Written Evidence Submitted by Tony Blair Institute for Global Change (TFP0026)

The following submission represents the collated views of tech and public policy experts at the Tony Blair Institute for Global Change (TBI). As an inter-disciplinary group of policy experts drawn from the tech industry, government, and academia actively working with stakeholders across the intersection of the tech industry and politics, TBI is well placed to respond to this inquiry on Tech and the Future of Foreign Policy.

A. EXECUTIVE SUMMARY

The new union of DFiD and the Foreign Office into the FCDO aims to reduce the division between development and foreign policy into a forward-thinking entity that acknowledges the fundamental role of development in safeguarding British interests and values overseas. New and emerging technologies are exponentially increasing the surface area in which these interests need to be secured and promoted whilst irrevocably transforming the environment, issues and tools of traditional diplomacy and foreign policy. The shift in the nature and distribution of power in the technological age has led to countries seeking to alter the balance of power through co-opting the international system with self-interested policies that threaten the liberal world order that the UK seeks to promote. The economic and social power of the tech companies has created a new class of non-state multi-national actors whose role is critical in global stability. New and emerging technologies also create enormous opportunity that can be harnessed to support the development and poverty reduction aims of the FCDO and promoting fundamental UK values of democracy and human rights. To achieve these aims, the FCDO has an opportunity to build an integrated digital foreign policy strategy that is rooted in liberal and democratic values and advocates for new forms of multilateralism and multi-stakeholder engagement that will allow the UK to leverage its role as a technology superpower.

We recommend that the FCDO:

- Establishes a tech-first foreign policy strategy that takes account of how technology cuts across almost all domains and is a core part of 21st century diplomacy and multilateralism.

- Develops a tech diplomatic corps to liaise with private tech companies through policy pipelines to bilateral tech hubs and clusters globally.

- Actively supports an open and progressive vision of the internet as central liberal democratic values and critical to supporting emerging economies reaping the full economic, social and cultural benefits of the tech revolution.

- Leverages the UK leadership of the G7 to ensure that like-minded nations coordinate a consistent and coherent message in international standards setting bodies for responsible and ethical standards within new technologies.

- Coordinates alignment between UK departments engaging in international fora to ensure the development of international standards and governance initiatives that support responsible development and use of new and emerging tech such as distributed ledger technology (DLT).

- Provides broad international cyber-security cooperation including technical assistance and capacity building that not only reduces the global digital divide, but also supports the growth of emerging digital economies and facilitates the beneficial uses of new and emerging technologies.

B. RESPONSE TO INQUIRY

The Potential Impact of New Technologies on UK Power & Influence

Long before Vladimir Putin's statement in 2017 that the state that controls AI will rule the world triggered a new level of technological power competition, the potential of new emerging technologies was growing exponentially. Whilst each advance in machine learning, quantum processing, autonomy, nanotechnology, biotechnology, and distributed ledger technologies offer the potential to alter traditional notions of great power competition, it is in the interdependence of these technologies that the greatest challenges and opportunities lie. The increased surface area has altered the economic, social and economic environment in which foreign policy has operated with new paradigms of power and power distribution, new types of conflicts, challenges to norms of sovereignty and the liberal ideal of global interdependence. New foreign policy issues have emerged from cybersecurity to maintaining a free and open internet, and traditional diplomatic tools have been recalibrated to include digital diplomacy efforts.

The Integrated Review envisions building strategic advantage through the growth of the UK's science and technology power, as well as leading as a responsible and democratic, cyber power. The vision for expanded regulatory, science & tech and cyber diplomacy is underpinned by the objective of the UK being a "force for good" in the international arena. However, the associated proliferation of tech-oriented departments and programmes creates risks of lack of coherence and policy confusion when trying to address the spectrum of 1000 global digital policy processes & initiatives.

Countries such as Switzerland, Netherlands, France, Denmark and Australia have designed digital foreign policy strategies to have a holistic approach to the intersection of tech and foreign policy objectives. This has included creating new diplomatic structures such as tech ambassadors, ensuring collaboration between national government departments, and incorporating multi-stakeholder initiatives. The FCDO has a more bird's-eye view of tech's transformation of the environment, issues and tools of foreign policy and development which they should leverage to build an integrated digital and technology foreign policy strategy and ensure that FCDO interests do not become secondary to the individual interests of the various commissions and taskforces. The FCDO needs to ensure that new and emerging technologies are developed and used to strengthen its work as a "force for good" and maintain its soft-power. For example, if the FCDO is engaged in building Disarmament, Demobilisation & Reintegration or refugee assistance programmes, an integrated digital and technology foreign policy strategy would support and promote technologies such as digital ids or digital payments that would increase the efficacy of the programmes. But it would also develop the regulatory frameworks that could protect against the potential risks of new tech deployment, for example the lack of access and cyber security.

It is recommended that:

- The FCDO establishes a digital and technology foreign policy strategy that connects across technology and complex societal issues such as trade, health, education, capacity development, and human rights. This should coordinate across government departments to ensure a coherent tech foreign policy that is consistent in its approach and promotion of liberal and democratic values throughout the supply chain of foreign policy tools and services.

FCDO engagement with private technology companies for responsible development and use of data and new technologies

As the private sector are the primary creators and exporters of technology it is critical that they are engaged in visualising the frameworks to promote the responsible development and use of data and new technologies. The private technology companies, as creators, have the unique understanding of the potential of their technologies, although they may not always see the potential misuse. An integrated foreign policy framework that incorporates input from a broad base of stakeholders across disciplines and levels will challenge technology companies to consider potential misuse of their technologies at all levels of the supply chain during the innovation process. Co-creation should be encouraged across governments and beyond to the private sector, for example the FCDO should work with DCMS to champion and support the UK as a global leader in safety tech innovation. This will lead to safer technologies as well as a more robust vision of standards, norms and regulatory frameworks that the FCDO needs to promote in international fora. Ensuring that private companies are integral in developing the solutions will ultimately lead to greater responsibility to ensure compliance with the frameworks.

It is recommended that:

- The FCDO should expand its influence and collaborate with the private sector, academia, research, and civil society. It should do this through defined policy programmes, where the aim is to agree broad alignment of objectives, which all parties can own and deliver.

- Practically this means expanding its network of bilateral tech hubs, clusters and tech ambassadors in key global tech centres. This can also include building pipelines through innovation fellows representing key technologies within the FCDO that as well as coordinating with private technology companies on solving grand challenges presented by the potential misuse of new technologies. This would coordinate private sector participation in diplomacy and would put the UK on the frontline of influencing the responsible use of data and harnessing emerging tech for social and public good.

Leveraging alliances to shape the development of, and promote compliance with, international rules and regulations relating to new and emerging technologies

The playing field of international bodies involved in developing rules and regulations for emerging technologies has the potential to become a battleground between large powers. This is becoming an increased concern in standards setting bodies that shape discrete elements of emerging technologies. China's influence in these bodies as well as through the MOUs on standards that it has established with 80-90 countries as part of the BRI & Digital Silk Road could potentially lead to governance models contrary to the UKs liberal and democratic values and that may limit the FCDOs international development objectives.

UK leadership of the G7 provides the opportunity to ensure that like-minded nations coordinate a consistent and coherent message in international standards setting bodies for responsible and ethical standards within new technologies. This would support the UK's objective – outlined in the Integrated Review – to become a technology superpower. Extending models such as the US-led Quad Critical Technology Working Group and the S10, like-minded nations should work together with China in ensuring the neutrality of standards bodies. The FCDO integrated digital technology strategy should take the leadership across UK departments to work towards standards for development of secure, resilient, reliant and trustworthy technologies and governance models that protect innovation, FCDO development goals and the UK's power and influence.

It is recommended that:

- The FCDO should assume leadership of an inter-departmental taskforce on emerging technology standards, rules and regulations to align all representation in international bodies and groups of like-minded countries as well as to ensure that approaches are consistent with the FCDO's objectives.

- To ensure coherence of interests when engaging in technology diplomacy and representing the UK in negotiating rules and regulations, the FCDO should provide for a trained cadre of tech ambassadors at embassies and consulates. Key principles of values for rules, standards and regulations for emerging technologies and data governance should be a fundamental part of FCDO training.

Responding to the challenge of technology nationalism & digital fragmentation

The proliferation of conflicting regulatory, geopolitical and governance approaches in international institutions and standards may appear to protect states' self-interest in the short term but over time creates divergence and friction that reduces the long-term value and potential of technology. In the absence of proactive cooperation, China has played a major role projecting its internet governance model across the Indo-Pacific, Africa and the Middle East, through the BRI & Digital Silk Road.

It is imperative that liberal democracies cooperate in establishing global frameworks to limit the expansion of restrictive internet models abroad, resist authoritarian standards proposals and supporting emerging economies to adopt open internet infrastructure & policies. This is increasingly relevant in regions in which data governance regimes are nascent, such as the

Middle East, where data localisation raises concerns that data regulation activities could be used for law enforcement rather than protecting consumer privacy and supporting digital trade.

The UK should leverage its G7 presidency to provide active leadership on data governance and encourage cooperation between like-minded nations on promoting internet standards & governance bodies that support internet openness, as well as providing more effective and competitive internet infrastructure support for emerging economies. This should be part of a wider FCDO integrated digital strategy that engages with data governance models in key strategic geographies, such as the Indo-Pacific, and ensures that the internet ecosystem as a "force for good."

It is recommended that:

- The FCDO should promote a new model of internet internationalism that coordinates with like-minded countries in assuming leadership of internet standards and governance bodies to limit the expansion of restrictive and unilateral models that fragment the internet ecosystem.

Navigating the opportunities & challenges of cryptocurrencies and distributed ledger technologies (DLTs)

The development of cryptocurrencies and DLTs will have a transformative effect on traditional foreign policy tools, monitoring compliance with international agreements and enforcement mechanisms, as well as offering tremendous opportunities for the development goals of democracy promotion and poverty reduction. It is important not to conflate cryptocurrencies with the potential of other applications of DLTs that can be used in securing payment systems and supporting digital governance that boost liberal and democratic values. Similarly, blockchain based technologies can be utilised in ensuring compliance in trade agreements e.g. ensuring sustainable fishing.

Blockchain technologies and cryptocurrencies present a number of challenges to sanctions regime enforcement for the UK and its allies. There have been attempts by states to create state-sponsored cryptocurrencies in order to bypass international oversight including Venezuela's attempt to launch the Petromeda (Petro) and threats from Russia and Iran to follow similar paths. The UK Cryptoassets Taskforce brought together HM Treasury, the FCA and the Bank of England to consider the impacts of DLTs, however, there has been little discussion of the intersection with foreign policy or the new UK sanctions regime introduced in July 2020.[1] The US Cyber-Digital Task Force spearheaded by the US Department of Justice has been more active in setting out approaches for addressing the challenges of cryptocurrencies[2] though the Cryptocurrency Enforcement Framework that has facilitated the seizure of cryptocurrency used for terrorist financing and imposition of economic sanctions for virtual asset related malicious cyber activity. The US model highlights the potential of inter-departmental cooperation to be able to address the threats of cryptocurrencies to international regulatory and criminal enforcement efforts, as well as the primacy of international collaboration to ensure cooperation on cross-jurisdictional enforcement. The initial US enforcement actions also highlight the need

[1] Cryptoassets Taskforce Final Report (October 2018)

[2] Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Framework (October 2020)

to ensure clarity of approaches so that industries do not withdraw from the positive uses of DLTs in order to avoid falling foul of the sanctions regime.

It is recommended that:

- The FCDO convenes a multi-stakeholder and inter-departmental blockchain network to extend the current UK Cryptoassets Framework in line with foreign policy objectives. This should include a new programme of policy and regulatory sandboxes including the Ministry of Justice, the NCSC, NCF, the Counter-Terrorism Operations Centre, Department of Trade, National Economic Crime Centre, industry stakeholders and international law experts to synchronise understanding of DLTs with an integrated digital foreign policy strategy.

- The UK coordinates with its G7 partners to formulate principles for global governance of DLTs that harnesses the stabilising benefits of DLTs whilst providing sufficient transparency, cooperation and partnerships for prosecution and enforcement of those misusing the global virtual asset ecosystem.

- The FCDO should coordinate with the Department of Trade to take a leadership role in the WTO exploring the role of DLTs in FCDO & WTO ensuring compliance with international trade agreements.

- The FCDO establishes a multi-stakeholder network to incubate DLTs that support the UK's agenda addressing democracy promotion and poverty reduction abroad including the gradual integration of DLTs in e-voting, promoting trust in charitable organisations, the administration of public services and social problems, and the development of regional and interorganisational private blockchain networks to encourage enterprise adoption.

Building resilience against abuses of new and emerging technologies

Just as the changing nature of conflict has required strategic shifts such as the introduction of multi-dimensional peacekeeping strategies, the increase and diversity of actors utilising new technologies and the consequent vulnerabilities requires technologically resilient development strategies. The UK cyber-power and defensive cyber capabilities plans in the Integrated Review address building resilience on a national level, however, there was less attention paid to the role of technology as part of the "force for good" objectives of the FCDO development agenda.

The interconnectivity of the digital and cyber ecosystem requires that FCDO development programmes must harness the positive uses of digital and tech tools whilst simultaneously strengthening capacity to protect against abuses. Encouraging digital banking without building the capacity to prosecute cyber-criminals limits the potential value of FCDO's strategic aims in supporting emerging digital economies. The FCDO should use its digital development and capacity building force to support the development of cyber governance institutions in emerging digital economies. FCDO strategies should help societies reap the benefits of digitalisation whilst providing the tools to limit the negative externalities.

It is recommended that:

- The FCDO should coordinate inter-departmental and international initiatives to strengthen the international mechanisms that combat cybercrime and consumer harm threatening advanced and emerging digital economies.

- The FCDO integrated strategy should promote broad international cyber-security cooperation including technical assistance and capacity building to reduce the global digital divide, support the growth of emerging digital economies and facilitate the beneficial uses of new and emerging technologies in democracy promotion, poverty reduction, and protection of human rights.

ACKNOWLEDGMENTS:

This response has been prepared by Dr Melanie Garson & Max Beverton-Palmer with contributions from: Kasra Aarabi, Blaise Bayuo, Andrew Bennett, Dr Henry Fingerhut and Daniel Rey.

We would be pleased to offer further evidence to the committee or to answer any follow-up questions. Please contact m.garson@institute.global and max.bp@institute.global.

1 June 2021