Foreign, Commonwealth
& Development Office

Wilton Park

Summary Report

Acting responsibly in cyberspace

Monday 14 – Wednesday 16 November 2022 | WP3146

Summary Report

Acting responsibly in cyberspace

Monday 14 – Wednesday 16 November 2022 | WP3146

In association with the Foreign, Commonwealth & Development Office

On behalf of the United Kingdom's Foreign, Commonwealth and Development Office, from 14th-16th November 2022 Wilton Park hosted a dialogue entitled Acting Responsibly in Cyberspace (Conference Number: WP3146). The dialogue included representatives from States, non-governmental organisations, industry and academia. The purpose of the dialogue was to explore, unpack and identify what constitutes the responsible exercise of (State) power in cyberspace. The dialogue was held under the Wilton Park Protocol.[1] A further, more detailed, technical report will follow covering the themes discussed during the dialogue. This summary report provides an overview of the key themes raised during the dialogue.

Cyber 'power'

1. The UK Integrated Review 2021 defines 'cyber power' as 'the ability to protect and promote national interests in and through cyberspace: to realise the benefits that cyberspace offers to our citizens and economy, to work with partners towards a cyberspace that reflects our values, and to use cyber capabilities to influence events in the real world' (p. 40 (for a similar definition see the UK National Cyber Strategy 2022)). Many conference participants accepted that 'power' is a broad notion encompassing a wide range of cyber-related behaviour, going beyond the use of offensive cyber capabilities and including, for example, cyber capacity building initiatives and participation in multilateral ICT processes. However, the term was not without contention, with some participants expressing concern that it implies the use of influence or even force within the international system.

'Responsible' cyber power

2. Some participants noted the difference between the concepts used by the UK National Cyber Strategy ('responsible and democratic cyber power') and the UN Group of Governmental Experts and UN Open-ended Working Group ('responsible behaviour of States in the use of ICTs'). Discussions focused mainly on what constitutes the 'responsible' exercise of cyber power and there was broad agreement as to its core characteristics: accountability, legitimacy, transparency and inclusivity. Discussions indicated the exercise of responsible cyber power is defined in both absolute and relative terms. Responsibility is absolute insofar as there are certain red lines which, if crossed, constitute an irresponsible exercise of cyber power. For example, participants concurred that State-backed ransomware attacks against other States' critical national infrastructure are irresponsible. But beyond these absolute requirements, indicators of responsibility are relative between States.

[1] Further information can be found at http://www.wiltonpark.org.uk/.

3. Concerns were raised that some States feel ‘powerless’ next to advanced cyber powers or even powerful industry actors operating within, across and beyond their territories. These participants emphasised that States possess different cyber capabilities and, consequently, the standards for the responsible exercise of cyber power should be calibrated accordingly.

4. Responsible use of cyber power was considered possible by all States, regardless of their governance structure. In this way, democracy was seen as indicative, if not constitutive, of responsible cyber power.

Capacity building

5. Participants agreed a key characteristic of responsible cyber power is a State’s willingness to support capacity building across the international system, and that advanced cyber powers shoulder a greater responsibility in this regard. Some participants went further and asked whether States owe a responsibility to protect less cyber capable States should they be compromised by a cyber incident. Participants noted that didactic cyber capacity building should be discouraged in favour of collaborative initiatives aimed at building States’ resilience and capabilities.

Private sector

6. Participants emphasised the multidimensional nature of the concept of State responsibility in cyberspace. States should act responsibly in relation to other States in the international system, whilst simultaneously engaging responsibly with the private sector operating in their territories. This requires States to work constructively with the private sector to develop expertise, encourage innovation, maintain digital services in their territories and, where necessary, regulate the private sector to ensure that it behaves responsibility in cyberspace.

7. Through its expertise, wealth, ownership of cyber infrastructure, pace of working and global agility, the private sector yields significant influence over the ICT domain. This recognition led to suggestions that standards of responsible cyber behaviour should be developed for the private sector (as distinct from States). However, some participants cautioned against investing private entities with State-like responsibilities given that they pursue different objectives and serve different constituencies than States. Moreover, such a move may dilute the governance role performed by States at the national and international levels.

Sufficiency of the existing voluntary norms

8. Participants agreed that responsible cyber powers should immediately implement the existing voluntary norms identified by the UN processes. Some participants pointed to the work of the Organisation of American States and Association of South East Asian Nations as examples of regional organisations acting as powerful influencers to implement norms across their member States. Creating additional norms of responsible State behaviour – even through the conclusion of international agreements (treaties) – had some limited support. Some participants gave the example of computer network operations (CNOs) that do not breach an operative rule of international law. For these participants, such operations can be considered ‘legitimate’ (and therefore responsible) only when they are precise, targeted, proportionate and subject to appropriate political and legal oversight. However, some concern surrounded defining responsibility beyond the voluntary norms already agreed through UN processes, fearing ‘arbitrariness’ (in part due to ‘legitimacy’ being subjective and its definition differing between States). Many participants stressed that existing norms remain the bedrock of the international political and legal regime applicable to cyberspace, and cautioned against pursuing any initiatives deviating from, or diluting, these norms.

ICT processes

9. The utility of existing UN processes on ICTs were interrogated. Some participants pointed to the UN's new Programme of Action as being the most appropriate forum to progress ICT-related discussions. There was also consideration of whether a 'UN-plus' model is needed given new developments in cyber security, although participants did not speculate on what form or shape it should take. Other participants expressed concern that moving away from the centralised and inclusive UN processes runs the risk of creating a disjointed approach to cyber governance.

Transparency

10. Participants agreed that transparency is critical to opening effective lines of communication between States and building trust and confidence between them. In particular, States were encouraged to be transparent about the threats they face in cyberspace, how they counter these threats and how they implement their national and international commitments. Some participants urged States to publicise (and, where necessary, update) national cyber strategies as well as national positions on how international law applies to cyberspace. As far as possible, transparent State-use of CNOs was encouraged – including publishing guidelines on the circumstances in which CNOs can be deployed and identifying the restrictions, safeguards and oversight mechanisms to which they are subject. While States were not expected to provide running commentary on their CNOs, secrecy was accepted as the exception rather than the norm – in other words, secrecy is only justified when required by operational sensitivities. Some participants were concerned that certain States are reluctant to speak openly about their cyber activities because they want to wait and see how other States act. But as these participants explained, the problem is that transparency cannot be 'retrospected in' – for trust and confidence to grow, transparency needs to be baked in from the outset. Some participants also noted the benefit of transparency is that it enables States to avoid the 'hypocrisy trap', that is, exercising cyber power without having sought to justify it previously.

Diversity and inclusivity

11. Participants discussed diversity and inclusivity at the international and national levels. At the international level, the importance of diverse and inclusive processes dealing with the identification and implementation of norms was encouraged. Ensuring that these processes are diverse and inclusive was seen as a continuing and adaptive exercise: these processes should be reconstituted as interest and expertise in cyberspace grows and as new realities emerge. The Open-ended Working Group was welcome in this regard for including all States as well as representatives from academia, the private sector and non-governmental organisations (even if the role of non-State actors is actually quite limited). Participants explained that future processes must incentivise and enable un- (or under-) represented communities to participate in cyber security discussions. However, as several participants underlined, achieving diversity and inclusivity is not a box-ticking exercise – stakeholders should be given a meaningful voice in shaping global conversations around cyber security.

12. At the national level, participants explained that States should foster a 'whole of society' approach to cyber security, requiring States to generate societal interest in cyber security, establish education and training initiatives to develop cyber expertise and work with all sectors of society (including marginalised groups) to build capacity and resilience. Some participants also emphasised that interested stakeholders should be given the opportunity to feed into national conversations on the regulation of cyberspace.

Conclusion

This report provides a summary of the key themes emerging from the Wilton Park Dialogue and is not designed to comprehensively document the participants' rich and wide-ranging discussions. Participants were keen to underscore that this dialogue provides a first step in clarifying what the responsible exercise of (State) power looks like in cyberspace and welcomed future efforts to progress these discussions.

Russell Buchan
Wilton Park | December 2022

Wilton Park reports are intended to be brief summaries of the main points and conclusions of an event. Reports reflect rapporteurs' accounts of the proceedings and do not necessarily reflect the views of the rapporteur. Wilton Park reports and any recommendations contained therein are for participants and are not a statement of policy for Wilton Park, the Foreign, Commonwealth and Development Office (FCDO) or His Majesty's Government.

Should you wish to read other Wilton Park reports, or participate in upcoming Wilton Park events, please consult our website www.wiltonpark.org.uk. To receive our monthly bulletin and latest updates, please subscribe to https://www.wiltonpark.org.uk/newsletter/