Written evidence submitted by BAE Systems plc (TFP0018)

At BAE Systems, we provide some of the world's most advanced, technology-led defence, aerospace and security solutions. We employ a skilled workforce of 89,600 people in more than 40 countries. Working with customers and local partners, we develop, engineer, manufacture, and support products and systems to deliver military capability, protect national security and people, and keep critical information and infrastructure secure.

BAE Systems Applied Intelligence

BAE Systems Applied Intelligence delivers cyber security and intelligence solutions which help our clients protect and enhance their critical assets. Building on our strong heritage of security and defence, our solutions and services help nations, governments and businesses around the world defend themselves against cybercrime, reduce their risk in the connected world, comply with regulation and transform their operations.

We have worked with the Foreign, Commonwealth and Development Office (FCDO) for many years and are a major cyber provider to the British government at home and around the world. As an FCDO supplier we also work very closely with the department to promote British industry and products abroad.

BAE Systems has responded to the specific questions below to support the inquiry carried out by the Foreign Affairs Select Committee.

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

As the UK government department responsible for protecting and promoting British interests around the world, it is the task of the Foreign, Commonwealth and Development Office (FCDO) to seek to strengthen its understanding of technology and its cascading impact on the UK's global role and influence.

Technology, in all its forms, offers myriad opportunities and threats to the UK's global interests. But when examining shifting power, not all technology is equal. While broad digitalisation and cloud technologies offer the UK a new opportunity to increase its global influence, other technologies, such as artificial intelligence (AI), quantum computing, biometrics and 5G/6G, have frequently been lauded as having the potential to help the UK extend its power overseas and counter the influence of its adversaries.

This requires an alternative narrative: one that promotes open choice and evidences how nations and populations can make themselves resilient to subversive influence through greater education and awareness. This is seen both from a technical level (for example, putting in place measures to detect when election influence is happening), as well as helping ensure that countries themselves become more resilient to this type of activity.

A number of countries are active in this sphere and others. These actors are not only strongly influencing global standards in emerging technology, but also acquiring and stockpiling key materials and minerals for existing technologies, such as rare earth metals and lithium. By influencing global standards, these actors will help domestic manufacturing industries take increasingly dominant positions in supply-chain deliveries, impacting global prices with potential serious negative global impact. The FCDO has an opportunity to steer

these countries towards more rules-based frameworks and avoid such scenarios from taking root.

In addition, the technology trends and associated challenges around the proliferation of information sources on social and traditional media has loomed large in recent years. This is likely to continue, primarily due to difficulties around governance and control of the many entities active on these platforms, including multinational corporations and state actors.

Technologies which are shifting power here include specific applications of AI, such as deep fakes of politicians in leading democratic countries, including the UK. Other countries particularly at risk are those which do not have robust democratic institutions or which lack the capability to deploy a more nuanced approach than simply switching off their internet in response to issues such as fake news or misinformation.

As a specific application of AI, deep fakes can have a very relevant impact on state influence, but AI in general can be both a force for good and bad. For example, there is an opportunity (one already recognised by the FCDO's Open Source Unit) for AI to be used to gain a better, more complete understanding of the public mood in all countries by using it to analyse data on social media – while at all times adhering to applicable laws and regulations. However, this opportunity could also be seen as a threat as it depends on the context in which it is being used. This is because AI, when applied to social media, accelerates the insights that can be gained from data on social media, and this can be used to automate responses and thus accelerate manipulation of sentiment through the same social media platforms.

Technology is also reshaping national security. Other nation states are increasing their investments in AI and autonomy in their military and the UK is doing the same: the recent Integrated Review called for a greater use of synthetic environments, AI and machine learning across all defence operating environments and against future threats to national security, which now encompasses risks facing the UK's wider Critical National Infrastructure, including healthcare.

The resilience of the NHS has never previously been considered in the same light as nuclear power plants, for example, or elements of the defence industrial base. However, Covid-19 has highlighted the importance of the security resilience of healthcare-related technologies, particularly around vaccine development and other leading-edge research – as evidenced by repeated attempted cyber hacks of vaccine research around the world since the onset of the pandemic.

And finally, when considering the FCDO's understanding of new technologies and their effect on the UK's influence, it would be remiss not to highlight how the department *itself* can use technology to strengthen its mission and wider diplomatic efforts.

The FCDO oversees a vast set of embassies and high commissions; a massive legacy that gives the UK a competitive advantage over other nations which lack such a genuinely global network to call upon.
The department has historically been very effective at bringing together information from across this network and using it to shape the UK's foreign policy. The FCDO has already made good strides in the field of digital diplomacy, including more than 700 official social media profiles across the world. This helps the FCDO achieve its foreign policy goals and proactively manage its image and reputation via content tailored to the unique characteristics of local audiences.

The department has also not been afraid to innovate: it was the first foreign ministry on Snapchat; the first to use Twitter for customer service on travel advice; UKinUSA was the first on BuzzFeed; its embassy in New Zealand was the first to use Periscope; and it was one of the first to broadcast via Facebook Live. In 2016 the then FCO was named best social media user, Snapchat user, blogger of the year, and Facebook page of the year, among the world's ministries for foreign affairs. Increased use of this expertise for further insight, as well as communications, is critical to keeping the UK at the forefront of global diplomacy.

Better use of data can also further strengthen this information pipeline, delivering deeper, more nuanced insights, helping the UK's understanding of shifting trends, as well as enabling the UK to be better informed of the activities of its allies and adversaries. For example, effective use of big data can help diplomats prepare for complex negotiations, removing bias on possible impacts and generally strengthening evidence-based decision making. Diplomats could also use a combination of geospatial data, satellite imagery and on the ground intelligence to forecast migration waves or humanitarian crises.

Furthermore, the digital trace left by online societal behaviour, of the type mentioned above (Twitter, Facebook and so on) captured in the form of researchable data, offers data scientists, including those in government, a unique insight into how to devise more effective policies and to increase understanding of global responses to global issues. Naturally, there are security-related restrictions on the types of software permitted to be installed on diplomats' computers, but enabling our government representatives to get hands-on experience of data analytics tools and fostering a culture of research to optimise genuine use of the data available, could significantly increase the UK's local understanding and wider influence in diverse geographies.

The FCDO also needs to be aware, though, that technology has levelled the playing field, enabling countries with a smaller network to achieve a more effective global reach. In the past, the department could rely on the sheer volume of its data to be better informed than other countries. Now, staying ahead of smaller nations requires a new cadre of trained data scientists and engineers to enter the diplomatic service, with the cost implications of recruiting such specialist staff.

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

Regular dialogue between the private sector and the FCDO, and the broader public sector, is vital to promote responsible behaviour and champion the British values of openness, fairness and transparency. The government can also use its regulatory powers through the likes of the National Cyber Security Centre and the Department for Culture, Media and Sport.

When it comes to international standards and norms, particularly those relating to technical standards which demand a high level of expertise, the FCDO should consider acting as a facilitator for industry to help represent the UK in international industry standards fora, such as the European Telecommunications Standards Institute.

Industry subject matter experts can use their participation in such fora to help develop international norms and standards. It's also important to remember that many companies are multinational, with interests that span the globe. This means they can play a unique role in trying to push for norms and government policies and rules that help support business.

When engaging abroad, through the FCDO working with such companies, as well as local organisations, a united front can be presented in promoting the UK's overseas interests across both the public and private sectors.

Digital trade and the cross-border flow of data is another area where there is a real opportunity to make an impact. Measured by bandwidth, cross-border data flows grew roughly 112 times over from 2008 to 2020 and this is only going to grow as broadband access spreads across the globe. But while goods and services have rules about how they are traded across borders, there is no data equivalent to the World Trade Organisation. Data rules are limited to pan-jurisdictions, such as the European Union's GDPR while in the UK, the Department for Culture, Media and Sport (DCMS) is responsible for leading engagement with countries around the world to identify and issue adequacy findings with whom personal data can be shared with minimal additional controls.

With the current international and trade investment frameworks designed long before the current globalisation trends, communications boom and pervasive IT, this is an ideal area for the FCDO to be influencing global policymaking: the department can play a role in building a world-leading understanding of the issues and promoting openness, fairness, transparency and democracy while working with DCMS to help ensure appropriate privacy standards.

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?

Each of these suggested approaches have merit, and to best address the challenges of technology nationalism and digital fragmentation the Government's approach should include elements of all three: the UK needs to be self-sufficient, it needs to work with allies and it needs to support a global framework.

While self-sufficiency alone is completely untenable and unaffordable for such an interconnected set of problems, countries *do* need to be self-sufficient in those things they literally can't do without, while also being flexible enough to join with other nations when needed. The definition of what constitutes critical technology is evolving as technology changes, and it's important to maintain self-sufficiency or at least be able to call upon robust supply agreements for those things deemed critical. Traditionally, this would have been defence equipment but now could include items such as vaccine technology.

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.

We recommend close collaboration with the European Union on emerging standards, particularly on emerging quantum communications standards through such international bodies as the European Telecommunications Standards Institute and the International Telecommunications Union. Such a move will help counter the attempts of other countries to strongly influence these standards to suit its space satellites and exploit emerging quantum communications technology.

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?

Part of addressing the threat of misinformation and also abuses of technologies will be down to resilience in society, such as awareness and education. This is really about countering the influence and reach of state actors in the UK's partner countries in Africa, Asia and so on, while also finding issues of common ground on which to build up trust and support relationships.

When it comes to building resilience, it's important that the FCDO leads from the front – there is an opportunity for the department to demonstrate best practice use of technology and security following the recent merger between the Foreign and Commonwealth Office and the Department for International Development.

For example, the department could work closely with the Centre for Data Ethics and Innovation (supported by DCMS) and the AI Council to support academic research on responsible usage of emerging technology. It could do this by promoting its digital strategy of shifting resources and programmes online, together with highlighting the efforts of other parts of government to digitally transform their operations – all of which can be done because it can rely on effective cyber security.

In dealing with challenges of emerging technology and resilience, the UK has a strong history of assurance, which is about building robust systems supporting critical events such as elections, the use of biometrics or AI and building greater trust in algorithms and machine learning. The way to do this is by getting the assurance right. Wherever we are talking about enabling the take up of technologies, part of that is advocating a robust approach to the assurance of these technologies. The UK has a good story to tell and that's something the FCDO could be taking global. It also resonates with messages about Secure by Design promoted by the NCSC.

Another technology to promote trust building networks is financial services; one of the UK's core strengths. Promoting financial inclusivity is an important enabler for developing economies but there are cyber threats which make people worried about depositing their money into particular applications or mobile banking. The FCDO can help run programmes to build trust in these services as where a population is adopting banking more generally, then this is a positive societal development.

May 2021