NCC Group—written evidence (DRG0005)

House of Lords Communications and Digital Committee inquiry into Digital Regulation

Introduction

NCC Group is delighted to have the opportunity to engage with the Lords Communications and Digital Committee's important inquiry. As a UK-based global cyber security and software resilience business, we have a deep understanding and experience of the ways in which regulatory and non-regulatory interventions have – and in some cases have not – driven up security standards in the digital sphere. It is through this lens that we are keen to offer our support and expertise to the Committee.

The digital landscape is incredibly complex, changing at pace and is increasingly embedded in all parts of the economy and society. As the digital landscape evolves, so too does the threat landscape. The use of new, evolving and interconnected digital technologies inevitably presents new security risks. Meanwhile, the arsenal available to hostile actors who could target digital technologies is constantly developing. Good, evidence-based and data-driven regulation plays a central role in ensuring the right steps are taken to minimise these risks and maximise cyber security.

Against this background, we welcome the Government's recently published Plan for Digital Regulation – in particular its commitment to build a common framework for digital regulation that is outcomes-focused and keeps the UK safe and secure online. We believe, however, that the UK's approach to digital regulation could be strengthened in the following ways:

- There needs to be a shift away from the current reliance on advice, guidance and voluntary measures to secure the UK's digital systems towards more stringent, forward-looking regulatory intervention and mandating of security requirements. There are many examples where non-regulatory schemes have been under-resourced, have failed to change behaviour and, in some cases, have simply been ignored by affected organisations. Good regulation, on the other hand, can drive positive behavioural change and always comes with giving expertise, capability and resource to regulators to do their jobs meaningfully.

- Flexibility, agility and periodic regulatory and legislative reviews need to be built in from the outset to keep pace with modern technological and societal developments. This ideally should include requirements for regulators and policymakers to engage regularly with innovation centres and industry experts.

- To achieve genuinely forward-looking outcomes, the Government should invest in coordinating and improving horizon-scanning, whilst also engaging digital natives from the outset.

- Efforts should be made to move away from a 'tick-box' compliance approach to security regulation to one where there is a true understanding of cyber threats and accountability at an organisational level. This should include regular and independent assessments of organisations' and sectors' level of real-world resilience, ability to withstand incidents, and shocks across the digital technology ecosystem.

- In assuming a greater role in offering outcomes-based frameworks, digital and sectoral regulators must be strengthened in their powers, resources and capabilities.

NCC Group is passionate about sharing our expertise and insights with policymakers and parliamentarians who are tackling crucially important questions about the evolving digital sphere. We would be delighted to give oral evidence to the Committee's inquiry to help explore the proposals we raise in our submission in more detail.

Questions

1. How well co-ordinated is digital regulation? How effective is the Digital Regulation Co-operation Forum?

The Digital Regulation Co-operation Forum (DRCF) is a welcome recognition that digital regulation cannot be treated as another vertical sector, but needs to be understood as a cross-cutting horizontal that underpins the vast majority of industry sectors today. The DRCF attempts to set shared priorities and collaborate to avoid regulatory contradictions and conflicts are welcome. However, it is, as yet, too early truly to judge the DRCF's effectiveness. It remains to be seen if it can establish itself as an influential forum in the regulatory landscape or will become another body in an increasingly complex landscape.

For the time being, we maintain that the UK's digital regulatory system is complex, often fragmented and sometimes contradictory in its approach. This is particular the case in cyber security. The currently fragmented and inconsistent organisational structures and regulatory environment make it very challenging for organisations effectively and efficiently to improve cyber risk management practices. We do believe that central oversight and coordination should be strengthened, not least to maintain cyber security as a political priority. To drive organisational clarity alongside a clear sense of purpose and direction, we would welcome efforts to:

- Clarify roles and responsibilities of current public sector cyber actors and agencies, including for policy development, technical authority advice (National Cyber Security Centre (NCSC)), regulation and enforcement; and,

- Coordinate and consolidate the number of cyber stakeholders in Whitehall by creating a single cross-government cyber capability.

2. Do regulators have the powers and capabilities, including expertise, to keep pace with developments? What is the appropriate balance between giving regulators flexibility and providing clarity in legislation?

Many regulators struggle to keep pace with developments in what is an extremely fast-moving environment. As a result, most regulation is developed to address a harm that has already taken place, as opposed to being genuinely forward-looking. For example, the Government's 'Secure by Design' proposals for Internet of Things devices – whilst extremely welcome and necessary – followed only after the development of IoT botnet Mirai. Whilst the proposals will stop such botnets in future, the damage has already been done.

To overcome this issue and avoid a knee-jerk approach to regulation, flexibility, foresight – informed by improved horizon scanning (see question 3) and engagement with external experts – and periodic reviews need to be built into the UK's digital regime from the outset. This ideally should include requirements for regulators and policymakers to engage regularly with innovation centres, digital natives and industry experts. UK industry has a wealth of expertise and knowledge which could be more effectively utilised to support regulatory outcomes.

More broadly, we appreciate the greater flexibility that regulation offers to adapt to changing threats and technologies – as opposed to establishing requirements in legislation that quickly become outdated and require (often in demand) parliamentary time to change. However, we believe it is right that fundamental questions of technology regulation – including those related to digital ethics – are first debated in Parliament to set the fundamental framework that guides how the UK approaches technology, digital and cyber security issues.

3. How effective is digital regulators' horizon scanning? How could this be improved?

Effective horizon-scanning and adoption of technical at-machine-speed solutions will be key to achieving a genuinely forward-looking approach to regulation.

At present, there is a myriad of horizon scanning activity and initiatives across government, the private sector and academia, as well as multiple government bodies and advisers whose remit involves considering future risks and opportunities, including the Regulatory Horizons Council, departmental Chief Scientific Advisers, Science Advisory Councils, UK Research and Investment (UKRI) etc. There is significant overlap and duplication of effort, with no central coordination and collation of data. We believe that a review should be conducted to better understand what assessments are already being undertaken across academia, the public and private sectors, and how this analysis could be better coordinated and drawn upon. In simple terms, we feel strongly that there are better mechanisms available to produce data-derived insights into future technologies and their related challenges than multiple excel spreadsheets held in different departments by different accountable owners who, often, do not share information with each other. Instead, we are aware that horizon scanning and strategic foresight is increasingly sophisticated in the UK investment sector where the volume of venture capital or private equity investment often serves as a relevant indicator to identify growth technologies and technology penetration in different markets. Policymakers should consider how they might tap into this analysis to better understand market trends and subsequently assess whether a regulatory response might be required now or in the future.

Further, the Government should consider new and innovative ways of collecting and analysing data in machine readable ways in real time, learning lessons from the private sector and counterparts internationally. For example, Georgetown University's Centre for Security and Emerging Technologies (CEST) Foretell platform is enabling policy horizon scanning in the security and technology sectors on an unprecedented scale. The platform is gathering views from experts on a mass scale, continuously, which it then analyses, condenses and shares with policymakers, with a view to equipping them with the foresight needed to address the challenges and opportunities of emerging technologies. A similar platform – potentially led by the Regulatory Horizons Council – could be established in the UK.

5. What is your view of the Committee's proposal in *Regulating in a digital world* for a 'Digital Authority', overseen by a joint committee of Parliament?

In principle, we support efforts to address the crosscutting nature of digital issues and enable informed and timely policymaking in the fast-evolving digital sphere. We would, however, need further clarity on the remit of the Digital Authority before assessing whether we believe it would be an effective measure.

If it is to be a digital regulator of sorts, we would be concerned that digital technologies will be treated as a vertical sector – which does not reflect their true cross-sectoral nature. We believe the better alternative would be to upskill existing sector regulators with digital skills to allow them to do their jobs more effectively when regulating the way in which their sector is changing and evolving as a result of digital technologies.

A Digital Authority that acts as a central clearing house or source of expertise to collate horizon-scanning data and push this out centrally might be a more effective mechanism for helping sectoral regulators to ensure digital regulation remains up to date. However, policymakers would need to consider how it would sit alongside the existing National Technical Authority for cyber security – the NCSC – and to ensure lessons from the NCSC's experience are learned so that regulators and government departments are required to have regard to the Authority's input rather than take it or leave it as they choose.

6. How effectively do UK regulators co-operate with international partners? How could such co-operation be improved?

When it comes to the digital sphere, no country is an island. We therefore welcome the Committee's question, and believe that international regulatory cooperation should be front and centre of policymakers' and regulators' minds when developing the UK's approach to digital regulation. Indeed, shaping the international order is key objective of the UK's Integrated Review of Security, Defence, Development and Foreign Policy, and has been hailed as crucial to the UK's future national security[1].

[1] https://www.ncsc.gov.uk/speech/lindy-cameron-first-year

In aligning the UK's domestic and international approach, we recommend that the Government:

- Pick priorities to create focus, targeting the biggest global issues such as ransomware and supply chain security;

- Utilise existing successful partnerships, including the 'Five Eyes' alliance;

- Invest time in developing practical outcomes with other governments, that go deeper than high-level principles; and,

- Ensure that civil society and industry – who will play a central role in delivering governments' objectives - are involved in discussions from the outset.

When developing domestic regulation, UK regulators must take into account the international landscape – considering how domestic and international regulation interacts and how this dynamic could impact on the international competitiveness and success of UK technologies and sectors. As a rule, global principles should remain a guiding light for UK regulation. Where UK regulation is world-leading, efforts should be considered from the outset as to how the UK Government will turn UK principles into global principles that others will then have to follow.

October 2021