Written evidence submitted by the UK Computing Research Committee (TFP0001)

Call for Evidence on Tech and the Future of UK Foreign Policy[1]

Compiled on behalf of the UK Computing Research Committee, UKCRC.

UKCRC is an Expert Panel of the British Computer Society (BCS), the Institution of Engineering and Technology (IET), and the Council of Professors and Heads of Computing (CPHC). It was formed in November 2000 as a policy committee for computing research in the UK. Members of UKCRC are leading computing researchers who each have an established international reputation in computing. Our response thus covers UK research in computing, which is internationally strong and vigorous, and a major national asset. This response has been prepared after a widespread consultation amongst the membership of UKCRC and, as such, is an independent response on behalf of UKCRC and does not necessarily reflect the official opinion or position of the BCS or the IET.

Prof. Chris Johnson
Pro Vice Chancellor (Engineering and Physical Sciences), Queen's University Belfast.
c.w.johnson@qub.ac.uk

Response:

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

[1.1] Machine Learning and AI have increasing application, from the chatbots and recommendation engines used widely in eCommerce to vision systems and facial recognition in autonomous vehicles, security systems and weapons. The UK has strength in AI research, However, it is important that policy makers are aware both of the strengths and limitations of this technology in relation to the impact this it might have on Foreign Affairs. AI can identify trends in social media and in wider forms of public discourse at different levels of granularity both within and across national borders. However, it is less well suited to determine the implications of those trends for UK policy.

[1.2] Current machine learning systems are powerful at finding correlations in huge datasets but they are not "intelligent": they cannot usually justify their actions, correlations are often coincidences, the training data often contains biases that the AI system inevitably mimics, and the correlations may be spurious and based on inappropriate criteria and may be 'brittle' in that tiny changes to the object may cause the system to misidentify it. Such systems should only be used with extreme caution, informed by human judgement, where any error could cause serious harm. The UK should prioritise collaborative research to exploit the strengths of AI to inform Foreign Policy, to mitigate the weaknesses in current AI whilst recognising that achieving human-scale intelligence is beyond current research horizons.

[1.3] The UK has great strengths in an area known as *systems engineering*; this brings together design, safety and regulation across all the engineering disciplines with a strong focus on the end-users of technical innovation. This inter-disciplinary approach has enabled the UK to develop high-value systems with a record of reliability and integrity that other nations have struggled to replicate in areas ranging from aircraft engines to healthcare and renewable energy generation. These approaches are likely to be increasingly important because most software development contains large numbers of defects, many of which lead to cybersecurity

[1] https://committees.parliament.uk/call-for-evidence/420/tech-and-the-future-of-uk-foreign-policy/

vulnerabilities. Our ever-growing digital society is therefore built on weak foundations. Our reputation for high-integrity systems engineering creates opportunities for us to help other countries in re-engineering national critical infrastructures that are resilient to future threats and failure modes.

[1.4] UK domestic policy can also be informed by the approaches being developed within systems engineering. Current strategies to address these vulnerabilities tend to be reactive rather than strategic and cannot be effective until it becomes the norm for critical systems to be built using provably safe and secure methods.

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

[2.1] The FCDO already benefits from a number of strategic alliances – for example, working to promote the UK cyber security industry with overseas partners. These initiatives have helped to develop international markets but have not, so far, been focused on the *responsible* development and use of data and new technologies. These issues have been considered by UK Research and Innovation working with BEIS and also, to a certain extent by the Centre for Protection of National Infrastructure through its Trusted Research Guidance[2].

[2.2] There are significant opportunities to learn from other countries. In particular, Israel and Singapore have leveraged domestic strengths in AI and cyber security to increase their international influence. Research investment has been coupled with policy support – for instance through the use of regulatory 'sandpits' for the development of autonomous systems. Such initiatives have created technological eco-systems; which encourage and sustain the international growth of domestic private technology companies.

[3] How can the FCDO engage with private companies to encourage internationally accepted norms for the use of social media as well as to maximise the benefits for diplomacy presented by social media?

[3.1] The largest social media companies are too large for national governments to be able to regulate them effectively. There are technical, ethical and fiscal limits on the ability of individual countries to influence these companies.

[3.2] The UK should collaborate closely with overseas partners either to refocus existing organisations or potentially create new mechanisms for establishing consensus and encouraging joint action where social media is jointly perceived to violate accepted norms. This is likely to require changes in international law; informed by a thorough understanding of the technical underpinnings of social media.

[3.3] The FCDO should encourage our partners to inform and be informed by the innovative work of the Competition and Markets Authority (CMA) within this area – for instance, as they work to ensure 'influencers' [3] and on-line gambling companies [4] continue to comply with UK law. We also welcome their work on algorithms, competition and consumer harm which identifies a number of the domestic and foreign policy concerns we have mentioned relating to the use of AI[5].

[2] https://www.cpni.gov.uk/trusted-research-guidance-academia

[3] https://www.gov.uk/cma-cases/social-media-endorsements

[4] https://www.gov.uk/cma-cases/online-gambling

[5] https://www.gov.uk/government/publications/algorithms-how-they-can-reduce-competition-and-harm-

[3.4] We would also encourage the Committee to consider and promote the recent work of HM Treasury on the UK approach to Cryptoassets and Stablecoins as a further strong example of government considering the implications of technical innovation on both domestic and foreign policy[6].

[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?

[4.1] We would argue that the UK should promote the work of the CMA and HM Treasury with our overseas colleagues, during the G7 Presidency. As mentioned in [3.3] and [3.4], they have coupled a sound understanding of the technical infrastructures, together with a sensitivity to a host of social and ethical issues and their background in market regulation. This provides a template that others might usefully copy.

[4.2] Encouraging others to follow the model established by these initiatives is also likely to increase the effectiveness of the CMA's and HM Treasury's work. Many of the intentions behind their engagement with emerging technologies require the support and cooperation of our international partners.

[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?

[5.1] There is a delicate balance to be struck between 'technology nationalism' and 'digital sovereignty'. On the one hand, the UK benefits immensely from our diverse, international supply chain; providing access to leading technologies that support industry and enrich our daily lives. On the other hand, this creates almost unique levels of inter-dependency and vulnerability to disruptions in global supply chains either as a result of policy changes or other contingencies.

[5.2] We cannot make ourselves self-sufficient across the broad range of emerging technologies, nor should we try to do so. Digital fragmentation and the diversification of technical engineering talent across the world makes it unlikely that we would ever be able to sustain leadership across anything but a small subset of infrastructures.

[5.3] We would, however, advocate a risk-based approach that identifies and safeguards the technical and engineering infrastructures upon which the UK depends. Where appropriate this may be done through global inter-dependencies across diversified supply chains. In other contexts, we should take the considered decision to work with like-minded nations to ensure we do not become dependent on any other single nation for core infrastructure technologies that might then be used as a strong external lever on UK foreign and domestic policy.

[6] What opportunities and challenges do cryptocurrency and distributed ledger technologies such as blockchain present for the way the FCDO does diplomacy (for example, enforcing sanctions), and

consumers/algorithms-how-they-can-reduce-competition-and-harm-consumers

[6] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf

how can the FCDO harness these technologies as new tools of influence or to promote compliance and transparency in international agreements?

> [6.1] Section [3.4] of our response has already made reference to the excellent work of HM Treasury through their consultation on the UK approach to Cryptoassets and Stablecoins[7]. We would encourage the Committee to work with them on the wider implications of this for UK Foreign Policy to ensure a "joined up" approach especially with respect to Stablecoins.
>
> [6.2] Distributed Ledger Technologies (DLTs) have a role to play where a secure decentralised database and transactions are important. Such applications are relatively uncommon. It would be unwise to incorporate blockchain and similar DLTs into critical infrastructure without very high assurance that the system architecture, implementation and protocols are secure and will remain so for decades. Any use of DLTs within diplomacy would need to consider, for example, post-quantum cryptography.

[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?

> [7.1] We recognise the value of the UK National Risk Register [8] in helping build resilience in civil society, in Government and business.
>
> [7.2] There are clearly lessons that need to be learned from recent events, see for example the work of the Lords Select Committee on Risk Assessment and Risk Planning [9].
>
> [7.3] However, we note the UK National Risk Register is not primarily focussed on the implications of those hazards and threats for foreign relations. The FCDO might be encouraged to develop an addendum, which traces these implications especially as they relate to the changing nature of technology. For instance, one side effect of the pandemic has been to increase our reliance on networked systems both for video communication but also for the distributed control of key infrastructures. This has clear implications for the cyber security and supply chain concerns raised in sections [5.1-5.3] of our response.
>
> [7.4] It is important that the focus of the National Risk Register includes significant investment in risk reduction as well as in resilience; UK foreign policy provides means of intervening to reduce external threats. Future national security will depend on a joint approach to reducing the impact of each risk materialising, and on diplomacy to reduce the probability that they will materialise.

[8] What would the implications be of the dollar losing its dominant position for international transactions? Will digital currencies force a change in the balance of power?

> [8.1] As mentioned in section [3.4] and [6.1] of our response, HM Treasury has conducted a detailed and excellent analysis of the implications of cryptoassets as part of their on-going consultation in this area.

[7] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf

[8] https://www.gov.uk/government/publications/national-risk-register-2020

[9] https://committees.parliament.uk/committee/483/risk-assessment-and-risk-planning-committee/

[8.2] It seems unlikely that the dollar will lose its ascendency at least in the medium term as the dominant means of international transactions – however, there are distinctions to be drawn between e-money tokens that can be redeemed at face value at any time, security tokens which are akin to electronic securities and unregulated tokens that include bitcoins etc. A key concern in any increased reliance on the last of these for international transactions is their present volatility – leading to the development of 'stablecoins' which often retain a link to a fiat currency; such as the dollar.

[8.3] HM Treasury is proposing to create a new regulated category of 'stable tokens' and has proposed a number of principles guiding their actions in this area. We would welcome support from the FCDO in promoting this work and in encouraging other countries to adopt broadly similar principles.

10 April 2021