Written evidence from Simon Jones (TFP0016)

I have been invited to submit evidence on the basis of my role as the co-author of the Harvard Belfer Center's National Cyber Power Index 2020 (NCPI)[1], published September 2020, and co-founder of Dartkite, a data-driven consultancy group.

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

The NCPI provides a comprehensive assessment of national cyber power for the 30 most active countries in the cyber domain. Our research shows that much of the debate around national cyber power focuses only on cyber offense and defence, without accurately characterising the way different countries employ their cyber capabilities and with too little understanding of the domestic and foreign policy objectives they attempt to achieve through cyber means. We have identified eight broad objectives that countries, including the UK, pursue via cyber means:

1. Domestic surveillance: Surveilling and Monitoring Domestic Groups;
2. Cyber defence: Strengthening and Enhancing National Cyber Defences;
3. Information control: Controlling and Manipulating the Information Environment;
4. Intelligence collection: Foreign Intelligence Collection for National Security Purposes;
5. Industrial growth: Commercial Gain or Enhancing Domestic Industry Growth;
6. Wealth generation: Amassing Wealth or Extracting Cryptocurrency;
7. Destructive capabilities: Destroying or Disabling an Adversary's Infrastructure and Capabilities; and,
8. Norms: Defining International Cyber Norms and Technical Standards.

Overall, in the NCPI the UK was ranked as the third most powerful country in the world in cyber terms, behind only the US and China.

While this is impressive, of the 23 countries included in the NCPI that had published more than one national cyber strategy, each one has increased the range of national objectives it is seeking to pursue via cyber means. Therefore, if the UK simply maintains its current cyber efforts, it risks letting others overtake it.

The NCPI highlights a number of key areas in which the FCDO should focus its attention:

1. While the UK was the highest scoring country for 'norms' intent, it was only ranked seventh for 'norms' capability. To enhance its 'norms' capabilities, the FCDO should seek to increase the breadth and depth of its international cyber engagement. It should look to sign bilateral cyber agreements with like-minded countries, and improve its engagement in multilateral organisations and treaties. The FCDO should develop an overarching strategy for shaping international cyber norms, which should include the ends, ways, and means that the FCDO will bring to bear to influence international cyber and IT technical standards organisations.

[1] Julia Voo, Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy and Anina Schwarzenbach. 'National Cyber Power Index 2020.' September 2020. Retrieved 10 May 2021, https://www.belfercenter.org/publication/national-cyber-power-index-2020

2. For the 'information control' objective, the UK only ranks seventh for both capability and intent. The US is the highest scoring country for intent for the 'information control' objective, emphasising the importance it places on combating foreign propaganda and terrorist communications, with China and Russia the second highest and third highest scoring countries respectively for intent for the 'information control' objective. The UK should be more assertive in the information space, signalling its willingness to call out and attribute foreign propaganda and disinformation. The FCDO should also seek to engage NATO and European Allies in this mission: notably, beyond the UK and US, only Germany and France are in the top 10 for intent for this objective, with Germany and France ranked eight and ten respectively.

3. Countries are increasingly using cyber capabilities for commercial gain or to enhance their domestic industries. This includes both state-sponsored industrial espionage to steal technology from overseas, as well as efforts by countries to develop their cybersecurity workforces and industrial bases through investment and public-private partnerships. The UK ranks third in intent terms for this objective, which is impressive given that China and Iran, who occupy first and second place, are suspected of having conducted or sponsored industrial espionage. The FCDO has an important role to play in deterring countries from pursuing industrial espionage and helping to build mutually beneficial partnerships with like-minded countries on cyber skills and technology development.

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?

It is welcome that the Integrated Review articulates the UK's desire to be a 'responsible and democratic cyber power', acknowledging that to achieve this the UK must take 'a whole-of-cyber approach'[2]. However, there is little detail in the Integrated Review about the FCDO's vision for cyber and tech diplomacy, the specific goals it will achieve by delivering this vision, or the ways it will use data to inform cyber and tech diplomacy and decision-making.

Building on the NCPI's findings, the FCDO can enhance UK cyber power in a number of ways, including:

Data driven assessments of the cyber priorities of allies and adversaries. Knowing a country's cyber priorities allows the UK to better defend itself against threats, compete with adversaries, and complement allies. The NCPI is based on entirely open source and publicly available materials and while we acknowledge that this has limitations, we have been able to quantify and measure national cyber power. The FCDO should enhance its ability to measure the progress of countries to meet their cyber priorities, and its ability to identify

[2] 'Global Britain in a competitive age. The Integrated Review of Security, Defence, Development and Foreign Policy.' March 2021. Retrieved 12 May 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf

influential cyber actors within countries. It should use this analysis to inform its country engagement strategies and develop influence campaigns.

Leverage public-private partnerships to compete in cyberspace. Russia and China are the highest and second highest scoring countries for intent for the 'domestic surveillance' objective in the NCPI. Given the high priority these countries place on this objective, to compete in cyberspace the UK could seek to prevent the export of technology that enables surveillance of domestic populations. The FCDO could collaborate with privacy and internet freedom groups, and also support the development of products and services that allow citizens in repressive regimes to access accurate and uncensored news and information.

Build and grow networks of independent organisations to tackle and refute disinformation.

The percentage of British citizens on social media and receiving their news from internet-based sources creates a fertile ground for adversaries to exploit with disinformation and propaganda – in part explaining why the UK only ranked in seventh place in capability terms for the 'information control' NCPI objective. The FCDO should seek to amplify the voices of independent organisations that can help to analyse and attribute disinformation and propaganda, including think tanks, research centres, and universities, bringing these bodies together to share analytic best practices and research. Related to this, the FCDO should also ensure that it quickly responds to foreign disinformation, referencing independent analysis where possible to strengthen its case.

Horizon scanning and private sector engagement. Increasingly, online services, social media platforms, and new technology used by UK consumers will come from Asia Pacific. The FCDO can play a greater role in anticipating data privacy and security considerations associated with these products by analysing and examining them as they come to prominence in their domestic markets, and whether they adhere to common security and privacy standards.

To enable this, the diplomatic network should build and maintain meaningful links with private sector tech firms and research institutes in Asia Pacific and beyond. The FCDO should deploy technologists, commercial experts, and personnel with practical experience of cyber governance, compliance, and risk management to countries with significant tech hubs to help identify and anticipate emerging technology. It should also make better use of open source and market data to identify organisations of interest and measure the impact of its engagement.

May 2021