Report

Acting responsibly in cyberspace

Monday 14 – Wednesday 16 November 2022 | WP3146

Report

Acting responsibly in cyberspace

Monday 14 – Wednesday 16 November 2022 | WP3146

In association with the Foreign, Commonwealth & Development Office

1. From 14th-16th November 2022, Wilton Park hosted a dialogue on behalf of the United Kingdom's Foreign, Commonwealth and Development Office entitled *Acting Responsibly in Cyberspace* (Conference Number: WP3146). The dialogue included representatives from States, non-governmental organisations, industry, and academia and its objective was to analyse what constitutes the responsible, democratic exercise of (State) cyber power. This report provides a summary of the dialogue's main sessions and complements a separate report that offers an overview of the core themes raised during the dialogue (available here). The dialogue was conducted under the Wilton Park Protocol.[1]

Introductory Remarks

2. Participants observed that, until recently, cyber diplomacy was an under-developed niche. However, the rapid integration of cyberspace into every aspect of modern life has led to cyber diplomacy becoming a professional discipline that is at the heart of national and international affairs.

3. Participants agreed that States face a range of cyber threats that emanate from State and non-State actors alike. Participants also agreed that malicious cyber operations represent a threat to national security as well as to international peace and security. To counter these threats, States need to strengthen cyber resilience across their societies, prevent healthy competition spilling over into destructive conflict, and shape an international order that advances common interests and objectives.

4. 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)). Cyber power is therefore a broad concept that includes a range of ICT-related behaviour, not just considerations in the use of offensive cyber capabilities. Participants explained that the question is not whether cyber capabilities should exist or even be used – rather, the question is under what conditions these capabilities can be used responsibly and what expectations should be encouraged of States and other actors to act responsibly in the cyber arena.

5. A main objective of the dialogue was to develop better understandings of the challenges faced by States when formulating cyber policy; develop a shared sense of what the responsible exercise of power looks like in cyberspace; identify what practical steps are needed to ensure the responsible exercise of cyber power; and, overall, explore how actors can work together to create a free, open, peaceful, and secure cyberspace

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

A Vision for Responsible Cyber Power

6. A key theme of this session was that responsible cyber powers must form effective partnerships with all ICT stakeholders. In particular, participants observed that responsible States should work with the private sector to support innovation, grow resilience, share information, and counter cyber threats. State engagement with the private sector can take the form of law, policy, guidance, or *ad hoc* cooperation. Some participants noted that while regulation of the private sector may be necessary, it should be seen as a last resort, explaining that regulation is not an effective substitute for genuine partnerships between States and the private sector. Participants also underscored that countering cyber threats is most effective at the grass roots level – States therefore need to encourage and incentivise good cyber hygiene across all segments of society (the so-called 'all of society' approach to cyber security).

7. Participants agreed that the focus of debate should be on what constitutes the 'responsible' exercise of cyber power. While democracy is an important indicator of whether cyber power is exercised responsibly (because of the checks and balances inherent to democratic models of governance), participants accepted that non-democratic States can still act responsibly in cyberspace. Democracy is thus indicative rather than constitutive of responsible cyber power.

8. Participants observed that the conflict in Ukraine demonstrates the important role played by the private sector in cyber security, such as 'Starlink' keeping Ukraine online during the 2022 conflict and other tech companies protecting Ukraine's data and patching vulnerabilities in its systems and networks. Participants suggested that, in addition to States, tech companies should behave responsibly in cyberspace and this raised the question of what responsibly looks like from the perspective of the private sector and how the sector should be engaged on this issue. First and foremost, participants explained that companies should see themselves as custodians of cyberspace and should act to protect this unique ecosystem. One participant raised the question of whether norms of responsible behaviour should be developed at the international level for the private sector. Another participant expressed concern that this development may weaken the role of the State in the ICT environment and transfer governance-related responsibilities from States to private companies. This was considered problematic given that private companies primarily pursue profits rather than protect and promote national interest.

Acting Responsibly in Cyberspace

9. Given the increase in malicious cyber activity and that cyber threats can emerge quickly and without warning, one participant explained that States have a positive responsibility to exercise their cyber power and counter cyber threats before they emerge. Put differently, this suggests a State's failure to exercise its power to address cyber threats can be seen as irresponsible.

10. Other participants explained some States are concerned by this pro-active exercise of cyber power because it can undermine respect for the principles of sovereignty, non-interference, and independence. They stressed that States must respect international law in cyberspace and especially the United Nations (UN) Charter. For these participants, the key issue is that States work together to develop a better understanding of how international law applies in cyberspace. Clarifying how international humanitarian law (IHL) applies to cyberspace was noted as critical, despite being under-studied by the UN Group of Governmental Experts (GGE)/UN Open Ended Working Group (OEWG) processes. Hope was expressed that the next OEWG report addresses IHL. It was mooted that establishing common understandings of how international law applies to cyberspace may require States to prioritise the common good over national interests, whilst another participant noted broad and permissive interpretations of international law should be resisted because they disadvantage developing States and create instability and insecurity.

11. Some participants saw the UN OEWG as providing the best forum to discuss cyber security issues because of its diverse and inclusive membership. However, it was also posited that non-State actors are still not given a meaningful voice in the OEWG. The UN Programme of Action holds promise in this regard but the critical question is what will be its legitimising principle? Another participant noted that, whatever process follows the OEWG in 2025, the UN's 11 voluntary norms must provide the guiding framework for responsible cyber behaviour and the UN's acquis must be respected.

12. Several participants discussed the role of States in preventing their cyber infrastructure being used for malicious purposes by other actors. These participants emphasised that this is a relative standard – States have different responsibilities depending on their capabilities and priorities and this raised questions for how stronger States can best support those States still developing their capabilities.

13. Several participants stressed that capacity building is a critical feature of responsible cyber power, commenting that States with advanced cyber capabilities have greater responsibility to work with States with less advanced cyber capabilities. Moreover, these participants remarked that capacity building initiatives should be collaborative and cooperative and tailored to meet the needs of the recipient States.

The Role of Legitimacy in Regulating Cyber Behaviours

14. A participant proposed six criteria for cyber operations to be considered legitimate and thus responsible: 1) cyber operations must comply with the requirements of international law and the UN's voluntary norms; 2) cyber operations must be subject to democratic oversight (including political and legal oversight mechanisms); 3) the legal framework governing the use of cyber operations must be transparent (to the extent that operational sensitivities permit); 4) cyber operations must be controlled and targeted; 5) cyber operations must proportionate insofar as they avoid or at least minimise unintended consequences; and 6) decision-making processes must be diverse and include a 'mix of minds'.

15. In response, another participant emphasised the importance of State consent in developing the rules of the road for cyberspace. This participant opined that defining 'responsible' cyber power in terms that go beyond the requirements of international law can lead to arbitrariness given that the notion of 'legitimacy' is subjective. This participant explained that an 'extra-legal approach' to the concept of responsible cyber power raises concern and anxiety for developing States in particular. Another participant explained that a new legal framework may be needed for cyberspace and, if so, a new treaty may be the best way forward. Another suggestion proposed the International Law Commission study the topic of responsibility in cyberspace. Yet, these legislative approaches were also questioned given that different actors are playing different 'games' in cyberspace with little desire to establish universal rules and norms for this domain.

Accountability for Actions in Cyberspace

16. It was noted that there is very little (public) focus on the military's role in defending critical civilian infrastructure from cyber attacks, and suggested that States should consider what an increased role for the military looks like in this context, especially given the blurring between cyber peace and cyber war. Concern was expressed that civilian employees of private corporations (with the support of intelligence agencies) bear the brunt of defending privately owned critical civilian infrastructure and that this responsibility should be (partially) borne by the military; but if not, what are the implications for private citizens expected to participate as front line defenders against cyber hostilities?

17. Some participants were concerned by the growing militarisation of the cyber security profession. Civilian workers increasingly perform roles typically undertaken by the military. This raised questions surrounding informed consent to undertake these roles, and the awareness of the consequences e.g., that civilian operators may become lawful targets under IHL. One participant opined that the militarisation of cyber security runs counter to

the ‘all of society’ approach. Discussions around the militarisation of cyber security raised a broader question as to whether IHL can adequately protect civilians from cyber warfare and whether gaps in protection are emerging. However, another participant rejected the contention that there are gaps in IHL when it comes to the protection of civilians and civilian objects.

18. A participant highlighted the drastic change in the cyber threat landscape in recent years as well as the important role the private sector plays in mitigating cyber threats. This participant emphasised that the private sector must work with governments and users to build relationships of trust and that effective communication is key to achieving this. This participant also explained that governments and the private sector must be upfront about the technological vulnerabilities they face and work together to resolve them. Moreover, governments should work with the private sector when determining attribution because the skills, knowledge, and resources of the private sector can make this process quicker and more accurate.

19. Participants emphasised the importance of self-attribution when it comes to accountability: States should be open about what cyber operations they engage in and how and why these decisions are taken. Yet, some participants noted that self-attribution may not always be possible, or may only be possible in broad terms, given operational sensitivities. Participants explained that self-attribution is critical to stimulating broader conversations around what constitutes the responsible exercise of cyber power.

20. A participant explained that accountability at the national level requires States to implement regulatory frameworks governing their use of cyber capabilities (including cyber strategies, laws, policies, etc.). This view, translated to the international level, holds States accountable to the UN’s voluntary norms, with States required to issue reports outlining how they are implementing them. Reports or surveys on implementation can help raise awareness across the world order of where cyber capacity building is needed. It was contemplated whether a repository for cyber security incidents can be established to share knowledge of malware and malicious actors. These discussions led one participant to question the legitimacy and effectiveness of the UN processes, especially regarding work on norm-implementation. The question was posed as to whether a ‘UN-plus’ model is needed to advance discussions on responsible State behaviour in cyberspace.

Adopting a Collective and Inclusive Approach

21. A participant explained that inclusivity does not in itself make processes legitimate or lead to better outcomes – inclusivity is not a box-ticking exercise. Rather, inclusivity is about making sure the right actors are in the room bearing in mind their skills, knowledge, and experience. Moreover, inclusivity is not just about representation – actors must be given a meaningful voice in discussions. Engagement should also be seen as a gradual and adaptive process: As the ICT environment develops, new actors may need to be integrated into international cyber governance models.

22. Some noted the OEWG adds little by way of inclusivity due to the limited role afforded to non-State actors and the dominant role played by technologically advanced States.

23. The private sector was observed as being not homogenous, but rather includes three main groups: Internet technology companies, companies selling Internet-connected products, and companies selling technology or providing it as a service.

24. The inclusivity of international cyber governance requires the involvement of all relevant stakeholders, which means that States must adopt appropriately tailored engagement strategies. Inclusivity is important because, as one participant highlighted, the cyber security profession can act as an early warning mechanism for cyber threats and vulnerabilities.

Transparency and Trust-building in a Digital Age

25. Participants discussed China's role in building 'smart cities' in Africa and particularly in Kenya, noting the technology provided by China affords operators significant surveillance capabilities over domestic populations, thereby allowing access to vast amounts of biometric data. Whilst the development of 'surveillance cities' in Kenya are justified on the basis of crime prevention, there is little evidence this technology is used for legitimate public needs; yet, there is evidence to suggest it is used to suppress political opponents.

26. China's interest in weaving its surveillance technology into Kenyan society was observed as financial because it generates revenue for Chinese companies. But China's interest is also security based because it enables social control and affords China influence over Kenya and the wider African region.

27. Another participant spoke about the importance of education and training in establishing trust and transparency in cyberspace. This participant explained that the importance of education and training in new and emerging technologies should be enshrined in national cyber strategies and communicated across all levels of society. Ultimately, cyber resilience starts at the individual level.

28. Institutions, such as the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), were praised as leading the way in providing high quality training and education in cyber security.[2]

29. Another participant exhorted governments develop cyber security training initiatives in tandem with the private sector because it is the private sector that has the knowledge and expertise.

30. The value of government transparency was raised, including around the implementation of the UN's voluntary norms because they are key to building trust across the international community. States also need to be transparent about the threats they face and how they respond to them – for example, do they condone the paying of ransoms for ransomware attacks? In particular, it was stressed that States should be transparent about their cyber capabilities from the outset because it is difficult for transparency to be 'retrospected in' later on. Another participant noted that greater transparency can help States avoid the hypocrisy trap, that is, of using cyber capabilities without having first acknowledged their existence.

Applying Principles of Responsible Cyber Behaviour

31. Participants discussed whether the UN's voluntary norms continue to represent an appropriate framework for evaluating responsible State behaviour in cyberspace or whether additional norms are needed. Some participants stressed that the existing norms were sufficient and that the critical next step is to focus on their implementation.

32. Regional organisations (such as the Organization of American States, Association of South East Asian Nations, and the European Union) were noted as useful fora to discuss ICT issues and facilitate the implementation of cyber norms.

33. It was suggested States be prepared – individually but ideally collectively – to 'name and shame' actors who engage in irresponsible cyber behaviour because this can lead to greater accountability. States should be confident of their decision to 'name and shame' actors because misattribution can generate tension and lead to instability.

34. It was also flagged that the international political and legal system has developed sophisticated means and mechanisms for the peaceful resolution of international

[2] The CCDCOE conducts research and runs training exercises in cyber security with the aim of equipping States with the skills and knowledge needed to react quickly and effectively to cyber security incidents. The CCDCOE's Locked Shields exercise is a leading initiative in preparing States for cyber war.

disputes. States were encouraged to consider how these means and mechanisms can be harnessed in the context of cyber disputes.

Responsible Cyber Power – What Next Steps and Where to Go?

35. By way of conclusion, the hosts of the dialogue encouraged participants to reflect on three questions; participants' responses are detailed below:

36. What have you learnt from the dialogue?

- 'Cyber power' is a potentially divisive concept because it places too much emphasis on offensive cyber capabilities
- Cyber capacity building is key – in cyber, States are only as strong as the weakest link
- States do not need to reinvent the wheel when it comes to identifying responsible cyber power: States need to build on the existing work of the UN processes associated with responsible behaviour
- Effective international cyber governance requires all stakeholders to be included in discussions and, moreover, for them to be given a meaningful voice
- Effective cyber security requires a 'whole of society approach' – States cannot achieve cyber security on their own
- Regulating the private sector may be necessary as a last resort but what is critical is for States to build durable partnerships with companies

37. What will you do differently?

- Increase transparency around cyber capabilities
- Better messaging/communicating to national and international actors
- Build stronger partnerships with the private sector
- Increase support for capacity building
- Clarify cyber terminology and push for a common language
- Map/survey implementation of UN's voluntary norms
- Leverage support and influence of regional organisations

38. What do you want to happen?

- Broaden discussions beyond like-minded States – avoid risk of echo chamber
- Sharing best cyber practices
- States need to articulate their own vision and standards for responsible State behaviour in cyberspace
- Franker discussion of offensive cyber capabilities – when, where, and how will they be used? What checks and balances are they subject to?
- States need to clarify the meaning of the UN's voluntary norms – ambiguity favours powerful States and disadvantages the weakest
- Support the 2025 Programme of Action
- Provide the private sector with a 'louder' voice in international cyber governance forums

39. The participants generally agreed this dialogue was useful to begin detailed examination of these issues. Participants were keen to underscore 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 | January 2023

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/