Written evidence submitted by RAND Europe (TFP0036)

What technologies are shifting power? What is the FCDO's understanding of new technologies and their effect on the UK's influence?

Democratising access to digital spaces, technologies and services has significantly increased the number of actors that are able to leverage technological advances for a widening range of purposes. As a result, technological innovation has provided significant opportunities for global governance through democratising access to knowledge and information, as well as enabling new linkages between different actors and communities worldwide. Increasing connectivity has, for example, provided new opportunities for democratic participation and the exercising of freedom of opinion and expression through online platforms, as well as exchange of best practices among civil society organisations and others working to foster human rights in a digital age.

However, this democratising access has also posed significant hurdles that civil society, government and business have to navigate. For example:

- Data commodification has become central to the digital economy, with surveillance capitalism growing rapidly. A lack of oversight and control is evident as new data-intensive technologies emerge, resulting in significant gaps in appropriate understanding of security requirements and human rights safeguards. Data, digital technologies and services are also increasingly used as governance commodities, with digitalisation of public services improving their quality and delivery while also increasing the risk of unintended consequences and corresponding impacts for human rights.
- The digital age has also seen a rapid increase in the exploitation of digital spaces for illicit and criminal purposes, including the targeting of others through online harms, and weaponisation of the information environment for mis- and disinformation, propaganda, and recruitment of supporters (e.g. by non-state armed actors). Communities around the world also face weakening human rights safeguards as access to protective tools and information is restricted through monitoring, blocking, or filtering of online content or the criminalisation of encryption and privacy-enhancing technologies.[1]

In conjunction with wider political and socio-cultural trends, including declining social trust and increasing public uncertainty, technological change thus facilitates a context in which actors including the UK have to fundamentally reconsider established means for achieving influence. In this context, new and emerging technologies shape the character, dynamics and distribution of global power in various ways:

- State actors have traditionally benefited from a range of diplomatic, military, economic, financial and other levers of power through which they can project and exercise influence over others. **Technological change however provides new tools that can be used to exert influence domestically, regionally and globally**. For example, new information and communications technologies (ICTs) can enable the increasing adoption of digital diplomacy (also known as e-diplomacy or public diplomacy 2.0).[2] Advances in augmented reality/virtual

[1] For a further discussion of these and other trends see Bellasio, Jacopo, Linda Slapakova, Fiona Quimbre, Sam Stockwell. 2021. 'Human Rights in the Digital Age'. Santa Monica, Calif.: RAND Corporation (forthcoming).

[2] The People's Republic of China (PRC) has, for example, made increasing use of digital spaces including Twitter and Facebook to strategically amplify its narratives and sow divide among non-mandarin speaking

reality (AR/VR) are also altering traditional approaches to conflict mediation by creating virtual spaces for engagement away from the negotiation table. In contrast, blockchain and distributed ledger technologies are challenging the design and implementation of international sanctions regimes. It is in this context that actors including the UK may face new challenges and opportunities to advance their interests in global governance and exert influence vis-à-vis others.

- **Digitalisation and emerging technologies also provide state and non-state actors with tools for exerting influence more rapidly and at a greater scale, particularly in the information environment.** Telecommunication infrastructures including optical fibre, light-fidelity, and 5G networks are, for example, providing enabling tools for accessing as well as disseminating information and knowledge, and therefore influence, more rapidly and widely than ever.[3] These tools allow actors to communicate with greater number and variety of different audiences, leading to rapid dissemination and internationalisation of narratives and phenomena (e.g. conspiracy theories). As a result, actors including the UK face new questions regarding the required pace and reach of activity through which they exert influence, and how the increasing pace and complexity of global phenomena, such as the spread of false or misleading information on social media, can be effectively mitigated.
- **Lastly, technological advances can provide competitive advantages for some state and non-state actors over others and contribute to the redistribution of power across different actors and societies**. Emerging technologies can amplify or constrain efforts by state and non-state actors to shape international politics and thus contribute to wider systemic change in the distribution of global power. Multi-national corporations and non-governmental organisations play an increasing role in national strategies and geopolitics, either through directly shaping global governance or with governments leveraging industry to develop partnerships and shape international development. As new technologies enable the democratisation of different political, diplomatic, economic, trade and financial activities, civil society and private sector actors are also increasingly engaged in co-designing and co-delivering new ways of providing diplomatic services. This poses new questions as to which actors the UK engages with to exert its influence and which may, on the other hand, constrain its ability to do so, requiring the FCDO to adapt more rapidly to a changing global power distribution between state and non-state actors.

These various impacts of technological change create many adaptation challenges and introduce greater uncertainties regarding the adequacy of existing organisational structures, practices and ways of working. In the context of increasing pace and complexity of technological change, the FCDO should therefore build greater resilience and adaptability to this landscape, recognising that:

---

communities. It has also leveraged TikTok and WeChat to appeal to anti-Western sentiments in different regions and extend censorship and surveillance systems to its diaspora. France has also used digital services (mostly Twitter, webpages and apps such as Ariane) to increase engagement with the French and foreign civil society, promote French culture and francophonie abroad, and advocate for democratic principles and freedom of expression.

[3] China's Belt and Road Initiative (BRI), and more specifically its Digital Silk Road, is often highlighted as the most relevant example of telecommunications infrastructure-building being used as a means of creating new trade ecosystems, deepening existing trade relationships, and ultimately exercising and projecting influence overseas. However, this is not exclusive to the PRC – Japan has, for instance, also incorporated telecommunications infrastructure building in its foreign policy when it launched its Expanded Partnership for Quality Infrastructure (EPQI) and Blue Dot Network (BDN) initiatives to foster economic relationships and counterbalance the influence of China in the Asia-Pacific.

- Significant shifts in the distribution of power or practices through which power is exercised are not likely to materialise out of isolated technological advances. Rather, such shifts are likely to emerge out of the **interaction among multiple technological trends**, such as advances in artificial intelligence (AI) and the proliferation of smart devices and ICTs.[4]
- The impact of technological advances should also not be considered in isolation from **political or socio-cultural trends that shape how technologies are adopted and used in society.** For example, the exploitation of AI in disinformation should be considered in the context of a wider decline in public trust in institutions and the media and the declining role of fact in public discourse – a trend also known as Truth Decay.[5]

How can the FCDO engage with private technology companies to influence and promote the responsible development and use of data and new technologies?

As digitalisation and the maturing of emerging technologies advance, so does the imperative for the UK to engage with private sector actors on issues of key interest to the UK in the context of national security and prosperity as well as global governance. There are several potential priority areas for this engagement, each characterised by dilemmas and trade-offs between the harnessing of technological advances for public good and mitigating the potential risks stemming from the same utilisation of these technologies:

- **Content moderation**: Content moderation is the key mechanism through which private sector actors address challenges of mis- and disinformation as well as online harms. As content moderation practices evolve (including through algorithmic content moderation), there has been an increasing recognition of the dilemma between addressing online harms more effectively and efficiently through automation and the risks this poses to freedom of expression and the democratic civic space. Engagement with the private sector is thus required to, as a first step, improve transparency of content moderation practices, strengthen accountability and identify opportunities for improving the performance of algorithmic content moderation tools.
- **Privacy and data governance**: As a key pillar of the global digital economy, data sharing provides myriad opportunities for strengthening human rights safeguards, advancing international development and national prosperity. However, exploitation of data as an economic and governance commodity and lack of security and data protection safeguards in technology development can present new risks to human rights as well as national security. As such, new principles and approaches are required to provide and promote sufficiently robust privacy and data protection safeguards that are fit for the digital age.
- **Responsible innovation**: A key area of concern for the UK and its international partners and allies is to ensure that opportunities for the innovation of emerging technologies, including AI, are maximised but align with relevant ethical and human rights safeguards. Addressing it will require the development of new technology governance models that are sufficiently future-proof to limit the risk of unintended consequences and corresponding impacts on

[4] See Bellasio, Jacopo, Linda Slapakova, Luke Huxtable, James Black, Theodora Ogden. 2021. 'Innovative Technologies Shaping the 2040 Battlefield'. Santa Monica, Calif.: RAND Corporation (forthcoming).

[5] See Jennifer Kavanagh & Michael D. Rich. 2018. 'Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life'. Santa Monica, Calif.: RAND Corporation. https://www.rand.org/pubs/research_reports/RR2314.html

societal resilience and human rights, while avoiding excessive risk aversion which would constrain the pace of innovation.

While the international community has historically relied on self-regulation by platforms and other private sector actors, it is increasingly recognised that the above-described dilemmas cannot be resolved or navigated through this mechanism alone. There is, however, ongoing debate over the standards and principles which should guide the interaction of states and global technology companies in a matter that allows emerging technologies to be harnessed effectively and in line with established international human rights frameworks. **The FCDO will thus necessarily have to navigate a dynamic field in which perspectives and evidence on 'what works' continue to evolve**. There are several overarching principles which the FCDO can implement in this context:

- The UK has various mechanisms at its disposal ranging from national regulation to 'softer' regulatory approaches such as international standard-setting and promoting codes of conduct. As some of these mechanisms may be outside of the FCDO's remit, the FCDO should clearly identify how its activities cohere and align with those of national regulators, wider UK government and other organisations within the UK. Cross-government and wider national engagement should be ensured to identify common principles (including those relating to international human rights safeguards) as well as issues of interest where the FCDO can make a difference through engagement with platforms and other private sector stakeholders.
- Further to cross-government coordination, the FCDO should pursue engagement with global technology companies in collaboration with the UK's international partners and allies to identify and foster consensus on key standards or principles where possible (e.g. in relation to privacy and data protection). The FCDO's engagement with civil society organisations in different countries and regions should also complement direct engagement with global technology companies to strengthen local capacity to provide additional accountability mechanisms and lobby the private sector from different political, economic and cultural contexts.
- Evolving information and technology governance models will require an inclusive global perspective. To date, however, discourse on relevant new standards and principles has been dominated by the Global North, despite the impact that practices such as content moderation have in the Global South. This has limited understanding of the local and regional nuances that shape the effectiveness of different regulation and governance practices. The FCDO should therefore seek to promote global inclusivity in the context of its own engagement with private sector actors and international organisations on issues such as content moderation.

Should the Government's approach to meeting the challenges of technology nationalism and digital fragmentation be based on self-sufficiency, joining with allies or like-minded nations or supporting a coherent global framework?

With intensifying global power competition and efforts to centralise information and technology governance at the national level, the future global information environment may feature the emergence of the 'splinternet'. This denotes 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. Further to the challenges this may pose for the human rights landscape and the UK's ability to project and exert influence in the information space, this may reduce the UK's technological edge over others or drive

global innovation within reduced normative and ethical constraints, thus increasing the risk of wider societal harms.

As these challenges evolve, the UK needs to consider whether to build self-sufficiency, collaborate with selected partners or foster global coherence depending on its own capabilities, priorities and perspectives on the ethics and human rights dimensions of technological innovation. **These options may not be mutually exclusive, but rather pursued in a mutually reinforcing way on the basis of a comprehensive assessment of the costs, risks and benefits of different areas of UK action.** In this sense, the FCDO should consider:

- Engaging with wider UK government to identify technological areas in which sovereign control over technology development may be essential in the context of a geopolitically fragmented information and technology environment (e.g. critical national infrastructure and technologies used in the context of intelligence). In tandem, engagement with UK industry and academia could help identify national skills and capabilities that the UK could use to develop these technologies and grow UK industry globally, with corresponding opportunities to extend UK influence.
- Engaging with selected like-minded partners to ensure coherence, strengthen interoperability and build consensus on the normative and regulatory aspects of information and technology governance. Such engagement would be key to reducing the vulnerability of the UK technology sector in light of increasingly fragmented global technology markets and mitigate potential risks of adversaries exploiting power vacuums that may emerge out of a geopolitically fragmented information and technology environment.
- Fostering global action to promote the universality of human rights in the context of digitalisation and technological innovation. Through this, the FCDO can help conceptualise risks associated with the 'splinternet' in well-established international human rights standards as well as the international sustainability and development agenda (e.g. through explicitly linking unrestricted internet access to the right to education and global health).

In considering the different options for sovereign action, international partnering or global initiatives, **the FCDO will require a clear articulation of its 'value proposition' to different target audiences, including governments, international institutions and civil society organisations in various countries and regions of interest**.[6] This should take into account potential areas of unique capability and expertise the FCDO as well as wider UK government and other organisations within the UK (incl. industry and academia) can offer.

It should be noted that **increasing technology nationalism and digital fragmentation are not certain to materialise, and the FCDO can thus take proactive steps to reduce risks of a global 'splinternet' emerging in the future**. Civil society engagement can serve as a bottom-up mechanism to strengthen the capacities of local actors to actively shape national policy and regulation. This could help to avoid or mitigate increasing restrictions on internet and technology access as well as provide a global monitoring and reporting mechanism on the impacts of technology nationalism and digital fragmentation.

[6] For a more in-depth discussion of this concept, see Black, James, Richard Flint, Ruth Harris, Katerina Galai, Pauline Paille, Fiona Quimbre, Jess Plumridge. 2021. 'Understand the Value of Defence: Towards a Defence Value Proposition for the UK'. Santa Monica, Calif.: RAND Corporation (forthcoming).

How can the FCDO help build resilience in civil society, in Government, business and foreign relations against the threats posed by abuses of new technologies by state and non-state actors? Can the FCDO support trust-building networks?

Acting at the intersection of foreign relations and development, the FCDO is uniquely placed to influence international policy and practice, build trust, support capacity building initiatives, and contribute to resilience-building through innovation, both within the UK and globally. The FCDO is also well-placed to recognise and assist in mitigating the potential negative impacts of rapid technological innovation, particularly those that inhibit the realisation and protection of human rights in a digital age. Building capacity both internally within the FCDO to navigate this rapidly changing context, as well as externally to strengthen institutional and civil society capacity in partner nations will allow the FCDO to assist in building resilient governance mechanisms and adaptable civil society partners around the globe.

To use capacity-building effectively and strategically, the FCDO will need to consider how its capabilities and expertise best align with the requirements of its target audience. This will require a nuanced understanding of the FCDO's own knowledge, expertise, and capabilities, particularly unique capabilities and expertise held within the department and the wider UK government. Several additional principles should be considered:[7]

- The FCDO could invest its existing capacities in both institutional (top-down) and civil society (bottom up)-based interventions as a **combinatory and holistic framework** that uses elements of each. Key principles in this context will be incorporating knowledge and insights from across the UK government in capacity-building initiatives and striving to embed an active focus on diverse perspectives.
- To build trust effectively and ensure the options proposed result in durable impact, the FCDO will need to **work collaboratively with local stakeholders and key target audiences** to identify appropriate solutions while ensuring local ownership. This should include the tailoring of capacity-building interventions to gaps in local capacities and infrastructure (e.g. considering the limits to connectivity) and ensure that interventions reflect local cultural and socio-economic nuances.
- Foreign relations and development initiatives are inextricably interlinked. Ensuring that the UK's partners overseas are able to build technological and societal resilience in an age of rapid digital innovation is vital in contributing to long-term global stability. Thus, **integrating technological resilience capacity-building into FCDO-funded programming and wider diplomatic efforts** would assist in the development of resilient governance mechanisms and societies in partner and beneficiary countries where this resilience may not yet exist.

Finally, the FCDO should be able to capitalise on past successes and its global reputation to **continue to build on established principles and good programming practices to maximise the impact, sustainability, effectiveness, and efficiency of its activities**. Good practices such as comprehensive planning, risk assessment and evaluation and embedding knowledge-, skills-, and competence-transfer in capacity-building initiatives should serve to maximise learning and foster long-term ownership, trust, and resilience.

---

[7] See Bellasio, Jacopo, Linda Slapakova, Fiona Quimbre, Sam Stockwell. 2021. 'Human Rights in the Digital Age'. Santa Monica, Calif.: RAND Corporation (forthcoming).

About RAND Europe

RAND Europe is a not-for-profit policy research organisation that helps to improve policy and decision making through independent research and analysis. RAND Europe's work includes recently published or forthcoming studies for the UK and European governments, institutions, and other organisations on human rights in the digital age[8], technology and the future of cybercrime[9], and the role of emerging technologies in the context of border security[10], counter-disinformation[11] and defence.

For more information about RAND Europe's research in this area, please contact:

Ruth Harris
Research Group Director – Defence, Security and Infrastructure
RAND Europe
Westbrook Centre, Milton Rd
Cambridge, CB41YG
United Kingdom
rharris@randeurope.org

June 2021

[8] https://www.rand.org/randeurope/research/projects/protecting-human-rights-in-the-digital-age-.html

[9] https://www.rand.org/pubs/research_reports/RRA137-1.html

[10] https://www.rand.org/pubs/external_publications/EP68583.html

[11] https://www.rand.org/randeurope/research/projects/using-machine-learning-to-detect-malign-information-efforts.html