Written evidence submitted by Nesta (TFP0032)

About Nesta - Next Generation Internet team:
This response has been prepared by the Next Generation Internet team at Nesta, the UK's Innovation Foundation. The NGI team primarily works on thematic areas related to the resilience, sustainability and trustworthiness of the internet and technology governance, both areas of great relevance to the Integrated Review.

Respondents:
Katja Bego, Principal Researcher and Future Internet Lead, Nesta
Markus Droemann, Senior Public Affairs and Policy Manager, Nesta

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

The next decade is likely to present a period of unprecedented technological change, with adoption of new innovation across various sectors of our economies and societies set to accelerate in lockstep. This pace of change, as rightly pointed out in the Integrated Review, means it is more important than ever for Britain to be at the forefront of these developments, understand the possible directions of travel, and work closely with like-minded allies to ensure technological innovation does not further contribute to an already charged geopolitical landscape, infringes on fundamental human rights, or worsens the climate crisis.

This accelerated technological change will furthermore not happen in a vacuum. Rising competition over innovation and its governance will be matched by similarly increased geopolitical rivalry over, for example, space, our open seas, and the Arctic. The interplay between these dynamics means it is likely that we will see existing and future innovation being deployed in contexts we currently cannot fully anticipate. To understand these types of emerging complexities and risks, it is therefore vital that the FCDO continues to maintain a robust foresight and horizon-scanning function, tasked with exploring the possible futures that might emerge when we explore the clash points between such mega-trends (think here also of systemic risks related to aging populations - most major powers are expected to see their populations shrink by 2050, polarisation and the fragility of the global world order, urbanisation and (de)globalisation).

In any case, several technologies will inevitably be at the core of these tensions, notably artificial intelligence and new tools for cyber and hybrid warfare, all of which are already extensively discussed in the review. In our response below, we focus on several additional areas that may be less high on the current agenda, or are otherwise particularly illustrative of the kinds of newly emerging risks that may come to a head in decades to come.

Green Tech and shifting resource dependencies: The UK's renewed focus on climate diplomacy, its role in convening COP26, and its leadership position in developing solutions key to facilitating the green transition, from zero-emission vehicles to AI, put the country in a strong position to promote the responsible and sustainable adoption of green tech. It however also necessitates taking a long view of the shifting resource dependencies that the widespread adoption of clean energy and green tech is likely to induce.

Connected and emerging technologies play a unique dual role in the fight against climate change and environmental degradation. They can both exacerbate and help solve global challenges such as escalating carbon emissions or depleting resources. With the advent of the IoT and 5G, the rapidly growing proliferation of connected devices risks enabling a blind 'tech-solutionism' that might do more harm than good, with the increased environmental footprint that comes with the production and deployment (and resulting induced demand) of these kinds of systems possible outweighing the energy savings they are meant to help facilitate.

As the UK incentivises the adoption of green technologies at home and abroad, especially in developing countries, it should also actively promote awareness of the trade-offs involved in adopting technological solutions to address environmental challenges. Where technology is deployed at scale to tackle environmental challenges, the cost-benefit of the entire technological lifecycle should be considered and, where appropriate, provisions should be made to enable the reclaiming and recycling of devices, as well as the off-setting of such activities.

The recovery of rare minerals in discarded devices does not only have environmental benefits but can also become a geopolitical imperative. The success of renewable technologies, for example, is likely to shift global power dynamics and resource dependencies away from oil-rich countries towards countries that control access to certain metals and rare earth elements, vital in both green and connected device supply chains.

As a result, control over these resources is increasingly hotly contested, furthering regional instability and creating risky dependencies in vital supply chains. Resource-rich countries may also find themselves under foreign political influence as a result of selling or trading control over mining operations to strategic competitors. For example, the DRC accounts for roughly 60 per cent of the world's cobalt output, but over 99 per cent of it is exported to China. In the long term, such arrangements are likely to affect the UK's direct relationships with countries in question, and could even shift alliances in international fora and global governance bodies, e.g. when it comes to technological standard-setting or voting behaviour in UN bodies.

Quasi-platforms and meta-platforms: Responding to the social, political and economic challenges of the digital economy, the UK has developed a promising, emerging approach to platform regulation, led by strong agencies and based on the enforceability of codes of practice. However, given their central role in the transnational digital economy, the UK cannot afford to act alone in reining in the power of platforms, whether through content regulation, competition rules or tax frameworks. This presents a formidable challenge since global consensus-building, for example on digital taxation in the OECD, is a slow-moving process incompatible with the rapidly changing nature of the technology landscape.

As the UK's approach to platforms continues to take shape domestically, the FCDO and the UK's regulators and agencies should continue to capitalise on their convening power and expertise - in research, policy and foresight - to champion the adoption of effective, forward-looking, anticipatory platform regulation everywhere.

In particular, the UK should promote an approach that remains sufficiently flexible to capture new services and technologies that do not currently qualify as platforms, but which - advertently or inadvertently - share many key characteristics. For example, these new services may serve gatekeeper functions, facilitate the accumulation of vast datasets, or steer social interaction, collaboration and influencing. Such 'quasi-platforms' may range from stock trading apps, which can be used across borders to exercise political speech and economic influence, to online video games, which are used for content delivery, advertising and social interactions. They will by definition escape easy categorisation, which presents a challenge for lawmaking but may find an effective response in anticipatory regulation.

In addition to quasi-platforms, another transnational challenge, especially from a competition perspective, is the rising popularity of meta-platforms, which combine the services of multiple platforms and services. Meta-platforms could adopt even more powerful gatekeeper roles, controlling the discoverability of online content and services, and leading to a greater centralisation of both data and economic activity.

A particular case of the meta-platform is the 'multiverse', a concept still in development but already garnering significant global investment. Building on the trend towards platformisation in online games, the multiverse, or several multiverses, would act as a virtual environment connecting users, delivering content and enabling transactions in a far more immersive and game-like experience than today's social media or video games. Without global and anticipatory regulation, successful 'multiverses' could become a de-facto infrastructure, sitting alongside the world-wide web, centralising the functionality of search engines, social media, advertising networks, online marketplaces, video games, audiovisual streaming and other content delivery platforms. If widely adopted, metaverses would significantly increase the complexity of regulating content, while raising new questions about net neutrality, accountability, competition and discoverability.

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

Collaborating without creating new dependencies: The UK's 'own-collaborate-access' and 'business science' frameworks provide sensible approaches to support, build and use capabilities in technological priority areas. However, it should not open a backdoor to an over-reliance on private sector technology companies when it comes to the provision of public sector services. The government should furthermore be vigilant when it comes to giving access to large amounts of public sector data that could put major tech companies, which as it stands already control vast amounts of personal data and benefit from significant network effects, an ever greater competitive advantage. The past two years have shown how many governments, in a scramble to respond to the unprecedented events of the COVID-19 pandemic, have turned to private sector companies for short-term technology fixes to understandably highly complex issues. As the dust starts to settle on the pandemic, the government must make sure these short-term crisis solutions do not lead to long-term lock-in.

Supply chain resilience: The Integrated Review rightly points out the need for the UK to diversify and secure its supply chains. This includes securing access to key production inputs, such critical minerals, but also extends to commercial and public sector technologies,

including telecommunications equipment and data-intensive services. The COVID-19 crisis has brought dependencies and systemic opacity back to the fore, setting in motion a period of supply chain relocalisation and diversification across the West, as well as a renewed push for building trust in technology, for example through open source development and hardware audits.

It may be in the UK's interest to use this momentum to return to the domestic development of critical technologies, while simultaneously championing more transparency and diversity across the value chain. The UK should also work closely together with allies to ensure diversification of the most critical upstream nodes in the supply chain - the recent semiconductor shortages have shown how overreliance on narrow chains can often go unnoticed until problems emerge. In an increasingly contentious geopolitical landscape, overreliance on in some cases only one or two companies in the global supply chain (such as Dutch ASML and Taiwan's TSMC) is bound to lead to further - likely more disruptive, and perhaps deliberately manufactured - crises in the future.

Scrutiny of foreign investment: the UK's Investment Security Unit, which is meant to protect intellectual property and companies against national security risks and intervene in inward investment where necessary and appropriate, should adopt a broader understanding of what constitutes a national security risk and relevant asset. Over the coming years we can expect to see companies that would not normally be considered systemically important or a critical infrastructure continue to accumulate increasing amounts of personal data, health data, and other types of sensitive or competition-relevant data. For example, mobile games are becoming an increasingly important source and beneficiary of data harvesting. With state-owned or state-affiliated actors beginning to invest in the sector on a large scale, the potential downstream use and abuse of data collected by these companies should come under greater scrutiny, as they have in the United States and India. We must also be wary of the single points of failure the accumulation of such enormous data sets can produce, an argument in favour of redecentralisation of the data economy and various aspects of the internet's stack more generally.

Public procurement: Government spending and investment can make the public sector a crucial player in the market for innovation. This approach has already been adopted in the Government's Social Value in Procurement framework and its Green ICT procurement strategy, among others. By combining proactive procurement with forward-facing, bold regulation and sharing UK expertise in these areas with partners globally, the UK can set standards for the kinds of technology and innovation we want to see. In the technology sector, this might include setting conditions for interoperability and data portability, promoting more ethical and accountable AI systems, or defining minimum standards for the repairability and lifespan of procured technology. Steering the development of new technology in this way also helps governments themselves to become a market for responsible alternatives, which would otherwise find it difficult to find a sustainable path to profitability.

4. How can the FCDO use its alliances to shape the development of, and promote compliance with, international rules and regulations relating to new and emerging technologies? Is the UK taking sufficient advantage of the G7 Presidency to achieve this?

We welcome the efforts the government is taking in putting technology governance on the top of the agenda of the UK's G7 presidency, with particularly the planned Tech Forum in September a highly-necessary intervention at a time when global conversations about technology have become especially wrought. The Tech Forum should be used as an opportunity to agree on a shared set of values between like-minded nations, but should also take concrete steps towards kicks-starting a truly global forum for setting world-wide rules and norms around the governance of cyberspace (and acceptable state behaviour in this context - an area currently woefully underregulated, but one where the UK can play an important leadership role), as well as reaching agreements on responsible behaviour in space and in the increasingly fuzzy landscape of future conflict (from new forms of hybrid warfare to the the use of autonomous weapons on the battlefield).

The UK government must also work closely together with allies in the Global South, to ensure that both national governments and civil society actors in these countries can meaningfully participate in the often resource-intensive and opaque multi-stakeholder processes that underpin our current internet governance system. This does not just create a more resilient and diverse standard setting process, but also prevents these countries from shifting their priorities towards the multilateral, nation state-driven standard-setting bodies, which are unfortunately often dominated by countries that hold different values when it comes to the use of government repression and surveillance. In our current era of grey war and increased competition, standard-setting processes will become increasingly politicised and a potential tool countries will try to leverage to strengthen their own spheres of influence.

5. 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?

The government's approach should involve a combination of all three of the above, but should always keep the promotion of openness and shared global governance approaches as its ultimate aim.

In the currently wrought geopolitical landscape, such a commitment to openness and cooperation has proven to not always be advisable or even possible. Indeed, recent events have shown that self-sufficiency, particularly when it comes to the security of and access to key production inputs and critical underpinning infrastructures (from undersea cables to 5G to the storage of data), might indeed be a worthy objective. However, this renewed focus on achieving technology sovereignty must not come at the expense of championing values like privacy, sustainability and fair competition.

A retreat behind borders is furthermore leading to increased fragmentation of the technology and digital sphere. The weaponisation of standard-setting processes is already emerging as one of the key new areas of geopolitical competition, a worrying trend that the UK can contribute to countering by ensuring governance processes remain open and representative, for example by promoting continued multistakeholderism and preventing further fragmentation of the internet itself (which currently appears on a path towards the eventual emergence of a fully-fledged splinternet through the proliferation of incompatible, competing standards, for example around 6G).

As standard-setting processes have become an increasingly effective theatre through which to exert power and shape future innovation, the UK and its allies must become more proactively present in these fora, and ensure values-led approaches remain at the core of new governance frameworks. A recent example where only a handful Chinese companies were involved in shaping the ITU's new rules around facial recognition technology, an area of innovation widely considered to be particularly high-risk, shows the risks involved with inaction.

There should furthermore be efforts to renew collaboration with both the United States and the European Union, built around strengthening norms and rules around shared principles and values. Different fora might be appropriate for different actions - from bilateral collaboration in certain cases, to, for example, championing NATO's efforts to devising shared rules for deploying artificial intelligence in a security context, or indeed the G7's Tech Forum in September.

7. 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?

Beyond shaping more inclusive standard-setting processes, and helping ensure the security and resilience of underlying infrastructures and systems, the FCDO can also play an important stewardship role in the development of safe and fair technology - particularly in support of civil society and press freedom around the world. It can do this through launching a dedicated FOSS fund, inspired by the US' Open Technology Fund but with a broader remit, and supporting the development of digital public infrastructure.

FOSS fund: the UK should consider launching - potentially in collaboration with like-minded allies, notably the European Union, a dedicated fund for the development of open source, secure solutions for, for example, secure communications, to help empower journalistic outlets and civil society worldwide. This fund should have a relatively broad remit to fund and maintain alternative open source solutions outside of this more political realm as well.

Open source, interoperable alternatives can challenge the dominant platforms and ensure the UK and allies can reduce their reliance on a handful of Big Tech companies determining what we read, see and share (platforms that have in many ways began to act more as de facto infrastructures than individual solutions on top of the internet's existing infrastructures).

Digital Public Infrastructure: The FCDO - in collaboration with other government departments - can further bolster these efforts by boldly investing in the development of digital public infrastructures, which could help move the logic of the current digital economy away from business models that favour the accumulation of data by an ever-smaller number of powerful actors, towards one that is more distributed - and thus more secure and fair- by nature; a move from a platform to a protocol economy.

We see growing momentum around the idea of digital public infrastructure across Europe and the United States (premised on the idea that every citizen should have access to their own secure digital identity and personal data wallet, which would empower them to share their own data with third parties on their own terms. This in turn would allow new entrants to

the market to compete meaningfully without having to resort to accumulating their own data lakes); the UK government should seize the initiative in bringing these ideas to fruition.

June 2021