Cybersecurity in the Commonwealth: Towards Stability and Responsible State Behaviour in Cyberspace

7 October 2019
Introduction

The April 2018 Commonwealth Heads of Government Meeting (CHOGM), held in London, saw the creation and the adoption of the Commonwealth Cyber Declaration (‘the Declaration’). The Declaration outlines the framework for a concerted effort to advance cybersecurity practices to promote a safe and prosperous cyberspace for Commonwealth citizens, businesses and societies.

In this context, Chatham House’s International Security Department (ISD) embarked on a new project, Implementing the Commonwealth Cybersecurity Agenda, in June 2018. This initiative aims to develop a pan-Commonwealth platform to take the Declaration forward by means of a holistic, inclusive and representative approach. The aim is to improve cyber policymaking by broadening knowledge. To achieve this, the project has the following objectives:

1. Initiating a structured dialogue on cyber capacity-building in the Commonwealth, based on ongoing initiatives under the Declaration to discuss progress, challenges, mitigation measures and best practices;

2. Creating an informal network that connects key Commonwealth policy influencers with capacity builders and sources of expertise at Commonwealth and global levels; and

3. Sharing and developing a common understanding of best practices.

The main project activities include four events and subsequent reports summarizing the main discussion points, conclusions and key considerations.

The first three events and reports each focused on one pillar of the Declaration, as below:

- Event 1: A cyberspace that supports economic and social rights online.²
- Event 2: Build the foundations of an effective national cybersecurity response.³
- Event 3: Promote stability in cyberspace through international cooperation.

The fourth and final event and report will build on the previous outputs and provide an overview of the progress achieved in 2018–20 in respect of the Declaration by the UK Foreign & Commonwealth Office’s (FCO) Commonwealth Cyber Programme.

Event 3 summary

The third event of this project took place in Addis Ababa, on 7 October 2019, under the title ‘Cybersecurity in the Commonwealth: Towards Stability and Responsible State Behaviour in Cyberspace’.⁴ The event took the form of a roundtable and considered the third pillar of the Declaration – Promote stability in cyberspace through international cooperation – and its four action points.

Set against the backdrop of the ongoing processes of the United Nations General Assembly, namely the UN Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) on responsible state behaviour in cyberspace, the third event sought to explore the role and contribution to be made by Commonwealth members in these dialogues.

---

² The report from event one could be accessed on this link, https://chathamhouse.soutron.net/Portal/Default/en-GB/RecordView/Index/182669.
³ The report from event two could be accessed on this link, https://chathamhouse.soutron.net/Portal/Default/en-GB/RecordView/Index/189876.
⁴ The first event under this project was held on 4 October 2018 at Chatham House in London. It addressed the issue of Supporting Economic and Social Development and Rights Online. For the summary, see https://chathamhouse.soutron.net/Portal/DownloadImageFile.ashx?objectId=2851; the second event was held on 8 March 2019 in Barbados, and addressed the issue of Building the Foundations of Effective National Responses in the Caribbean, a summary can be found at: https://chathamhouse.soutron.net/Portal/DownloadImageFile.ashx?objectId=3161.
The participants at this roundtable included representatives from Commonwealth countries to both the GGE and OEWG – most of whom were from African countries – as well as regional and international organizations working towards increasing stability in cyberspace. The roundtable was made up of four thematic sessions.5

**Session 1: The Global Cyber Governance Journey: Overview, Trends and Status quo**

The first session provided an overview of global cyber governance to date and an update on current discussions that are taking place at the UN, regional and sub-regional levels. This charted the development of conversations on cyberspace over the past decade, including the previous and current processes at the UN in the GGE and OEWG. The session highlighted the variety of stakeholders that are involved in these processes, in addition to state actors, which brings with it many challenges and opportunities.

**Key discussion points**

- There has been an increasing realization in the past decade that the benefits brought by the development of cyberspace have been matched by equally numerous opportunities for malicious misuse, particularly between states.
- To deal with threats in cyberspace, some states have developed new legislation and have updated existing laws (such as their criminal codes), which in some cases have undermined the human rights of their citizens with implications for freedom of expression and privacy rights.
- While governments remain the primary guarantors of international peace and security in cyberspace, the roles of the private sector, academia and civil society in contributing to this are very important.
- At the global level, a range of non-binding frameworks have emerged that focus on norms surrounding responsible state behaviour, primarily through the consensus reached by the GGEs in 2010, 2013 and 2015. These have been complemented by industry initiatives and multi-stakeholder arrangements, such as the Paris Call for Trust and Security in Cyberspace and the Global Commission on the Stability of Cyberspace.

**Recommendations**

- Looking ahead, it is vital to minimize the extent to which the two UN processes, GGE and OEWG, are politicized, as this will serve only to limit the possible achievements of both. The focus should be on what these processes are aiming to achieve in terms of responsible state behaviour in cyberspace.
- A major recommendation raised was the importance of sharing knowledge and best practices on cyber governance between Commonwealth countries, and at the global level more generally, so they can help shape the debate and to identify the most effective ways in which this can be done. Discussions revolved around the need for greater and additional means to propagate these practices and information.
  - Specifically, the creation of digital help desks was proposed, which could serve as regional repositories of information for state representatives who are unable to take part in the GGE and OEWG processes. Participants discussed how technological platforms and tools, facilitated by private-sector companies, can help achieve this goal, and enable wider and more informed active participation in the global cyber governance discussion.
- While the development of cyber-related legislation is proving challenging to several states, these laws are essential for cyber governance and for providing human rights guarantees online and offline. However, in some cases these laws have been misused, particularly by limiting and prosecuting critical and dissenting views.

---

5 For the event agenda, see Annex.
Session 2: Cyber governance from a Commonwealth perspective: Challenges

Discussion in the second session focussed on the challenges faced throughout the Commonwealth in developing cyber governance capacity. Consideration was given to the policy, material and cultural obstacles encountered at the national, regional and international levels. While this session primarily sought to identify and discuss the challenges presently faced within the Commonwealth, participants also raised potential mitigation measures to tackle these challenges.

Key discussion points

• At the national level, there was consensus among participants that while technical challenges remain in the pursuit of good cyber governance, it is becoming increasingly apparent that the challenges faced are multi-disciplinary in nature, which requires collaborative solutions across ministries and sectors. Even when measures are adopted, such as national strategies or laws, the implementation of these measures remains difficult.
  o This was highlighted in the case of Mauritius, where it was noted that a national cybersecurity strategy has been adopted, however, the associated legal provisions to implement this strategy are currently not in place.

• The importance of creating a shared language and understanding was discussed as a challenge that needs to be addressed at the national level and across the Commonwealth in order to facilitate progress towards developing better cyber governance, particularly across states.
  o A lot of cyber governance terms and their usage remain undefined even within countries, let alone at the regional and international level. One recurring question that arose at multiple points throughout the meeting was whether all stakeholders agree on what good cyber governance means and what it looks like. Without shared understanding, if not agreement, on these fundamental definitions, cooperation between stakeholders is likely to be undermined.
  o On an even more fundamental level, it was noted that as English remains the main language for training and capacity-building efforts in the Commonwealth, populations who are not fluent in this language in Africa and other parts of the Commonwealth are often left behind. Even when this is mitigated through translation, for example, some of the benefits of these efforts are lost. The importance of knowing the audience and exploring the best ways to connect with them in developing knowledge and capacity-building was highlighted as an essential way forward.
  o Similarly, communicating clearly and conveying the reality that cybersecurity is ubiquitous throughout all areas of governance is a growing necessity, given that this now encompasses human rights, internet governance, digital trade, cybercrime and technological development to name but a few.

• Another challenge identified was the pace at which digital uptake has occurred in Commonwealth countries. On the one hand this has created many opportunities, however, the quick uptake has meant that some basic challenges, such as affordable access and skills have not been dealt with properly. In many instances, the conversation has jumped, perhaps prematurely, to more sophisticated areas, such as the potential impacts of AI, without resolving the basic issues first.

• On a related note, due to the fast-paced nature of the evolution of technology, it is proving a challenge for many countries to keep pace in terms of enacting legislation that addresses the emerging threats that normally arise from these developments, especially in the area of cybercrime.

Recommendations

• At present, most countries in Africa are in the process of enacting laws and cyber strategies. This presents a timely opportunity to harmonize these approaches in a way that fosters cooperation between
these countries. Commonwealth nations in Africa could achieve this by following the foundations laid out in Commonwealth model laws and good practices as well as in the Declaration.

- International cooperation, particularly through knowledge sharing and capacity-building efforts was again raised as an essential requirement for overcoming the identified challenges to cyber governance. Specifically, it is important that existing capacity-building efforts that benefit several countries, such as the current initiative being undertaken in Mauritius to establish a repository for cybercrime expertise in Africa, are disseminated and shared effectively throughout the region.

- To tackle these wide-reaching challenges, there is a need for informed leadership that goes beyond the presidential or prime ministerial level and spans across different ministries in order to facilitate in aiding cooperation and coordination.
  - This could assist in consolidating the number of fragmented projects across various independent ministries. At present, this is consuming financial and personnel resources, which can lead to the duplication of efforts and suboptimal use of important and often scarce resources.
  - There is also the need for presidents and ministers to focus on this issue to take leadership of capacity-building. At present, there is a lot of discussion surrounding the need for greater leadership, however, it is still unclear how these discussions will translate into actions.

**Session 3: Cyber governance from a Commonwealth perspective: Opportunities**

This session explored the opportunities available to Commonwealth nations and looked at how to realize them. Attention in this session focused on current attitudes towards addressing cyber governance within governments and methods by which this narrative can be advanced, the avenues through which this can be pursued and some of the potential pitfalls.

**Key discussion points**

- When considering Commonwealth countries’ development of cyber governance capabilities, it was accepted that countries throughout the Commonwealth have very different requirements and that greater parity is needed. To achieve this, participants stated that those countries at an early stage of this process would need to pass through development phases more quickly, rather than simply leapfrog to the level of more advanced Commonwealth countries.

- The malicious use of Information and Communication Technology (ICT) by state and non-state actors creates risks for all states, and the misuse of ICTs may harm international peace and security. Although the conversations in OEWG meetings, and the First Committee more generally, are focused on maintaining peace and security, malicious activity committed by non-state actors for criminal purposes puts populations, livelihoods and economies at risk. Therefore, it is very important that linkages are made to the work of other UNGA committees that address these issues, namely the cybercrime work within the Third Committee. This can prevent a siloed approach, support states in having a good understanding of the big picture and work towards consistency in states’ policymaking at the global and national levels.

- In order to increase the prioritization of cybersecurity within national policy agendas, the linkages should be made explicit between good cybersecurity and strong digital economies. Essentially, a higher level of cybersecurity can encourage investment in the economy and make a country more competitive.

- At the same time, while it was acknowledged that cooperation is essential to promote a secure cyberspace, cooperation between countries needs to be made on a clear basis as there is a risk if cooperation extends to the extent that it becomes a dependency, particularly in the critical national infrastructure sectors.

- Throughout this session, a recurring theme was how best to prioritize and mainstream the discussion of cybersecurity within governments to encourage them to act on existing potential and opportunities. While there was agreement that cyber issues can no longer be viewed as the preserve of one ministry,
namely ICT, it was noted that this is a process that needs to be carefully managed in a collaborative manner between departments.

**Recommendations**

- Efforts should be made to boost the role of African countries in this sector, participants called for these nations to ‘own a piece of cyberspace’. As part of this process there is a need to highlight success stories within Commonwealth countries and foster more South–South cooperation in cyber governance. This includes placing a greater emphasis on providing more services locally to avoid exacerbating present dependencies on other states.
- Many leaders consider cybersecurity too technical an issue to be handled by them alone, which explains their cautious approach. This problem needs to be demystified in a way that clarifies the need to treat cybersecurity as a national security issue. In Africa, for example, having a few senior ministers or presidents driving the cybersecurity agenda forward can play a crucial role in inspiring other countries in the region to follow suit.
  - To facilitate this change, participants proposed the introduction of leadership training, regional champions and experience sharing.
- The GGE and OEWG present opportunities to gather more evidence on the harm that attacks cause and bolster this knowledge base. This is particularly the case since threats in cyberspace have various impacts on different states. For example, while one country may consider an attack against its critical national infrastructure as the biggest threat from cyberspace, another country, with a lower level of digitization, may view the impact of disinformation and fake news on its democracy as a greater threat. Therefore, it is very important that in regard to cyberthreats that the OEWG and GGE meetings discuss the different capacities, perceptions and impacts of threats in different states. This in itself would be a constructive awareness building measure among and between states.
- National strategies for cybersecurity should be localized and tailored in order to be effective rather than based on existing broader strategies to traditional challenges.
- On a related note, it was suggested that in light of the general lack of cybersecurity skills in government, trained officials could rotate between ministries, and help spread their knowledge across governmental departments.
- Several participants suggested that in order to address the cyber skills shortage, curriculums in universities should be updated as soon as possible to reflect the ubiquity of cyber issues in all areas of work. In particular, this should increasingly consider subjects other than ICT and engineering, such as law.

**Session 4: Way forward for better cyber governance in the Commonwealth: needed capacity and existing platforms**

Discussions in this session focussed on the Commonwealth’s cyber governance horizon. This included consideration of the next phases of the GGE and OEWG processes and ways in which both the Commonwealth and Commonwealth countries can contribute towards the two processes. The session also explored the utility of global initiatives, such as the Global Forum on Cyber Expertise.

**Key discussion points**

- A lot of attention focused on the importance of promoting inclusive cyber governance and not exacerbating existing disparities between states.
Cybersecurity in the Commonwealth: Towards Stability and Responsible State Behaviour in Cyberspace

At the UN level, the most developed states tend to be the most proactive actors in the debate on responsible state behaviour in cyberspace. This needs to change and developing states should play a bigger role in driving the UN processes in order to help bridge the gap in capacity between countries.

- Participants supported the inclusive approach to the global cyber governance discussion, which is now evident in the OEWG.

Discussion also considered the practical limitations of the current UN processes, in terms of participation, duration and needed resources. Participants discussed the challenges faced by states with smaller delegations, acknowledging that the level of expertise developed among policymakers will largely be determined by the level of resources available. Unless these obstacles are addressed, small countries and developing countries will suffer disproportionately as a result of having less coordinating capacity, which highlights the opportunities that exist for regional organizations such as the African Union.

- One participant noted that as the GGE experts from Africa are mostly from Commonwealth member states, this creates a good opportunity for Commonwealth countries to coordinate and align their positions so they can achieve a better impact within the GGE and other global platforms.

- At the same time, there was an acknowledgment of the merits of adopting and using a global framework for cyber governance and how this should be modelled.

  - It was suggested that there will be limited scope to address cyber challenges collaboratively as long as states remain unaligned, due to their various ideological standpoints and differing definitions of a global cyber governance.

Recommendations

- It is important for regional organizations to do more to coordinate statements among their members and participate at OEWG meetings to ensure that states with limited capacity are represented and that their voices are heard.

  - Regional groupings such as the Commonwealth and the African Union should emphasize the accessibility of the discussion and make efforts to encourage broad participation. More is required to build capacity at the political level to engage in this process.

- Any mechanism for institutional dialogue will need to fit in the greater ecosystem of cyber discussions within the UN to avoid duplication.

- Participants also suggested that cyber governance should be made a matter of priority in the Commonwealth. This could be done by looking at various threats or special meetings of the Commonwealth to make sure that cybersecurity issues are regularly raised for the issue to gain real traction. It was also suggested that Commonwealth countries should align their positions on these issues in UN forums, in line with the Declaration.

- The Commonwealth should look at existing avenues for collaboration in the cyber sector that already have firm foundations, such as the Commonwealth model laws.6 As there are substantial commonalities of legal systems across the Commonwealth, there is already greater scope to deal with similar challenges in terms of jurisdiction and parliamentary legislative programmes.

- A framework for coordination will be necessary to encourage collective decision-making in the realm of good global cyber governance and this should be a priority. There was hope among some participants that this will eventually be enveloped in the roles undertaken by the UN in the future, however, at present this journey remains far off.

---

Final remarks

As per the third pillar of the Declaration, this event explored the opportunities for Commonwealth countries to promote stability in cyberspace through international cooperation. This pillar of the Declaration has taken on increased significance since its ratification in 2018, following the establishment of the dual-track process taking place at the UN on responsible state behaviour in cyberspace. In convening representatives to the GGE and OEWG from Commonwealth member states in Africa, it became evident that opportunities to promote cooperation must be taken at all levels if the cybersecurity gap between nations is going to be successfully reduced.

A recurrent theme that arose throughout the sessions was that the current processes taking place at the UN level serve as some of the greatest opportunities for countries to have a say in helping build cyberspace to reflect commonly shared values. It was, however, acknowledged that this opportunity is presently unbalanced among UN members, not least as a result of varying access to resources and cyber expertise. These, among other challenges, can be partially mitigated through the pooling of human and economic resources, namely through regional organizations and global networks, provided that cooperation and coordination is promoted.

While this event was focussed specifically on the third pillar of the Declaration – *Promote stability in cyberspace through international cooperation* – the conclusion is by no means the end of the discussion on this topic within the ISD project. This pillar, and its related projects under the FCO programme, will be discussed in the fourth and last conference of this project. The last conference will take place at Chatham House in London in February 2020 and will aim to provide an overview on the progress made in the Commonwealth since the Declaration was announced in 2018. In addition, it will examine future challenges and potential solutions going forward.
Annex: Event 3 Agenda

09:30–10:00  Registration, tea and coffee

10:00–10:30  Welcome, introductions and context

10:30–11:30  Session 1: The Global Cyber Governance Journey: Overview, Trends and Status quo

11:30–11:45  Coffee break

11:45–13:15  Session 2: Cyber governance from a Commonwealth perspective: Challenges

13:15–14:15  Lunch

14:15–15:45  Session 3: Cyber governance from a Commonwealth perspective: Opportunities

15:45–16:00  Coffee break

16:00–17:30  Session 4: Way forward for better cyber governance in the Commonwealth: needed capacity and existing platforms

17:30–17:45  Final Remarks