, the new global strategic landscape that is being shaped by the development and use of technology. **Chapter Two** explores the different ways in which technologies are changing the role and influence of the nation-state, the spaces that private companies and non-state actors are occupying in geopolitics and diplomacy, and what this means for the FCDO's ways of working and whom it should be engaging with. **Chapter Three** examines growing geostrategic competition over technology standards and regulations in the context of a fragmented global technology landscape, and the prospects for the FCDO to facilitate cooperation amongst democracies and engagement with digital deciders to counter the influence of authoritarian standardisation agendas. **Chapter Four** examines the interlinkages and areas of inconsistency between the Government's international and domestic policies when it comes to its global Science and Technology (S&T) leadership ambitions. In **Chapter Five**, we set out recommendations for how the FCDO can measure its progress in delivering on the Government's S&T ambitions.

1 Integrated review of UK security, defence, development and foreign policy

1 Shaping and adapting to the changing role and influence of the nation-state

> *Technologies are shaped by and express power relations; they can also transform power relations.*[2]

6. The 2021 Integrated Review of Security, Defence, Development and Foreign Policy (hereafter "Integrated Review") argued that the ability to advance and exploit S&T will be an important metric of global power in the coming decade, conferring economic, political and military power on those nations who are able to establish and sustain technological advantage.[3] Last year, the head of MI6 warned that the "digital attack surface" that criminals, terrorists and hostile states threats seek to exploit against us is "growing exponentially" and that China in particular seeks global leadership in AI by 2030 in order to master intelligentized warfare, build globally capable surveillance systems and automate disinformation. In particular, Sir Richard Moore warned that China was seeking to export both the data and technology from around the world "expanding the web of authoritarian control around the planet".[4] New and emerging technologies are fundamentally altering the function and practice of diplomacy, for example through social media and communications platforms that enable governments to engage with global audiences in new ways. Furthermore, power centres in the form of private technology companies and big data brokers such as Acxiom, Oracle Data Cloud and Verisk are changing the state-centric global order. Private-sector actors are increasingly occupying new spaces, notably by being increasingly engaged in co-designing and co-delivering new ways of providing diplomatic services and functions.[5] An example of this is the partnership between Microsoft Philanthropies and the FCDO around Common Data Models and Standards, which aims to facilitate the seamless sharing of data across global aid agencies.[6][7] More broadly, companies such as Google and Meta not only provide access to information but their algorithms also determine which information is seen and thus how countries and issues are perceived.[8] This raises new questions regarding which actors the UK engages with to exert its influence and requires the Government to take account of a changing global power distribution between nation-states and non-state actors.

7. Our inquiry identified the following ways in which new and emerging technologies are reshaping the character, dynamics and distribution of global power:[9]

- **"Democratisation" of technology** Many technologies are becoming both more affordable and more commercially available, increasing their accessibility to a wider range of state and non-state actors, who can leverage technological

2 TFP0026
3 TFP0015; Integrated review of UK security, defence, development and foreign policy
4 Sir Richard Moore, Human Intelligence in the Digital Age - Speech by Richard Moore, Chief of the UK's Secret Intelligence Service, *International Institute for Strategic Studies*, 30 November 2021
5 Hamid Akın Ünver, Computational Diplomacy: Foreign Policy Communication in the Age of Algorithms and Automation 2017
6 TFP0017
7 The FCDO also has strategic partnerships with a number of private-sector companies, including through the Global System for Mobile Communications (GSMA) Association (which has over 800 members) and others including Unilever, Microsoft and Shell. See: TFP0015
8 TFP0036
9 TFP0036

advances for a wider range of purposes.[10] This phenomenon is commonly referred to as technology "democratisation". For example, online platforms have created new opportunities for global governance by facilitating easier access to knowledge, enabling democratic participation and freedom of expression.

- **Increased reliance on, and competition for access to and influence over, critical technologies,** such as semiconductors, 5G and 6G, AI- and AI-enabled technologies and cyber capabilities. The critical technologies underpinning our everyday lives are increasingly important as an arena of systemic competition between nation-states.[11] This trend has been intensified and accelerated by the Covid-19 pandemic, which has brought issues of supply chain resilience and technological self-sufficiency to the fore. Technology "superpowers" such as the US and China are investing to maintain their lead in areas such as semiconductors and communications technologies, and many other countries have announced significant investment in emerging technologies to bolster their post-pandemic resilience and, more broadly, to bolster their security, resilience and influence in a world where these technologies are critical to the functioning of society and the exercise of power.

- **Weaponisation and distortion of the information space** through new digital tools and platforms with new means for exerting influence. The same digital spaces that are democratising access to information are also being exploited for malign purposes, including exploitation of information for mis- and disinformation (proliferated by AI-enabled "bots"), propaganda, and recruitment of supporters by non-state armed groups.[12] Technologies that "distort the information space" and have subsequent effects on public trust and online civic culture such as deepfakes[13] are particularly concerning.[14] Deepfakes can be used to exploit or undermine public trust in the quality of information[15] or to coerce decision-makers or individuals with access to classified information.[16] "Information-distorting" functions are neither particularly complex nor difficult to deploy; for example, almost any smartphone user can create and disseminate seemingly authentic deepfake videos in seconds.[17] Witnesses suggested that democracies

10 TFP0036
11 TFP0015; Integrated review of UK security, defence, development and foreign policy
12 TFP0036
13 The Alan Turing Institute (ATI) defines deepfake technologies as "Synthetic audio, video or imagery in which someone is digitally altered so that they look, sound or act like someone else. Created by machine learning algorithms, deepfakes have raised concerns over their uses in fake celebrity pornography, financial fraud, and spreading false political information. 'Deepfake' can also refer to realistic but completely synthetic media of people and objects that have never physically existed; or sophisticated text generated by algorithms." See: The Alan Turing Institute, Data Science and AI Glossary
14 TFP0010
15 As a recent example, Russian disinformation campaigns in Ukraine have included the use of deepfake videos purportedly showing Ukrainian President Zelenskyy admitting defeat and surrendering to Russia. Matyáš Boháček
Matyáš Boháček and Hany Farid, Protecting President Zelenskyy against deep fakes, June 2022. A report by Europol published in April 2022 also highlighted the risk that deepfakes can be used to disrupt elections or undermine political institutions "by releasing a fake audio or video recording of a candidate or other political figure. See: disruption of elections or other aspects of politics by releasing a fake audio or video recording of a candidate or other political figure". Europol, Facing reality? Law enforcement and the challenge of deepfakes, p.11, 28 April 2022.
16 TFP0010; M. Caldwell, J. T. A. Andrews, T. Tanay & L. D. Griffin, AI-enabled future crime. Crime Science 9(14), 5 August 2020.
17 TFP0010

with open societies and a free press were more vulnerable to disinformation campaigns via social media, compared with countries with authoritarian governments.[18] Consequentially, the FCDO faces new challenges regarding how to mitigate the risks associated with the global proliferation of false or misleading information online.[19]

- **Speed, reach and volume of online information and communication.** The interconnectedness facilitated by online platforms and communications technologies has increased the number of actors in political and diplomatic processes, subsequently reducing the influence of foreign ministries and diplomats relative to that of online citizens.[20] Consequentially, the FCDO faces new challenges regarding the pace and reach of activities and structures through which it must exert influence. The huge volumes of online information and opinions now available to citizens are "weakening states' control over their nation's image, policy and branding."[21] The instantaneous nature of digital communication is also challenging traditional means[22] of diplomatic response to crises. While diplomacy has typically required careful, deliberative responses to crises, high-priority and high-risk political issues and events now proliferate rapidly online, far outpacing the ability of states to respond through traditional modes and policy processes.[23] Ministers now often respond instantly to events and announce policy decisions via social media, which circumvent the usual rigour of internal government discussions.[24]

- **New and expanded roles for private-sector companies.** Multinational corporations and non-governmental organisations are playing an increasingly prominent role in national strategies and geopolitics, either by directly shaping global governance through multilateral institutions or through national governments leveraging industry to develop partnerships and shape trade and

18 TFP0010
19 TFP0036
20 Google and Facebook, for example, each reach more of the UK's online population than the BBC. See: Pete Swabey And Martin Harraca, Digital power: how big tech draws its influence, *Tech Monitor*, 26 April 2022; Hamid Akın Ünver, Computational Diplomacy: Foreign Policy Communication in the Age of Algorithms and Automation 2017
21 Hamid Akın Ünver, Computational Diplomacy: Foreign Policy Communication in the Age of Algorithms and Automation 2017
22 Public communications in the digital age now often favour speed and timing, rather than accuracy. This is particularly true in times of crisis. This challenges traditional public diplomacy, which has typically involved careful and measured responses prior to the dissemination of information to the public. Ilan Manor, The Digitalization of Diplomacy: Toward Clarification of a Fractured Terminology, *Oxford Digital Diplomacy Research Group, University of Oxford*, 2018.
23 Hamid Akın Ünver, Computational Diplomacy: Foreign Policy Communication in the Age of Algorithms and Automation 2017
24 For example, the UK Defence Minister's tweet about the evacuation of Nowzad staff from Afghanistan in 2021 was interpreted by some FCDO officials as an official decision, which caused confusion. See: Ben Wallace, Twitter, 25 August 2021; Foreign Affairs Committee inquiry into Government policy on Afghanistan, Q521 (Nigel Casey) and Q532 (Sir Philip Barton,)

industrial strategies.[25] Private-sector actors are increasingly engaged in co-designing and co-delivering new ways of providing diplomatic services and functions.[26]

8. The following sections pick up on two of the major themes identified during the inquiry on the changing role of nation-states: namely, the new roles of private companies, and the subsequent need to adapt through technology diplomacy.

New roles for private sector companies

9. As outlined in paragraph seven, the world's major technology companies, such as Google, Meta, Amazon, Apple and Microsoft now wield unprecedentedly high levels of economic and social power. A new category of non-state multinational actors has been created, who play a critical role in national security, global stability and foreign relations.[27] For example, social media platforms are now the key actors facilitating the dissemination and internationalisation of narratives that shape global political, social and diplomatic discourse.[28] Russia's invasion of Ukraine in February 2022 has both exemplified and magnified the role that tech companies, infrastructure providers and social media platforms play during international crises.[29] These big tech companies own and maintain the digital platforms and services upon which governments now rely, such as communications platforms and infrastructure.[30] As a result, multinational companies now play central roles in the formulation of national strategies and the practice of geopolitics, helping to shape global governance through multinational institutions. Microsoft has now established diplomatic missions to the EU and UN and has spearheaded global diplomatic treaties such as the Paris Call for Trust and Security in Cyberspace[31] and the Rome Call for AI Ethics.[32] Governments are also leveraging industry to develop public-private partnerships (PPPs) to shape and deliver policy objectives, for example TRANSFORM, a PPP between the FCDO, Unilever and EY aimed at supporting the Sustainable Development Goals by working with impact enterprises to bridge the digital divide between the global north and south.[33] Moreover, Government departments are also reliant upon technology companies

25 The Downing Street meeting between then-Chief No.10 Advisor Dominic Cummings, the Prime Minister, and senior representatives from various big tech companies including Google, Facebook [Meta], Apple. Palantir, Amazon and Microsoft at the start of the Covid-19 pandemic is one example of technology companies being brought in to support Government decision-making in times of national crisis. One outcome of this meeting was that surveillance company Palantir was awarded large Government contracts to streamline data flows across the nation to support the Government's Covid-19 tracing and response. See: Gian Volpicelli, Inside Dominic Cummings's coronavirus meeting with big tech, *Wired*, 12 May 2020; Rodrigo Fernandez, How big tech is becoming the government, 5 February 2021.

26 TFP0036. For example, social media platforms and digital communication channels (such as WhatsApp) now act as "obligatory digital interfaces for social exchange", including for foreign ministries. Fernandez, How big tech is becoming the government, 5 February 2021.

27 TFP0026

28 TFP0027

29 Correspondence with Joe White, UK Technology Envoy to Silicon Valley, June 2022.

30 TPF0027

31 TFP0017

32 Alexis Wichowski, The US can't regulate Big Tech companies when they act like nations, *The Washington Post*, 29 0ctober 2020; Alexis Wichowski, Tech ambassadors are redefining diplomacy for the digital era, Tech Monitor, 16 February 2021; Simon Hansford, Boris Johnson stands at the edge of another Huawei saga if Amazon Web Services crushes UK cloud products, *City AM,* 18 June 2021; Sam Trendall, Unwrapping the government's 300m Amazon package, *Public Technology*, 7 May 2021.

33 Transform, Digital, with a human touch, 16 November 2021

for their very functioning; Amazon Web Services (AWS) for cloud hosting;[34] social media and communications platforms for internal communications and public diplomacy; and telecommunications companies for the maintenance of critical infrastructure.[35][36]

10. The Government's forthcoming International Technology Strategy, which is being jointly led by the FCDO and the Department for Digital, Culture, Media and Sport (DCMS),[37] is a promising indication that the FCDO is taking the foreign policy implications of emerging and disruptive technologies seriously. The FCDO's Director of Strategy and Engagement, Chris Jones, said the purpose of the strategy is "to set out the values that the UK and a network of partners want to see embedded in a technological sphere to set out the world we would like to see enabled by technology and ensure that is the model we pursue".[38] Yet while the FCDO acknowledged in evidence the importance of engaging with private sector companies, technological changes have implications that go beyond simply engaging with more actors: they require a fundamental reassessment of which spaces these private actors should occupy in global technology governance and service provision and what this means for the role of the nation-state. We are not persuaded that the FCDO is yet doing any meaningful thinking on the more fundamental question of what the growing influence and importance of these companies mean for its own role, or that of the Government, in diplomacy, security and other forms of public service provision. The forthcoming strategy presents an opportunity for the FCDO to articulate clearly its understanding of its future role and global influence, in the context of growing technology-centred geopolitical competition and shifting global power balances and roles. The forthcoming strategy also presents an important opportunity to set out a government-wide strategy for regulating foreign technology firms in four ways:

- A strategy aimed at helping UK firms partner with those can help us bolster and diversify our technology base;
- A defensive strategy of tighter China-oriented restrictions including geolocation data, social media platforms and consumer devices like smartphones;
- Military objectives like maintaining a military edge over China, limiting Chinese national security espionage, preventing Chinese sabotage in a crisis, limiting Chinese influence operations, and denying support for Chinese or China-enabled authoritarianism and repression;
- Economic objectives including countering unfair Chinese practices and intellectual property (IP) theft, and competing and leading in strategic industries.

It could also identify how the FCDO should work with key companies to promote democratic values and engage with partners and less economically developed countries to promote a values-based approach to technology development and use (see Chapter 3).

11. **The growing influence of private companies in global technology governance, and on the norms and rules that shape our societies, has profound implications for the**

34 Sam Trendall, Unwrapping the government's 300m Amazon package, *Public Technology*, 7 May 2021.
35 While this reliance in itself is nothing new, the range of technologies central to our critical infrastructure, and the degree of dependence on them, is growing; for example, cloud storage and broadband.
36 TFP0036
37 House of Lords Science and Technology Committee inquiry, Delivering a UK science and technology strategy, Q108 (Professor Charlotte Watts)
38 Q236 (Chris Jones)

future role and identity of the nation-state. The Government has yet to demonstrate that it has seriously considered its role and influence within this new environment and how it might manage the consequences of these shifts in influence and identity. ***In the forthcoming International Technology Strategy, we recommend that the FCDO clearly articulates what it understands its future role in global tech governance to be and how it intends to engage with private companies and relevant multinational bodies to project UK norms and values in global policy-making fora. We further recommend that the FCDO identifies a Minister with clear responsibility for this work within the Department and sets out how its work interacts with that of other Government departments.***

12. ***The UK's global technology leadership ambitions should be Government-led but will need to pull in significant support from the private sector as well as academia. There is an opportunity for the FCDO to exemplify the values articulated in the Integrated Review by leading on collaboration with the private sector and civil society, both in the UK and overseas, in the pursuit of its objectives. This should include working to ensure that the voices of smaller companies and less economically developed countries are heard in global fora. There is an opportunity for the Government to influence global best practice by sharing knowledge of the National Cyber Security Centre (NCSC) and drawing upon the expertise of our world-class institutes.***

13. ***The UK should work with allies to ensure global practice in frameworks designed to protect data, and to prevent our adversaries exporting data from around the world to build the massive data sets needed to develop algorithms to automate surveillance systems, military systems and disinformation systems. We need to think about data as a national security asset, which should be subject to an appropriate regime of export controls. Placing greater controls on the collection, aggregation and access to data available to China is a good first step to eliminating an obvious national-security vulnerability.***

Technology diplomacy

14. As discussed in the previous section, the changing global power distribution between governments and private actors requires rapid and effective adaptation by the FCDO. Recent measures taken by the FCDO make it clear that the Department is beginning to reassess the ways in which it engages with private-sector companies. In December 2020, the FCDO announced that it had appointed its first ever Technology Envoy to Silicon Valley,[39] a decision that had previously been called for by this Committee.[40] This role is a combined position of British consul-general in San Francisco and Technology Envoy, meaning that the Technology Envoy responsibilities constitute only half of the individual's role, and their remit is geographically specific to Silicon Valley. The role is therefore not as expansive as those of corresponding officials in countries such as Denmark and Australia,

39 Gov.uk, Joe White appointed HM Consul-General, San Francisco, and Technology Envoy to the USA , 4 December 2020

40 Correspondence with Dominic Raab MP, 13 January 2021.

who have established dedicated Technology Ambassadors[41] with global remits.[42] The FCDO has acknowledged that the Tech Envoy is a relatively new role and that "we need to take the time to look at the role, to ensure that it is working and see how we might enhance and evolve it", for example by exploring whether the current geographically-bound model or one with a roaming global remit is best suited to the UK.[43] Likewise the UK's current Tech Envoy, Joe White, told us that "my role as the UK's first Tech Envoy to the United States should be seen as a pilot from which to iterate to maximise impact for the UK across the globe".[44] In particular, simply establishing channels of communication between high-level policy personnel within the FCDO and Silicon Valley will not be sufficient for an effective technology diplomacy strategy that captures the full spectrum of issues and voices that must be considered and heard within global technology governance discussions. This is one area that should be considered by the FCDO when considering the future evolution of the Tech Envoy role. We look forward to seeing how the role evolves over time in order to support the FCDO's technology diplomacy most effectively.[45]

15. Products can have vastly different implications for users depending on the social, cultural and political contexts in which they are deployed. Witnesses to our inquiry emphasised that despite their global reach, large technology companies often have only a limited understanding of the specific and highly varied impacts of their products and services across different jurisdictions.[46] Technology companies generally have dedicated policy teams whom they deploy to engage with policymakers. Confining FCDO engagement to these dedicated personnel risks limiting understandings of the local and regional nuances that shape the effectiveness of different regulation and governance practices,[47] as well as how products and platforms[48] are used by different groups. The International Committee of the Red Cross (ICRC) emphasised that those developing technologies should adopt a "conflict-sensitive approach."[49] Such an approach would take into account the ways in which social media and surveillance, or communications technologies are implemented in conflict-stricken or unstable settings; for example, by facilitating government repression of protestors[50] or opposition groups or spreading incitements of violence and hate speech. The ICRC stressed that local civil society and media provide the essential contextual knowledge and cultural expertise needed to understand and document the local impact of products and services.[51] Understanding these local impacts, in turn, will be essential to inform the ways in which technologies

41 The specific responsibilities of technology ambassadors naturally vary from country to country, however, broadly speaking, the fundamental objective is to build understanding between governments and companies on geopolitical issues and to represent the values of citizens to the global tech industry. For example, Austrian tech ambassador Martin Rauchbauer has described his role as being that of "a translator between different worlds". Tech ambassador roles are also considered useful for implementing tech policy, particularly as governments struggle to devise coherent strategies for managing the power of big tech.

42 Strategy for Denmark's tech diplomacy 2021–2023; Q57 (Joe White); Q58 [Anne Marie Engtoft Larsen]

43 Q253 (Amanda Milling)

44 Correspondence with Joe White, June 2022

45 Correspondence with Joe White, June 2022.

46 Internews Europe (TFP0041)

47 RAND Europe (TFP0036)

48 A product is a consumable or usable piece of software (such as a computer of mobile phone) while a platform is a system that enables a product to work or communicate with another product (such as a social media app).

49 Q166 (Sarah Spencer).

50 For example, Amnesty International informed us that law enforcement authorities around the world have used facial recognition technologies to track down protestors, by using images captured through CCTV and other video surveillance devices and running them through facial recognition software to perform face analysis or search for potential face matches against a designated database. Amnesty international (TFP0005)

51 Internews Europe (TFP0041)

should be designed and rolled out in different jurisdictions, and what safeguards need to be put in place to mitigate their potentially harmful impact on local populations. Witnesses also noted that while high-level engagement with decision makers within companies is naturally desirable, FCDO access to product teams within companies is also critical, given where many of the concerns with technology design and implementation lie.[52] Should the FCDO primarily or exclusively engage with high-level policy teams in its tech diplomacy efforts, the localised effects of technologies (as described above) may not be captured. This would have consequences for the FCDO's ability to minimise harm to vulnerable populations and prevent conflict. In addition, engaging with regional teams would provide the FCDO with useful insights into the ways in which companies are using data and implementing technologies in these regions.[53]

16. ***We recommend that the FCDO prioritises engaging with product teams and technologists, rather than only policy teams, to gain a clearer understanding of the activities of companies that are developing and implementing new technologies, as well as helping to influence the activities of these companies. The Department will need to bring in and develop the internal skills and expertise it needs to effectively engage at this level***.

52 International Committee of the Red Cross (TFP0029)

53 Internews Europe (TFP0041)

2 The UK's place in shaping the international order

> *We need to decide what we want our technological future to be–that is the ultimate strategic challenge.*–Martijn Rasser, Center for a New American Security

Fragmentation of the global technology landscape and digital spaces

17. Witnesses to this inquiry repeatedly raised the issue of the bifurcation or fragmentation of the internet and global technology landscape.[54] Increasingly divergent perspectives on the norms and standards for internet governance and technology development are resulting in the emergence of competing visions for what the future technology landscape should look like and how it should be governed both at the national and international levels. While some witnesses referred to this phenomenon as the "splinternet",[55] the issue goes beyond fragmentation of digital spaces. In particular, we have heard loud and clear American policy makers explain how a 'partial decoupling' of U.S. and Chinese technology ecosystems is well underway and is set to accelerate. But we have also heard voices from the Indo-Pacific argue that such a decoupling is not seen as in their strategic interest. The UK must find a way of working in this new world.[56]

18. Concerns over supply chain resilience in critical sectors such as semiconductors, as well as those around the security and resilience of critical national infrastructure such as telecommunications, are driving a post-pandemic shift towards securing technology self-sufficiency or "technology nationalism".[57] China's "great firewall"[58] and Russia's increasingly similar model, the outflux of Western companies leaving Russia following the Ukraine invasion, and a growing shift towards indigenous industry demonstrate that this fragmentation is already here and that the shift towards it is accelerating.[59]

19. Increasing fragmentation of the international order is being expressed through technological developments. China's great firewall and Russia's internet censorship risk fragmenting the global internet and creating regionally-based international technology regulations. This splintering of the internet and global regulatory environment threaten the cohesiveness, interoperability and accessibility of the internet.[60] While this fragmentation is sometimes referred to as "bifurcation", involving competing democratic and authoritarian models, the reality is less binary. Democratic countries are also struggling to agree on many principles and standards in areas such as telecommunications infrastructure and data sharing. As these divergences from and between democratic models continue, the

54 RAND Europe (TFP0036); Q75 (Martijn Rasser); Q2 (Harriet Moynihan)

55 The term "splinternet" refers to a global internet architecture dominated by restrictive internet governance models driven by geopolitical conflict, and increasingly diverging perspectives on the norms and standards for internet governance and technology development. See: RAND Europe (TFP0036)

56 Jon Bateman, US-China technological "decoupling": A strategy and policy framework, Carnegie Endowment for International Peace, 25 April 2022

57 Marie Lamensch, As technology evolves, so does the nature of nationalism, *Centre for International Governance Innovation*, 27 September 2021

58 The "Great Firewall" refers to the Chinese government's centralised control over the internet infrastructure in China, meaning that access to many western platforms, as well as to certain content, is tightly controlled.

59 Q75 (Martijn Rasser)

60 HOUSE OF LORDS Select Committee on Communications 2nd Report of Session 2017–19, Regulating in a digital world, HL Paper 299

model of an open, interoperable, reliable and secure internet that prioritises liberal values, freedom of action and right to privacy is increasingly threatened by competing autocratic models of digital governance. These autocratic models propagated by countries such as China, Russia and Iran are premised on principles of government control and information security, which maintain that a country's sovereign interests should determine the acceptable use of technologies. They are tolerant of online censorship and higher degrees of surveillance[61] and have little respect for data privacy, compared to more democratic counterparts. Harriet Moynihan, Acting Director of the International Law programme at Chatham House, told us that the digital authoritarianism in Asia and other parts of the world has increased during the Covid-19 pandemic, for example through the widespread introduction of laws that provide governments with control over social media and greater surveillance powers.[62]

Countering authoritarian influence in international standard-setting bodies

20. Running parallel to the fragmentation described above is the intensifying competition between states seeking to shape the future international order through their preferred models of technology governance. Global technology standards are essential for ensuring interoperability between products and systems and for guaranteeing agreed levels of security.[63] As these standards determine the design and use of technology worldwide, they therefore shape the distribution of economic and political power.[64] As a result, standards have become a tool for geopolitical competition.[65]

61 Often under the auspices of law enforcement and national security.

62 Q8 (Harriet Moynihan)

63 Julian Ringhof and José Ignacio Torreblanca, The Geopolitics of technology: how the EU can become a global player, *European Council on Foreign Relations*, 17 May 2022

64 John Lee, Eric Zhang and Rogier Creemers, China's Standardisation System – trends, implications and case studies in emerging technologies,*Leiden Asia Centre,* April 2022

65 Julian Ringhof and José Ignacio Torreblanca, The Geopolitics of technology: how the EU can become a global player, *European Council on Foreign Relations*, 17 May 2022

Box 1: Summary of China and Russia's standard-setting objectives and approaches

Recognising the growing geopolitical importance of technology standards, China and Russia in particular are intensifying their efforts to embed autocratic norms into technology standards, particularly in fields such as 5/6G and surveillance equipment,[66] for example through China's continued promotion of its "new IP" model of internet governance[67] and its "Standards 2035" ambitions.[68]

The Chinese government's ambitions to lead on global technology standardisation are explicit. These ambitions were articulated in its "Standards 2035" published in 2020, followed by the National Standardisation Development (NSD) outline document in 2021.[69] The latter represents the Chinese government's first formal document outlining its ambitions to shape global technology standards in the coming decade.[70] These ambitions centre on aligning international standards with the Chinese government's own domestic priorities.[71] The document specifically mentions the ISO as a key arena for China's standards-setting efforts, given the central position the organisation holds in global standards-setting.[72]

Likewise Russia is championing its vision for a closed, nationally-controlled internet; for example, by supplanting the Internet Corporation for Assigned Names and Numbers (ICANN), the current multi-stakeholder group that coordinates internet domains.[73]

In December 2021, Russia and China publicly affirmed their 'no-limits' alliance and committed themselves to accelerate their technological decoupling from the West. The prospect of tighter Sino-Russian geopolitical and technological cooperation gives new urgency to the UK's ambition to become a science and technology superpower.[74]

66 Julian Ringhof and José Ignacio Torreblanca, The Geopolitics of technology: how the EU can become a global player, *European Council on Foreign Relations*, 17 May 2022

67 Originally, "New IP" was a set of proposals that were submitted by Huawei to the ITU's Telecommunications Standardization Advisory Group (TSAG) in September 2019. In January 2020, Huawei submitted a "New IP" proposal to the Focus Group on Technologies for Networks 2030. They proposed to develop new network protocols and architectures "by extending and redesigning the traditional IP [Internet Protocol]" to support new services for a "new Internet" by 2030. Whereas the internet today is decentralised and owned by everyone and no-one, the vision set out by Huawei would use a top-down model to place control in the hands of nation-states rather than individuals. The term "New IP" is now used to describe proposals that share features and concepts from the original submission to the ITU. The Internet Society, Huawei's "New IP" proposal - frequently asked questions, 22 February 2022.

68 China's National Standardisation Development outline, published in October 2021, sets targets for strong Chinese participation in international standardisation processes, including by drafting standards proposals and holding governance roles in key standardisation organisations.

69 Arjun Gargeyas and Megha Pardhi, What's behind China's new National Standardisation Outline Document? *The Diplomat*, January 14, 2022

70 Arjun Gargeyas and Megha Pardhi, What's behind China's new National Standardisation Outline Document? *The Diplomat*, January 14, 2022

71 One specific target in the plan is for 85 percent of China's domestic standards to be aligned with international standards by 2035. The Chinese Communist Party Central Committee and the State Council Publish the "National Standardization Development Outline, *CSET,* 19 November 2021

72 The Chinese Communist Party Central Committee and the State Council Publish the "National Standardization Development Outline, *CSET,* 19 November 2021

73 Isabella Wilkinson, Digital standards are key to protecting democracy, *Chatham House*, 17 May 2021

74 Julian Ringhof and José Ignacio Torreblanca, The Geopolitics of technology: how the EU can become a global player, *European Council on Foreign Relations*, 17 May 2022

21. Battles for control over standards are taking place in standards-setting organisations, which are increasingly being used as a theatre through which states seek to exert power and shape the trajectory of future technology development.[75] Deals struck in bodies such as the International Telecommunications Union (ITU) and the International Organisation for Standardisation (ISO) determine how technologies will be designed and implemented worldwide. The importance of increasing the UK presence in these fora, to ensure that UK values remain at the core of standards development and governance frameworks, cannot be understated. With China's growing assertiveness in these organisations, the consequences of inaction are clear.[76] In a recent example, a small number of exclusively Chinese-owned companies were involved in the shaping of the ITU's new rules around facial recognition--a particularly high-risk area when it comes to human rights.[77]

Martijn Rasser told us that

> China in particular has a strategic vision for what it wants to achieve with technology, and it is dedicating a vast amount of resources in order to make that vision a reality. Right now, the like-minded democracies in the world do not have that same type of strategic outlook …there just is not very much alignment between the democratic countries on these issues.[78]

22. China is becoming increasingly assertive in global standards-setting bodies. Between 2016 and 2019, 90 per cent of the standards proposals for surveillance technologies at the International Telecommunications Union (ITU) were put forward by China.[79] Aggressive Chinese standardisation efforts are evident through the multitude of Chinese-driven internet standards going through different ITU working groups at any one time,[80] as well as its increasing assertiveness in other international standards-setting organisations. For example, the Financial Times reported that Chinese-owned companies were responsible for 16 of the 65 proposals for new technical committees at the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) since 2014.[81]

75 TFP0032

76 In its 2022 Digital Strategy, the Government announced that it is aiming to increase the UK's formal representation in global digital technical standards bodies, for example by running for the UK's election to the International Telecommunication Union (ITU) Council in autumn 2022. Department for Digital, Culture, Media and Sport (DCMS), UK Digital Strategy, 4 July 2022.

77 TFP0032

78 Q67 (Martijn Rasser)

79 These standards are the technical specifications that shape the products, services, and processes consumers rely on every day, including everything from the dimensions of a cargo container to the protocols for routing internet traffic. These specifications are often highly influential: they allow products from different companies and countries to work seamlessly together, and they also help customers find and compare products or have confidence in the safety and performance of those products. See: Danny Bradbury, Welcome to the splinternet – where freedom of expression is suppressed and repressed, and Big Brother is watching, 4 January 2021.

80 Danny Bradbury, Welcome to the splinternet – where freedom of expression is suppressed and repressed, and Big Brother is watching, 4 January 2021.

81 Hideaki Ryugen and Hiroyuki Akiyama, China leads the way on global standards for 5G and beyond, Financial Times, 4 August 2020.

23. Global standards-setting organisations are intended to be politically and commercially neutral. While companies understandably push for their own patented technologies to be adopted as standards, the standardisation processes at these organisations are underpinned by impartiality, a principle that the organisations work hard to maintain.[82] Yet reports of distortionary practices at these organisations are increasing. While these organisations rest upon a norm of "let-the-best-technology-win", there are reported instances of Chinese participants being forced by the Chinese Government to vote for proposals tabled by Chinese technology companies such as Huawei.[83–84] Beyond China and Russia, there are a number of state regimes, such as the governments of Iran and Venezuela, with long-term interests in advancing autocratic models of technology governance for their own benefit and who thus are prepared to support China's standardisation proposals.

24. There is a real risk that UK companies and institutes may find themselves at a disadvantage relative to China's growing market power when it comes to defining standards for critical technologies–particularly those such as AI (and AI-enabled technologies such as autonomous systems), communications platforms and 6G. Should authoritarian governments achieve and sustain disproportionate influence in global standards-setting bodies, there is a significant risk that the design specifications and standards underpinning the technologies that we rely on in our everyday lives will not be aligned with the fundamental principles of democracy, privacy and human rights.[85] Systems will also lack free and open standards that will leave them vulnerable to exploitation and manipulation by autocratic governments seeking to limit civil liberties and human rights.[86] These standards have direct implications for the people of the UK, who may find themselves relying on products and systems that are not configured in their interests. For example, citizens may no longer be able to rely on their privacy settings.

82 Matt Sheehan, Marjory Blumenhal, and Michael Nelson, Three Takeaways From China's New Standards Strategy, Carnegie Endowment for International Peace, 28 October 2021

83 For example, there have been instances where Chinese government has instructed Chinese companies participating in ITU study groups to block consensus (even when doing so contravened the company's own interests)—to force the ITU to endorse its preferred standards in areas such as 5G. Chinese companies voting within the ITU process have previously been forced to vote en bloc, with delegates required to bring phones into their voting booths in order to prove that they supported the Chinese government's preferred options. See: Brett Schaefer and Danielle Pletka, Countering China's growing influence at the International Telecommunications Union, *The Heritage Foundation*, 7 March 2022

84 Matt Sheehan, Marjory Blumenhal, and Michael Nelson, Three Takeaways From China's New Standards Strategy, Carnegie Endowment for International Peace, 28 October 2021

85 Kristen Cordell, The International Telecommunication Union: The Most Important UN Agency You Have Never Heard Of, *Centre for Strategic and International Studies (CSIS),* 14 December 2022

86 Kristen Cordell, The International Telecommunication Union: The Most Important UN Agency You Have Never Heard Of, *Centre for Strategic and International Studies (CSIS),* 14 December 2022

Building democratic technology alliances and harnessing the FCDO's convening powers

25. At present, we are not convinced that the UK and its allies are doing all they can to win the battle over international technical standards. One of the UK's main global strengths is influencing rule-making and standard-setting. This was recognised by the FCDO in its evidence, in which it referred to "our significant strengths in diplomacy, regulation, research excellence, and academia".[87] Given these strengths, the FCDO told us that,

> the UK is well placed to influence the global debate, promote democratic norms and shape regulations for emerging technologies.[88]

Harnessing this strength will be key to realising the Government's ambition to establish the UK as a S&T superpower. However, the rules are being written by others and the UK risks being sidelined in these discussions,[89] becoming a "rule-taker" rather than a "rule-maker". Witnesses suggested that the Government's current approach to emerging technology governance is reactive rather than proactive in areas such as AI.[90] Experts from the AutoNorms Project at the University of Southern Denmark warned that if the Government continues along this trajectory, the UK risks becoming a state that follows the governance norms set by others and is thus limited in its ability to advance its own interests.[91]

26. We welcome initiatives undertaken by the FCDO to facilitate technology cooperation with like-minded countries, such as the recent establishment of the UK-Australia Cyber and Critical Technologies Strategic Partnership.[92] We also welcome the UK Government's efforts to build broader alliances and facilitate dialogue with like-minded countries, such as by inviting Australia, India, South Africa and South Korea to attend the G7 summit as guest countries in June 2021. While this is a constructive step forward, such ad-hoc measures will not be enough. Likewise, we appreciate the Government's efforts to use its 2021 G7 leadership to facilitate greater cooperation. At the G7 in June 2021, the Government secured commitments to preserving "an open, interoperable, reliable and secure internet", with the final communiqué also promoting multilateral fora such as the 'Future Tech Forum' in September 2021 and Global Partnership on Artificial Intelligence Summit in November 2021.[93] However, these efforts have not gone far enough - the two aforementioned fora have not meaningfully extended beyond emphasising the importance of dialogue and offering progress reports on already ongoing projects.

87 FCDO (TFP0015)
88 FCDO (TFP0015)
89 Q71 (Dr Ulrike Franke)
90 The AutoNorms Project is based at the Centre for War Studies, University of Southern Denmark. See: TFP0008
91 TFP0008
92 Other bilateral partnerships also appear to be in progress. For example last year, the Prime Minister and President Biden committed to developing a UK-US Tech Partnership, to strengthen UK-US cooperation in areas such as: the resilience and security of critical supply chains; data dialogue; R&D on emerging technologies; improving the accessibility and flow of data to support economic growth; online safety; regulation; and supporting scientific and technological progress.
93 The Global Partnership on AI (GPAI) was founded in 2020 to undertake and support applied AI projects and provide a mechanism for sharing multidisciplinary analysis, foresight and coordination—with the objective of facilitating international collaboration and synergies and reducing duplication in the area of AI systems governance.

Concrete commitments towards action remain scarce. Notably, witnesses pointed out that "the G7 Technology Ministers' statement stops short of proposing a new mechanism for international discussion of technology regulation."[94]

27. Witnesses noted that three technological spheres of influence are emerging that mean the UK must increasingly look three ways when it comes to technology regulation and development: towards the US, EU and China.[95] The Government's current position on the future of the global tech landscape and where it wants to situate the UK in relation to these competing spheres of influence is unclear. Crucially, the Government has not clearly articulated where it wants to place the UK relative to EU technology regulation efforts. If it does not do this thinking and act accordingly, it will not be included in discussions that will shape the future global regulatory environment.[96–97] While the EU and US engage in debates and measures to shape the future of global technology governance, the UK's involvement is limited. The UK is being left out of conversations on transatlantic tech cooperation between the US and EU (such as the US-EU Trade and Technology Council). UK efforts to engage bilaterally with the US and with European countries, and ad-hoc arrangements with other allies, will not be enough. In particular, the FCDO needs to work with departments to set out a holistic regime for staying aligned with the controls imposed on foreign technology firms by both the United States and the EU. We cannot become the weak link in the chain of the Western alliance's 'techno-defences'. We note for example, that the Foreign Secretary was recently unable to explain in evidence to our Committee how many Chinese firms were subject to some sort of UK control. This betrays a lack of grip we can no longer afford.

28. Evidence received throughout our inquiry has made it clear that we cannot effectively counterbalance the influence of digital authoritarianism without first establishing a joint vision for emerging technologies amongst the world's democracies. The US and the EU differ in their approaches to key tactical issues such as data privacy and the appropriate degree of private-sector regulation. However, through the Trade and Technology Council (TTC) the two blocs have identified and are building upon areas of shared values and interests (see Box 1). The TTC was announced at the US-EU summit in June 2021.[98] Cooperative efforts between the two sides remain a work in progress. Nevertheless, the TTC has taken concrete steps to identify and build upon areas of common interest and agreement between the US and the EU. This initiative between the world's two regulatory powerhouses risks sidelining the UK. The UK risks "remaining outside the room where decisions with implications for its economic and technological interests are made".[99] The European Council on Foreign Relations' Ulrike Franke told us that when it comes to transatlantic technology cooperation,

94 TFP0014
95 Q68 (Dr Ulrike Franke)
96 Q80 (Dr Ulrike Franke)
97 Microsoft suggested to us that the UK should maintain a strong relationship with the EU on cyber and emerging technology issues. For example, Microsoft suggested that the European Cyber Agora the European multistakeholder forum for discussions established among governments, private sector and civil society, provides a platform to discuss a unified European value-based approach to global cyber issues. TFP0017 (Microsoft)
98 Dr Ulrike Franke and José Ignacio Torreblanca, Geo-tech politics: why technology shapes European power, *European Council on Foreign Relations*, 15 July 2021
99 Stephan Lehne, Rivals or Partners? The EU-UK Foreign Policy Relationship After Brexit, *Carnegie Europe*, 30 March 2021

> the UK has been a bit left out… and the exclusion of the UK seems to have been somewhat of its own choosing.[100]

Box 3: Overview of the US-EU Trade and Technology Council

The Trade and Technology Council (TTC) was established in 2021 as a diplomatic forum through which the US and EU are negotiating enhanced cooperation in trade and technology policy, with the ultimate aim of promoting democratic digital governance. The TTC comprises ten working groups, each focusing on specific policy issues:

Working groups of the US-EU Trade and Technology Council	
Technology standards	Climate and clean tech
Secure supply chains	ICT Services security and competitiveness
Data governance and technology platforms	Misuse of technology threatening security and human rights
Export controls	Investment screening
Promoting SME access to the use of digital tools	Global trade challenges

The US-EU Trade and Technology Council (TTC) met for the first time in Pittsburgh on 29 September 2021. The second meeting took place in May 2022. The quick and harmonised US and EU export controls on advanced technologies that were imposed on Russia after the invasion of Ukraine in February 2022 have been described as the first success story of the TTC.[101]

29. The rise of digital authoritarianism creates a strong incentive for greater alignment between the world's more democratic countries on technology governance.[102] Multiple witnesses advised us that the UK Government should prioritise efforts to renew and strengthen collaboration with the US and EU, and that these efforts should build on shared principles and values to strengthening technology rules and norms.[103] The importance of including other countries such as Australia, Japan and South Korea was also made clear throughout this inquiry. Some degree of regulatory divergence is inevitable but there are many areas of shared values and interests that can be built upon. A more coherent democratic approach to vision and values for technology governance would not only support the UK's digital trade and technology relationships, but also help to align digital rules and standards, facilitate interoperability between digital systems, and provide a stronger counterbalance to authoritarian influences over global governance of the technology landscape and digital spaces. There is an opportunity for the FCDO to harness its strengths in convening and influencing to progress transatlantic technology cooperation towards a shared vision.

100 Q80 (Dr Ulrike Franke)

101 Frances Burwell, Rethinking the US-EU Trade and Technology Council after Ukraine, *The National Interest,* 13 March 2022.

102 Pepijn Bergsen, Carolina Caeiro, Harriet Moynihan, Marianne Schneider-Petsinger and Isabella Wilkinson, Digital Trade and digital technical standards, *Chatham House*, 24 January 2022

103 TFP0032

30. A strong and cohesive response by the UK and our allies is needed to restrict the growing influence of authoritarian governments in global standardisation processes. There is an opportunity for the UK Government to exercise thought leadership in this regard, and to build upon its diplomatic strengths to convene and influence. BAE told us that

> Purely pursuing a coherent global framework is fraught with risk and uncertainty, as gaining agreement with certain countries is very unlikely: there is a real risk of trying to take a generally global approach and then nothing happening due to international disagreements and disputes.[104]

31. We cannot achieve alignment on all issues - nor should we attempt to do so. Accepting tactical-level differences between nation-states will be necessary to achieve cohesion based on fundamental principles of democracy, human rights and a free and open internet, while also respecting state sovereignty. Despite tactical-level differences, democracies maintain a shared commitment to the rules-based international order. Establishing consensus on the fundamentals would place democracies in a stronger position to counter those with a different vision for digital governance.[105]

32. Views on the mechanisms by which this collaboration could take place vary. Nesta suggested that the appropriate fora for collaboration will vary depending on the issue at hand. For example, bilateral agreements may be effective in certain contexts, whereas other channels of influence may include Ministerial statements at the G7 or multilateral activities such as the UK championing NATO's efforts to deploy AI in a security context.[106] Others suggested that an ad-hoc approach to technology governance will not be sufficient to counterbalance digital authoritarianism, and recommended a "robust, well-staffed international mechanism rather than a series of ad-hoc meetings around the G7." Experts have also suggested that the US-EU TTC may present value as a useful starting point, and that there could be benefit to the UK connecting with this platform and encouraging the inclusion of other democracies.[107] Despite these differing views on the precise mechanisms for cooperation, one common theme is clear–the UK should not be seeking to carve out a "fourth way" in technology standards and governance. While the UK's unique strengths in diplomacy and S&T place it in a strong position to exercise thought leadership, attempts to do this alone and through ad-hoc bilateral arrangements risk weakening a fragmented western position vis-à-vis China and other states propagating authoritarian models of technology governance.

33. **The UK's position on technology standards vis-à-vis the US and EU remains unclear and the Government's stance on many elements of the Transatlantic Trade and Technology Partnership remains ambiguous. The UK therefore risks becoming a rule-taker rather than a rule-maker.** ***The Government should clearly articulate its position on data sharing, privacy and private-sector regulation, so that it can establish a starting point for discussions on deeper cooperation with the US and the EU. This***

104 TFP0018
105 Stephan Lehne, Rivals or Partners? The EU-UK Foreign Policy Relationship After Brexit, *Carnegie Europe*, 30 March 2021
106 TFP0032
107 Pepijn Bergsen, Carolina Caeiro, Harriet Moynihan, Marianne Schneider-Petsinger and Isabella Wilkinson, Digital Trade and digital technical standards, *Chatham House*, 24 January 2022

position should be set out within the forthcoming International Technology Strategy or a related policy document to inform the FCDO's efforts to influence standards and norms at the international level.

34. **We cannot meaningfully influence the global order without the cooperation and support of our partners. While there is an opportunity for the UK to exercise thought leadership, we cannot go it alone and should not seek to carve out a "fourth way" for the UK in global technology governance.** ***We recommend that the FCDO leverages its diplomatic influence and wider relationships to promote mutual understanding among the world's different regulatory blocs, to facilitate a cohesive international approach to technology governance, based on the shared values of democracy, openness and human rights.***

Strengthening partnerships with the world's digital deciders

35. When it comes to establishing democratic models of global technology governance and countering the influence of authoritarian governments, multiple witnesses emphasised the critical role of "digital deciders". This term refers to those states who are yet to align themselves fully with any competing model, having not decided upon their preferred approach to technology governance.[108] China and Russia have started a process of decoupling from the West, a process to which they seek to attract other countries. As summarised in Box 1, exporting its authoritarian model of technology governance is a central part of China's diplomatic strategy. Australia's Ambassador for Cyber and Critical Technologies, Tobias Feakin, warned us that "authoritarianism in a box" is being packaged up and given to other developing countries by authoritarian governments, supporting the surveillance and control of their populations.[109]

36. The Chinese Government has articulated a clear strategy for advancing standards alignment within countries participating in its Belt and Road Initiative (BRI). The 2021 National Standardisation Development (NSD) Document outline also sets out plans to increase dialogues on standards with BRIC countries (Brazil, Russia, India and China) and the Asia-Pacific Economic Cooperation (APEC) forum.[110] The Digital Silk Road, which forms part of the broader BRI, is one of the main channels through which the Chinese Government is seeking to export its digital governance models and expand its data access through building infrastructure in countries across Africa and the Indo-Pacific region. [111]

37. Witnesses warned us of the Chinese Government's long-term vision to capture "digital deciders" such as India, Singapore, Brazil and many African countries. The Chinese Government is currently filling the gap in the provision of digital infrastructure in Africa and the Indo-Pacific region to export and promote its model of digital authoritarianism. African countries such as Kenya, Mauritius, Ethiopia and Zimbabwe, and some countries in South America such as Ecuador, Bolivia and Venezuela, are already trialling the model for smart cities using products developed by Alibaba Cloud and Huawei, so Chinese-owned companies have written the instruction manual on how

108 Q2 (Harriet Moynihan)
109 Q62 (Tobias Feakin)
110 The Chinese Communist Party Central Committee and the State Council Publish the "National Standardization Development Outline", *CSET,* 19 November 2021
111 Matthew J Slaughter and David H McCormick, Data is power, Foreign Affairs, May/June 2021

smart cities in these countries can be operated.[112] This practice of exporting technologies and the standards accompanying them creates path dependencies; it means that countries that adopt Chinese standards will have an interest in these standards being adopted by international standard-setting organisations. This strengthens China's influence in these organisations. Digital deciders are likely to become combatants in a key battleground for technology influence in a fragmented digital landscape.[113] In this context, building stronger technology partnerships in the global south has never been more important.[114] Evidence taken in this inquiry has shown that building stronger relationships with these digital deciders should be a key focus for any future democratic technology alliance.[115] In recognition of this, the EU has launched the "Global Gateway" initiative, through which it seeks to use digital development investments in lower income countries to promote values-based digital regulation and geopolitical thinking. Similarly, the Japanese government has launched the Expanded Partnership for Quality Infrastructure and Blue Dot Network initiatives to counterbalance China's influence in the Asia-Pacific region by using infrastructure-building to foster relationships. [116]

38. Nesta emphasised to us that working closely with allies in the global south should be a priority for the UK Government, to ensure that their governments and civil society actors are able to participate meaningfully in the processes underpinning the world's internet governance systems, which can often be resource-intensive and opaque, and therefore inaccessible to many actors.[117][118] Facilitating more diverse participation would not only establish more resilient standard-setting processes, but also help to prevent these bodies being dominated by countries propagating different values in the use of government digital repression and surveillance.[119]

39. ***There is a strong case for the Government to establish deeper partnerships with "digital deciders" such as India, Singapore and Brazil. There is scope for the FCDO to have more dialogue with these countries and to form partnerships around the value of an open and global approach to tech rules and governance to counter the influence of authoritarian governments. The Government should increase its diplomatic efforts with countries who might otherwise align with models of digital authoritarianism, including by offering trade and investment opportunities in support of technologies that support democratic values and human rights. The Government should consider using funding streams such as the Conflict, Stability and Security Fund (CSSF) to support this work.***

112 Alex He, The Digital Silk Road and China's Influence on Standard Setting, *Centre for International Governance Innovation*, 4 April 2022, Richard Ghiasy and Rajeshwari Krishnamurthy, China's Digital Silk Road and the Global Digital Order, *The Diplomat*, 13 April 2021

113 The Register, Welcome to the splinternet, 4 January 2021

114 Chatham House, Digital trade and digital technical standards, 24 January 2022

115 For example, Harriet Moynihan stated that "There is real scope for the FCDO to have a dialogue and to form partnerships around the value of an open and global approach to governance and to the rules on that." Similarly, Martijn Rasser suggested that such engagement could be a focus for future transatlantic technology cooperating, telling us that promising area for UK-US-EU tech cooperation is promotion of sustainable and resilient critical infrastructure around the world, for example in Africa and Indo-Pacific, to counter Chinese digital authoritarianism. China is currently filling this gap in provision. Q76 & Q78 (Martin Rasser); Q2 [Harriet Moynihan]

116 RAND Europe (TFP0036)

117 For example, through the provision of expertise and resources, including through initiatives of the Science and Innovation Network.

118 Nesta (TFP0032)

119 Nesta (TFP0032)

3 Linking domestic and foreign policy: bolstering national capabilities to exert international influence

> *The UK must continue to develop and expand its thriving tech sector to ensure it remains strong on the global stage.*–Joe White, UK Technology Envoy to Silicon Valley.

40. The ability of UK Government and businesses to advocate internationally for standards conducive to UK values and interests rests upon a strong domestic industrial base. Industry representatives highlighted that cohesion and continuity between the UK's domestic and international policies will be key to realising the Government's global S&T leadership ambitions,[120] and to countering the efforts of authoritarian governments who are exerting their influence in international standards-setting organisations through state-backed entities. By building and leveraging the UK's domestic strengths, the Government would be better able to strengthen the UK's voice in international fora. The FCDO acknowledged that there are lessons to be learned from other countries. For example, Israel and Singapore have leveraged their domestic strengths in AI and cyber security to build their international influence. They have done this by coupling research investment with policy and regulatory support that creates technological ecosystems that encourage the international growth of domestic technology companies.[121] The FCDO informed us in written evidence that

> As technologies develop, those countries which back the full spectrum of interventions through finance, commercialisation, and policy will have the ability to establish global norms and standards… By investing time and resources now, the UK increases its chances to embed our values and inject our 'secure by design' ethos to ensure future governance supports our values, prosperity and national security.[122]

120 techUK (TFP0022)
121 UK Computing Research Committee (TFP0001)
122 Foreign, Commonwealth and Development Office (TFP0015)

41. The Government's ability to meet these international objectives will depend largely upon the domestic initiatives that are established and how they are implemented and enforced at home.[123] The Government has announced multiple initiatives aimed at boosting domestic industry in key areas, such as the Digital Growth Grant to boost UK digital start-ups.[124] We commend these initiatives, which will be essential for ensuring the UK's future self-sufficiency in key technology areas. However, there is currently a stark disconnect between the UK's domestic and foreign policy activities, as well as between the Government's stated ambitions and its actions.[125]

42. While early-stage R&D receives a welcome level of Government support, it is well-known that this funding often falls away before innovative ideas can be fully commercialised.[126] Overseas buyers can fill these gaps, meaning that intellectual property often moves out of the UK.[127] Similarly, domestic market conditions mean that start-ups that have initially received support often encounter difficulties when attempting to scale up their businesses in the UK. As a result, promising start-ups are often sold overseas, undermining the Government's ambitions to establish and maintain sovereign capabilities in key technology areas. We highlighted these risks in our 2021 report S*overeignty for sale: the FCDO's role in protecting strategic business assets*. We welcome measures the Government has taken to address these concerns, for example through the introduction of the National Security and Investment (NSI) Act 2021 and subsequent review of acquisitions we highlighted as particularly concerning.[128] However as long as the latter remain mostly confined to very early-stage innovation support, the market incentives for overseas sales will remain, as innovative ideas are unable to be fully scaled up and commercialised in the UK. This, in turn, will continue to undermine the UK's influence at international standards-setting bodies. In addition, there is a fast-growing risk of a 'control gap' between the UK and our allies in the way we coordinate delisting of foreign firms, banning share trading, exports and imports, granting and revoking trading licences, controlling the movement of data and applying sanctions to key executives

43. In its 2022 International Telecommunications Union (ITU) manifesto, the Government names key UK Sector Members that make an "active contribution" to the ITU, including ARM, Avanti, the BBC, BT, Inmarsat and Vodaphone.[129] Of the companies

123 British Foreign Policy Group, The UK Integrated Review of Foreign Policy Group: One Year On, March 2022

124 UKTN, Government launches £12 grant to boost UK digital startup growth, 12 April 2022

125 The Government clearly recognises the need for connectivity and cohesion across departments on these issues; it is the action, rather than the narrative, that is currently lacking. Joe White informed us that the process of developing and scaling technology companies "spans the remits of DfE (education), BEIS (R&D), DCMS (tech policy), FCDO (international norms and influence), DIT (market access and trade), HMT (capital and incentives), and the defence and security organisations which are both customers and partners in technology." He pointed out that "for the UK to design and implement a cohesive and agile strategy creating sustained science and technology advantage, it requires coordination and delivery across all these departments in both the domestic and international agenda." Correspondence with Joe White, UK Technology Envoy to Silicon Valley, June 2022.

126 The UK's Tech Envoy, Joe White, told us in correspondence that while the UK does have strong domestic technology capabilities, "there is still work to do on commercialisation of research and later stage capital investment." Moreover, he stated that "We [the UK] retain a communications and narrative problem in effectively telling our tech story to global markets which means we don't get the full recognition for our excellent progress." Correspondence with Joe White, UK Technology Envoy to Silicon Valley, June 2022.

127 PA Consulting, The Integrated Review's 'science sombrero': building the ecosystem while focusing on rapid impact

128 Third Report of Session 2021–22, Sovereignty for sale: the FCDO's role in protecting strategic British assets, HC 197; Department of Business, Energy and Industrial Strategy, Newport Wafer Fab acquisition called in for national security assessment, 25 May 2022

129 Department for Digital, Culture, Media and Sport, United Kingdom: Candidate for the International Telecommunication Union Council, 10 November 2021

named, two (ARM and Inmarsat) have been sold to foreign buyers. Should this pattern continue, the UK representation at institutions such as the ITU or ISA risks being eroded. Without a strong domestic industrial base, the UK will lack the representation that it needs to shape the international regulatory environment meaningfully in favour of UK values and interests.

44. **The integration of technology within UK foreign policy should reflect the intrinsic links between the UK's domestic capabilities and its global influence. The Government's recent measures to encourage growth and support start-ups within the UK technology sector are welcome, but they have been undermined by the Government's previous reticence to review and intervene in foreign investments that risk moving strategically important UK businesses overseas. This slow erosion of our domestic capabilities has implications for our ability to project influence internationally.** ***In its response to this report, we ask that the FCDO sets out and then reports back to the Committee on its plans and progress in integrating this work between departments.***

4 Measuring FCDO progress in delivering on the Government's leadership ambitions

45. The Government's *Integrated Review* places significant emphasis on S&T investment, an emphasis that is both necessary and welcome. The Government will shortly be publishing an International Technology Strategy. We were told that this strategy will build upon the Integrated Review and the vision for a "network of liberty" set out by the Foreign Secretary, setting out the Government's position on critical and emerging technologies.[130]

46. While we welcome the Government's increased investment in S&T, financial commitments and high-level strategies alone will not be enough to secure the UK's future security, resilience and global influence. The key to the success of these strategies will be in their delivery. This in turn relies on regular review, evaluation and adaptation. Regular review will be particularly critical given the rapid pace of technological developments; the FCDO's subsequent adaptation will require clear performance metrics that form the basis of these evaluations.[131] This is something that is recognised by nations that have already established technology diplomacy strategies, such as Denmark and Australia. Their clear key performance indicators not only guide the implementation of their strategies, but also send a clear message to their domestic and international audiences about what they are trying to achieve.[132] Developing performance metrics, as part of regular review and evaluation of how well the FCDO is delivering against its objectives, would serve both to guide the implementation and maximise the effectiveness of its International Technology Strategy. Such metrics could include instances UK contribution to international policy development and standard-setting mechanisms such as the ITU and ISO; examples of how the FCDO has contributed to wider UK Government technology policy development with annual reports or statements on how it has contributed to significant tech policy issues; and evidence of how it has supported digital resilience and infrastructure-building in emerging economies.

47. ***The FCDO's forthcoming International Technology Strategy should set out clear objectives and targeted actions for achieving them, to be used as a blueprint or framework that diplomats can easily use to guide their decisions and activities at Post level and to ensure a coherent approach across the FCDO's global network.***

48. ***We recommend that the FCDO designs and publishes in its forthcoming International Technology Strategy metrics on how it is supporting the Integrated Review's goal of establishing the UK as a science and tech superpower. Performance against these metrics should be set out in the Department's annual report and accounts.***

130 Q234 (Amanda Milling)

131 The Henry Jackson Society advised us to "examine technology utilisation [FCDO] diplomacy to develop a matured practice of evaluating technology programmes and their enhancement of UK influence." (TFP0012)

132 Q54 (Ambassador Engtoft-Larsen)

5 Conclusion

49. The battle between authoritarian and rights-based technological standards and values is playing out in multiple arenas. Some of these are well-known and receive a considerable degree of media attention. Others are opaque and unfamiliar to most citizens. The outcome of these unseen battles for influence will, however, be felt by us all. They will determine our future rights to privacy, the ways in which we are able to access and use information, and the extent to which we will be able to speak to one another across devices, platforms and jurisdictions. Malign actors are trying to rewrite the rules underpinning our international system and technology development. Standardisation provides them with the opportunity to do so. It is vital that the Government works with others to avoid a future in which rights-based and human-centred technology standards are not the norm. Despite the Chinese government's explicit strategy for exporting and embedding its own authoritarian principles of technology governance across the world, the Government's response has so far been incoherent and muted. The Government now needs to extend the UK's influence within the global technology landscape, to ensure that future technologies are developed and used in ways that align with our values and, crucially, uphold the rights and freedoms of people in the UK and across the world.

Conclusions and recommendations

Shaping and adapting to the changing role and influence of the nation state

1. The growing influence of private companies in global technology governance, and on the norms and rules that shape our societies, has profound implications for the future role and identity of the nation-state. The Government has yet to demonstrate that it has seriously considered its role and influence within this new environment and how it might manage the consequences of these shifts in influence and identity. *In the forthcoming International Technology Strategy, we recommend that the FCDO clearly articulates what it understands its future role in global tech governance to be and how it intends to engage with private companies and relevant multinational bodies to project UK norms and values in global policy-making fora. We further recommend that the FCDO identifies a Minister with clear responsibility for this work within the Department and sets out how its work interacts with that of other Government departments.* (Paragraph 11)

2. *The UK's global technology leadership ambitions should be Government-led but will need to pull in significant support from the private sector as well as academia. There is an opportunity for the FCDO to exemplify the values articulated in the Integrated Review by leading on collaboration with the private sector and civil society, both in the UK and overseas, in the pursuit of its objectives. This should include working to ensure that the voices of smaller companies and less economically developed countries are heard in global fora. There is an opportunity for the Government to influence global best practice by sharing knowledge of the National Cyber Security Centre (NCSC) and drawing upon the expertise of our world-class institutes.* (Paragraph 12)

3. *The UK should work with allies to ensure global practice in frameworks designed to protect data, and to prevent our adversaries exporting data from around the world to build the massive data sets needed to develop algorithms to automate surveillance systems, military systems and disinformation systems. We need to think about data as a national security asset, which should be subject to an appropriate regime of export controls. Placing greater controls on the collection, aggregation and access to data available to China is a good first step to eliminating an obvious national-security vulnerability.* (Paragraph 13)

4. *We recommend that the FCDO prioritises engaging with product teams and technologists, rather than only policy teams, to gain a clearer understanding of the activities of companies that are developing and implementing new technologies, as well as helping to influence the activities of these companies. The Department will need to bring in and develop the internal skills and expertise it needs to effectively engage at this level* (Paragraph 16)

The UK's place in shaping the international order

5. The UK's position on technology standards vis-à-vis the US and EU remains unclear and the Government's stance on many elements of the Transatlantic Trade and Technology Partnership remain ambiguous. The UK therefore risks becoming

a rule-taker rather than a rule-maker. *The Government should clearly articulate its position on data sharing, privacy and private-sector regulation, so that it can establish a starting point for discussions on deeper cooperation with the US and the EU. This position should be set out within the forthcoming International Technology Strategy or a related policy document to inform the FCDO's efforts to influence standards and norms at the international level.* (Paragraph 33)

6. We cannot meaningfully influence the global order without the cooperation and support of our partners. While there is an opportunity for the UK to exercise thought leadership, we cannot go it alone and should not seek to carve out a "fourth way" for the UK in global technology governance. *We recommend that the FCDO leverages its diplomatic influence and wider relationships to promote mutual understanding among the world's different regulatory blocs, to facilitate a cohesive international approach to technology governance, based on the shared values of democracy, openness and human rights.* (Paragraph 34)

7. *There is a strong case for the Government to establish deeper partnerships with "digital deciders" such as India, Singapore and Brazil. There is scope for the FCDO to have more dialogue with these countries and to form partnerships around the value of an open and global approach to tech rules and governance to counter the influence of authoritarian governments. The Government should increase its diplomatic efforts with countries who might otherwise align with models of digital authoritarianism, including by offering trade and investment opportunities in support of technologies that support democratic values and human rights. The Government should consider using funding streams such as the Conflict, Stability and Security Fund (CSSF) to support this work. (*Paragraph 39)

Linking domestic and foreign policy: bolstering national capabilities to exert national influence

8. The integration of technology within UK foreign policy should reflect the intrinsic links between the UK's domestic capabilities and its global influence. The Government's recent measures to encourage growth and support start-ups within the UK technology sector are welcome, but they have been undermined by the Government's previous reticence to review and intervene in foreign investments that risk moving strategically important UK businesses overseas. This slow erosion of our domestic capabilities has implications for our ability to project influence internationally. *In its response to this report, we ask that the FCDO sets out and then reports back to the Committee on its plans and progress in integrating this work between departments.* (Paragraph 44)

Measuring FCDO progress in delivering on the Government's leadership ambitions

9. The FCDO's forthcoming International Technology Strategy should set out clear objectives and targeted actions for achieving them, to be used as a blueprint or framework that diplomats can easily use to guide their decisions and activities at Post level and to ensure a coherent approach across the FCDO's global network. (Paragraph 47)

10. We recommend that the FCDO designs and publishes in its forthcoming International Technology Strategy metrics on how it is supporting the Integrated Review's goal of establishing the UK as a science & tech superpower. Performance against these metrics should be set out in the Department's annual report and accounts. (Paragraph 48)

Formal minutes

Tuesday 5 July 2022

Members present:

Tom Tugendhat, in the Chair

Liam Byrne

Alicia Kearns

Graham Stringer

Draft Report (*Encoding values: Putting tech at the heart of UK foreign policy*), proposed by the Chair, brought up and read.

Ordered, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 49 read and agreed to.

Summary agreed to.

Resolved, That the Report be the Third Report of the Committee to the House.

Ordered, That the Chair make the Report to the House.

Ordered, That embargoed copies of the Report be made available (Standing Order No. 134).

[Adjourned till Tuesday 12 July at 2 pm

Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the inquiry publications page of the Committee's website.

Tuesday 29 June 2021

Ria Thomas, Managing Director, Polynia Advisory; **Harriet Moynihan**, Senior Research Fellow at the International Law Programme, Chatham House — Q1–18

Toomas Ilves, Former President of Estonia; **Ashish Jaiman**, Director of Technology Operations, Microsoft; **Hugh Milward**, General Manager, Corporate, External and Legal Affairs, Microsoft — Q19–50

Tuesday 07 September 2021

Anne-Marie Engtoft Larsen, Tech Ambassador, Ministry of Foreign Affairs Denmark; **Tobias Feakin**, Ambassador for Cyber Affairs and Critical Technology, Australian Department of Foreign Affairs and Trade — Q51–66

Martijn Rasser, Director, Technology and National Security Program, Center for a New American Security (CNAS); **Ulrike Franke**, Senior Policy Fellow, European Council on Foreign Relations — Q67–80

Tuesday 02 November 2021

Katie O'Donovan, Public Policy Manager, Google UK — Q81–139

Joe Westby, Deputy Director, Amnesty Tech, Amnesty International; **David Sullivan**, Executive Director, Digital Trust & Safety Partnership; **Jason Pielemeier**, Deputy Director, Global Network Initiative — Q140–162

Tuesday 11 January 2022

Miranda Sissons, Global Director of Human Rights, Meta; **John Hughes**, Global Head of Geopolitical and Economic Public Policy Strategy, Twitter — Q163–182

Sarah Spencer, Digital Specialist Consultant and Digital Threats Advisor, International Committee of the Red Cross; **Balthasar Staehelin**, Director for Digital Transformation and Data, International Committee of the Red Cross — Q183–230

Tuesday 01 March 2022

Rt Hon Amanda Milling MP; **Professor Charlotte Watts**, Chief Scientific Adviser and Director for Research and Evidence, Foreign, Commonwealth and Development Office; **Chris Jones**, Director, Delivery and Analysis, Foreign, Commonwealth and Development Office — Q231–265

Published written evidence

The following written evidence was received and can be viewed on the inquiry publications page of the Committee's website.

TFP numbers are generated by the evidence processing system and so may not be complete.

1 Amnesty International UK (TFP0005)

2 Aradau, Professor Claudia (TFP0027)

3 Ayadurai, Dr Charmele (Assistant Professor Economics and Finance., Durham University); and Dr Sina Joneidy (Lecturer in Digital Enterprise, Teesside University) (TFP0003)

4 BAE Systems plc (TFP0018)

5 BBC World Service (TFP0035)

6 Bell, Professor Christine (Professor of Constitutional Law, Director Political Settlements Research Programme, University of Edinburgh) (TFP0030)

7 Bode, Dr Ingvild (Associate Professor & Principal Investigator, Centre for War Studies, University of Southern Denmark); Anna Nadibaidze (PhD researcher, Centre for War Studies, University of Southern Denmark); Dr Hendrik Huelss (Assistant Professor , Centre for War Studies, University of Southern Denmark); and Dr Tom Watts (researcher, Centre for War Studies, University of Southern Denmark) (TFP0008)

8 British and Irish Law, Education and Technology Association (TFP0007)

9 Carnegie UK Trust (TFP0014)

10 Creative Industries Policy and Evidence Centre, led by Nesta (TFP0011)

11 Dias, Dr Talita (Junior Research Fellow, Jesus College, University of Oxford; Oxford Programme on International Peace and Security, Oxford Institute for Ethics, Law and Armed Conflict, University of Oxford); and Rhiannon Neilsen (Research Consultant , Oxford Programme on International Peace and Security, Oxford Institute for Ethics, Law and Armed Conflict, University of Oxford) (TFP0023)

12 Drone Wars UK (TFP0009)

13 EPA (TFP0037)

14 Foreign, Commonwealth and Development Office (TFP0015)

15 Henry Jackson Society (TFP0012)

16 International Committee of the Red Cross (TFP0029)

17 Internews Europe (TFP0041)

18 Jones, Simon (Director, Dartkite) (TFP0016)

19 Kello, Prof. Lucas (Associate Professor of International Relations, Oxford University) (TFP0033)

20 LGB Alliance (TFP0038)

21 Microsoft (TFP0017)

22 Nesta (TFP0032)

23 Northumbria Law School, Northumbria University (TFP0013)

24 Open Doors UK & Ireland (TFP0019)

25 Oracle Corporation (TFP0006)

26 Parsons, Kathryn (Founder and CEO, Decoded) (TFP0031)

27 Protection Approaches (TFP0039)

28 RAND Europe (TFP0036)

29 Reprieve (TFP0034)

30 Sedex (TFP0021)

31 Stevens, Mr Anthony (President, International, Victor Insurance) (TFP0024)

32 Strong, Dr James (Senior Lecturer in British Politics and Foreign Policy, Queen Mary University of London); and Dr Elke Schwarz (Senior Lecturer in Political Theory, Queen Mary University of London) (TFP0020)

33 Tony Blair Institute for Global Change (TFP0026)

34 UK Campaign to stop Killer Robots; and Women's International League for Peace and Freedom UK (TFP0028)

35 UK Computing Research Committee (TFP0001)

36 Wadhwa, Tarun (Nonresident Fellow, Atlantic Council, GeoTech Center) (TFP0025)

37 Williams, Dr Heather (Lecturer, King's College London); and Marina Favaro (Consultant, King's College London) (TFP0010)

38 techUK (TFP0022)

List of Reports from the Committee during the current Parliament

All publications from the Committee are available on the publications page of the Committee's website.

Session 2022-23

Number	Title	Reference
1st	Missing in action: UK leadership and the withdrawal from Afghanistan	HC 169
2nd	The cost of complacency: illicit finance and the war in Ukraine	HC 168

Session 2021–22

Number	Title	Reference
1st	In the room: the UK's role in multilateral diplomacy	HC 199
2nd	Never Again: The UK's Responsibility to Act on Atrocities in Xinjiang and Beyond	HC 198
3rd	Sovereignty for sale: the FCDO's role in protecting strategic British assets	HC 197
4th	The UK Government's Response to the Myanmar Crisis	HC 203
5th	Global Health, Global Britain	HC 200
6th	Sovereignty for sale: follow-up to the acquisition of Newport Wafer Fab	HC 1245
7th	Lagos calling: Nigeria and the Integrated Review	HC 202
1st Special	A climate for ambition: Diplomatic preparations for COP26: Government Response to the Committee's Seventh Report of Session 2019–21	HC 440
2nd Special	Government response to the Committee's First Report of Session 2021–22: In the room: the UK's role in multilateral diplomacy	HC 618
3rd Special	Government Response to the Committee's Fourth Report: The UK Government's Response to the Myanmar Crisis	HC 718
4th Special	Government response to the Committee's Third Report: Sovereignty for sale: the FCDO's role in protecting strategic British assets	HC 807
5th Special	Never Again: The UK's Responsibility to Act on Atrocities in Xinjiang and Beyond: Government Response to the Committee's Second Report	HC 840
6th Special	Global Health, Global Britain: Government Response to the Committee's Fifth Report	HC 955

Number	Title	Reference
7th Special	Government Response to the Committee's Sixth Report: Sovereignty for sale: follow-up to the acquisition of Newport Wafer Fab	HC 1273