Wilton Park

Report: Acting responsibly in cyberspace II

Monday 15 – Wednesday 17 April 2024 | Santiago, Chile

In partnership with

the UK Foreign, Commonwealth and Development Office and the Ministerio de Relaciones Exteriores de Chile

Report:

Acting responsibly in cyberspace II

In partnership with
the UK Foreign, Commonwealth and Development Office and the Ministerio de Relaciones Exteriores de Chile

In November 2022, in partnership with the United Kingdom's Foreign, Commonwealth and Development Office, Wilton Park hosted a dialogue entitled Acting Responsibly in Cyberspace. The purpose of the dialogue was to explore the concept of responsible cyber behaviour (summary and full technical reports available here). From 15-17 April 2024, and this time in partnership with the United Kingdom's Foreign, Commonwealth and Development Office and the Ministerio de Relaciones Exteriores de Chile, Wilton Park convened a second dialogue in Santiago, Chile. This dialogue brought together a range of different stakeholders – including representatives from partner countries, international organisations, non-governmental organisations, industry, academia and civil society within the region – to examine what responsible cyber behaviour looks like in practice.

This summary report provides an overview of the key themes raised during the Acting Responsibly in Cyberspace II dialogue.

Cyber threats

1 Participants observed that there has been a diversification and democratisation of cyber threats in terms of malicious actors, victims, vectors and the evolving technology. They explained that the threat landscape will become increasingly complex and difficult to manage with the development of new technologies such as Artificial Intelligence and Quantum Computing. They also noted that there has

been a blurring of the threat landscape insofar as malicious cyber operations are no longer targeted against specific actors, sectors or infrastructure but are instead directed at all members of society. Participants also stressed that modern cyber security threats impact disproportionately on marginalised groups. One participant suggested that systematising cyber threats into "buckets of challenges" can help raise awareness, share best practices and find solutions. Participants emphasised that a critical step in addressing cyber threats is to develop effective attribution methodologies which allow the mask of anonymity to be lifted and for malicious actors to be identified. A participant suggested that the development of an international, impartial cyber attribution body may be useful.

2 Some participants maintained that inaction can also be a source of threats and instability in cyberspace, which makes the cyber threat landscape even more complex, diverse and unpredictable. Various examples were given of "threats through inaction", such as the failure of stakeholders to: report cyber threats and share threat information; direct sufficient resources to combating cyber threats; improve and develop digital literacy; empower individuals online; reduce reliance on outdated (and insecure) legacy systems; adopt the necessary cyber security laws, policies, strategies and standards; engage meaningfully with other cyber stakeholders; and participate in cyber governance processes, mechanisms and initiatives. These participants explained that inaction can embolden and incentivise malicious actors, disempower communities and create new threats as well as exacerbate existing ones.

3 Participants emphasised that countering cyber threats requires effective information sharing. Some participants noted that the sharing of information on threat actors and software vulnerabilities must go beyond the existing State-to-State or CERT-to-CERT models and include all relevant stakeholders such as industry and civil society actors.

Cyber governance

4 During the first Wilton Park dialogue, there was broad agreement among participants that the principles of accountability, legitimacy, transparency and inclusivity are the cornerstones of responsible cyber behaviour. Participants at the second dialogue affirmed the centrality of these principles in defining responsible cyber behaviour.

5 Participants discussed the United Nations' (UN) voluntary, non-binding cyber norms. Some participants noted that the implementation of these norms is a journey and that States have different speeds and require different types of support and assistance. Other participants observed that, while at one point in time simplicity may have been a virtue of these norms, the threat landscape has evolved and they may require further elaboration. One participant explained that Norm 13(e) (on the protection of digital rights) is in particular need of elaboration because there is currently too much ambiguity as to how human rights apply online and under what circumstances their enjoyment can be lawfully restricted. Some participants went further and expressed concern that gaps in the UN's cyber norms framework may have emerged – for instance, the theft of intellectual property in cyberspace was seen as a significant threat that may not be covered by the existing norms. However, other participants questioned the prudency of exploring whether new norms are needed, suggesting it may open up a "Pandora's Box".

6 Participants stressed the importance of ensuring accountability for breaches of the UN's norms on responsible cyber behaviour. One participant suggested that States should consider moving from a retributive to a restorative model of accountability. This participant explained that, in certain circumstances, the retributive model may not always be the appropriate approach and can come across as "heavy handed". Rather, we should think about why States have fallen

short in meeting the UN's cyber norms and work with them constructively to help raise compliance.

7 Accountability was also discussed in the context of cyber capacity building, which was identified as an important tool in raising cyber security standards and ensuring responsible cyber behaviour. While participants explained that providers should be transparent about what support they offer, to whom, and on what basis, others went further and suggested that there must be accountability for the way providers engage in cyber capacity building. One participant explained that there must also be accountability for *recipients* in order to ensure that cyber capacity building projects are worth the time and resources. This type of accountability process requires a consideration of how the effectiveness of cyber capacity building is measured, assessed and reported.

8 Participants observed that non-State actors continue to play an important role in cyber security and cyber governance and that the concept of "responsible cyber behaviour" encompasses such actors. In light of this, some participants considered whether bespoke rules and standards should be developed for the private sector, especially given the power they possess when compared with developing States – one participant even noted the potential for "big tech tyranny". Self-regulation is important but will not always be sufficient. National and regional regulation may therefore be necessary, but even this may not be enough in a global domain such as cyberspace and thus global standards may need to be set. One participant suggested that the "Ruggie Principles" on business and human rights may be a useful model when developing standards for the private tech sector. Some participants pointed out that the private sector is not homogenous and regulatory frameworks cannot treat all private actors the same, which poses a significant challenge when developing standards of responsible cyber behaviour for these actors. Moreover, developing such standards raises the difficult question of accountability – how can private actors be held accountable to these standards and, in particular, what accountability

mechanisms are available, are they effective, or will new mechanisms need to be developed?

9 The shape, constitution and mandate of future cyber governance processes was also discussed. Given the challenging geopolitical landscape, participants noted that national, regional and multilateral cyber governance processes have become increasingly important. However, some participants noted that the proliferation of such processes imposes significant resource costs on States and, for this reason, cyber security discussions should be centralised *as far as possible* in the UN or, if cyber security discussions are needed in other forums, it should be explained whether and how they relate to UN discussions. Moreover, these participants explained that to drive forward norm-development, ensure accountability, develop cyber capacity building and build confidence among cyber stakeholders, a global approach to cyber security is needed and the UN has the legitimacy to do this. One participant noted that inclusivity is critical because States are unlikely to comply with norms that they have not had the opportunity to shape.

10 Some participants expressed concern as to what UN cyber governance process will take over from the UN Open-Ended Working Group (OEWG) when its mandate comes to an end in 2025. Several participants explained that whatever this future process looks like, States need to think critically about the strengths and weaknesses of the current OEWG and, in particular, how its strengths can be maintained and its weaknesses jettisoned. Noting the lack of effective participation of non-State actors in the current OEWG, these participants underscored that, if a "whole of society" approach to cyber security is to be achieved, all relevant stakeholders must have the opportunity to participate meaningfully in future cyber governance processes and initiatives.

11 To enhance legitimacy and transparency, participants emphasised that States should develop legal and ethical frameworks to govern their behaviour and operations in cyberspace. In particular, this requires States to adopt national laws,

policies and strategies on cyber security, as well as national positions on the application of international law to cyberspace, and to make them publicly available. Further, they explained that these initiatives should be seen as iterative processes that must evolve in-step with technological developments.

Private sector

12 Participants explained that ensuring accountability in cyberspace requires effective reporting of cyber security incidents. Given that most cyber infrastructure is owned and operated by the private sector, there was discussion of how to incentivise industry to report cyber security incidents and patterns of suspicious behaviour to appropriate authorities, and to assume more responsibility for cyber security beyond the protection of critical national infrastructure.

13 There was also discussion of how to incentivise private actors to share resources and work better with regional organisations. A key theme emerging from this discussion was that the private sector needs to be incentivised to be proactive rather than reactive in addressing cyber threats and insecurity. One participant gave the example of the considerable cyber security benefits that have come from the introduction of multifactor authentication by Google and Microsoft. The question now is: how can instances of best practice be rolled out across the private sector and how can States encourage and support this process? Some participants explained that there needs to be a mixed methods approach to incentivisation. They suggested that negative incentives – through the passing of laws and regulations and the imposition of sanctions – can work and may be necessary, but that they can also be a blunt instrument and so positive incentives should be developed. Some participants identified a range of positive incentives that can be drawn on to galvanise the private sector into action: (i) economic incentives: only working with private actors that are trustworthy; (ii) market incentives: assisting trusted, private actors to access lucrative markets; and (iii)

social incentives: championing companies who contribute to an open, peaceful and secure cyberspace.

Prioritising cyber security

14 A recurring theme during the dialogue was the need for greater prioritisation of cyber security across all stakeholders. Participants stressed that politicians need to be encouraged to place cyber security on national, regional and international agendas, and make more resources available for cyber security. They discussed the need to champion this debate within their own organisations as well as the various ways to do this, including linking cyber security with political priorities such as election security, international development and the defence of allies.

15 Participants explained that companies need to be more transparent during the research and development phase of technologies so that risks and vulnerabilities can be assessed before products land on the market. As one participant noted, there needs to be a shift in the business model away from providing solutions for cyber security problems to ensuring that products are safe and secure throughout their life cycle – in this way, products need to be "secure by design". This participant drew an analogy between the cyber security and pharmaceutical sectors because, currently, both place too much emphasis on the treatment of the problem rather than the development of a cure, which has led to a "commodification of vulnerabilities" in the cyber security sector.

16 Given the "whole of society" approach to cyber security advocated by many States, some participants explained that individuals need to take more responsibility for their own cyber security. If "deterrence by denial" is a key driver of cyber security, this ultimately depends on good individual and organisational cyber hygiene, which requires citizens and organisations to learn how to use technology safely and responsibly. One participant noted that achieving cyber security is a "shared responsibility" incumbent on all actors. That said, another

participant noted that a "shared responsibility" approach should not detract from the fact that governments have the primary responsibility for the provision of security including cyber security.

Cyber security and human-centrism

17 The theme of human-centrism in cyber security cut across many discussions during the dialogue. Participants observed that, to date, the dominant approach to cyber security has been the protection of national security (and in particular the protection of critical national infrastructure) from damaging and destructive cyber attacks. However, participants explained that, in the contemporary era, malicious cyber operations are directed at a range of actors and entities and take many different forms. Increasingly, civil society actors are targeted in cyberspace and fall victim to cyber attacks, cyber surveillance campaigns and dis-, miss- and mal-information operations.

18 Many participants encouraged States to adopt a human-centric approach to cyber security, which focuses on the protection of human security, human wellbeing and human welfare in cyberspace. As an example, one participant explained that while States dedicate significant resources to identifying and countering perpetrators of ransomware attacks, more attention needs to be given to the victims of these operations who suffer a range of psychological, economic and social harms. One participant also observed that this human security approach requires a consideration of the human rights of malicious cyber actors on the basis that they do not forfeit their human rights protections simply because they engage in cyber criminality.

19 Participants agreed that moving to a human-centric model requires a fundamental change in mindset. They also explained that protecting human security in cyberspace requires significant additional resources, which brings us back to the importance of generating political interest in cyber security, developing cyber

capacity building and improving digital literacy. Yet, some commentators painted a more positive picture and identified examples of cyber security initiatives that already seek to protect human security in cyberspace, such as the Counter Ransomware Initiative and the Pall Mall Process.

Next steps: takeaways and action

20 By way of conclusion, the hosts of the dialogue encouraged participants to offer one key takeaway from the dialogue and one key action to take after the dialogue.

21 Takeaways:

- The importance of communication and dialogue in building transparency and trust.
- Given many States' resource constraints, cyber security discussions should be consolidated as far as possible in the UN. Where cyber security discussions are held in other forums, it should be make clear whether and how they relate to UN discussions.
- The importance of multistakeholder engagement.
- The benefits of developing a human-centric approach to cyber security.
- The pivotal role played by regional organisations in identifying cyber threats; responding to cyber security incidents; identifying synergies and divergences in cyber security laws, policies and strategies; sharing best practices; building trust; and developing cyber capacity building projects.
- The need to strengthen cyber networks within and across States.
- The importance of recognising that States and regions have different approaches to cyber security and thus have different needs and priorities.

22 Actions:

- To promote constructive cyber security dialogues within civil society, among cyber security professionals and across national agencies.

- To ensure that cyber security decision-making is the product of a “diversity of minds”.
- To ensure better representation and participation of stakeholders in UN cyber governance processes.
- To develop national, regional and international metrics to measure and rank cyber maturity.
- To produce publicly available State positions on cyber security to increase transparency for national and international audiences.
- To make cyber security information and resources more readily available and accessible to all members of society.

Russell Buchan

Wilton Park | June 2024

Wilton Park reports are brief summaries of the main points and conclusions of a conference. The reports reflect rapporteurs' personal interpretations of the proceedings. As such they do not constitute any institutional policy of Wilton Park nor do they necessarily represent 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 www.wiltonpark.org.uk/newsletter

Wilton Park is a discreet think-space designed for experts and policy-makers to engage in genuine dialogue with a network of diverse voices, in order to address the most pressing challenges of our time.

enquiries@wiltonpark.org.uk

Switchboard: +44 (0)1903 815020

Wilton Park, Wiston House, Steyning,
West Sussex, BN44 3DZ, United Kingdom

wiltonpark.org.uk