Cybersecurity in the Commonwealth: Supporting Economic and Social Development and Rights Online

04 October 2018
Introduction

The 2018 Commonwealth Heads of Government Meeting (CHOGM), held in London in April, oversaw both the creation and the adoption of the Commonwealth Cyber Declaration (‘the Declaration’).¹ The Declaration sets 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 project provides a pan-Commonwealth platform with the aim of taking the Commonwealth Cyber Declaration forward by means of a holistic, inclusive and representative approach. The ultimate aim is to improve cyber policymaking through improving knowledge. To achieve this, the project will have 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, mitigating 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 good practices.

The main project activities are concerned with the organization of four workshops and the subsequent development of a report from each workshop, summarizing the main discussion points, conclusions and key issues to be considered.

The first three workshops and ensuing reports will focus on one of the three pillars of the Declaration. The final workshop and report will build on the previous ones and provide an overview of the progress achieved in 2018–20 in respect of the Declaration by the various implementers under the UK Foreign & Commonwealth Office’s (FCO) Commonwealth Cyber Programme.

Workshop 1 summary

The first workshop as part of this project took place at Chatham House on 4 October 2018, under the title ‘Cybersecurity in the Commonwealth: Supporting Economic and Social Development and Rights Online’. The workshop considered the first pillar of the Declaration – A cyberspace that supports economic and social development and rights online – and its nine action points.

The 31 participants at this workshop included project implementers and stakeholders from the public and private sectors from a number of Commonwealth countries, as well as global stakeholders. The workshop was made up of three thematic sessions, together with one closed ‘practical’ session for the project implementers.² The closed session provided an opportunity for project implementers to discuss upcoming milestones and explore opportunities for collaboration and synergies. It also included a presentation by the FCO on recent programmatic and reporting updates.

---

² For workshop agenda, see Annex.
Welcome, introductions and context

The opening session included three presentations, on the FCO’s Commonwealth Cyber Programme, the Chatham House ISD project, and the Global Forum on Cyber Expertise (GFCE).

Key discussion points

- The FCO has designated £15 million to support implementation of the Commonwealth Cyber Declaration, including £5.5 million earmarked for projects under its Commonwealth Cyber Programme to provide technical assistance, training and advice to address a wide range of cybersecurity and cybercrime threats and issues.³
- The FCO Commonwealth Cyber Programme aims to link to larger global initiatives such as the UN Sustainable Development Goals, while delivering practical improvements across the countries of the Commonwealth.
- International collaboration, both among Commonwealth member states and between the Commonwealth and similar international platforms, is essential if the objectives of the Declaration are to be delivered.

Recommendations

- To improve cybersecurity in the Commonwealth countries and deliver on the Declaration’s objectives, it is imperative that governments and the private sector work together, it is also crucial for Commonwealth countries to cooperate together and with existing global initiatives
- Commonwealth countries are taking part in various international initiatives. For instance, 12 of the 53 Commonwealth countries are members of the GFCE. Such networks should be strengthened and widened, as they offer access to a wealth of expertise as well as opportunities to promote synergies.
- The themes of the GFCE’s Delhi Communique – cybersecurity policy and strategy; cyber incident management and critical infrastructure protection; cybercrime; cybersecurity culture and skills; and cybersecurity standards – are broadly similar to the themes of projects under the Declaration’s three pillars. These provide identifiable grounds for cooperation and comparison throughout the life cycle of the FCO Commonwealth Cyber Programme.
- There should be more substantial efforts to engage smaller countries within the Commonwealth, which often receive less attention, in ongoing cybersecurity initiatives.

Session 1: Cybersecurity in the Commonwealth: Supporting economic development

This session discussed how increasing reliance on the internet and intensified digitization have created more cyber vulnerabilities for Commonwealth countries, resulting in several economic challenges, and highlighted how the Declaration can help mitigate these challenges through the promotion of cybersecurity good practices. An overview of the current economic cybersecurity challenges was followed by a presentation on the Cybersecurity Capacity Maturity Model project and, and a presentation on the Declaration and its role in promoting economic growth in the Commonwealth.

Key discussion points

- Internationally, the incidence rate of cyberattacks, particularly for economic gain, is on the rise. This was highlighted recently at the regional level in a report on the cybersecurity of the banking sector in Latin America and the Caribbean, in which 92 per cent of surveyed banks reported having been subject to some kind of cybersecurity incident; 37 per cent of banks reported having suffered successful attacks, with economic reasons cited as the main motivation for the incidents.4
- While there continue to be major investments in information and communications technology (ICT) in most Commonwealth countries, there has been much less investment in cybersecurity measures. Reasons for this include a prevailing perspective that spending on cybersecurity does not provide a return on investment, and that cybersecurity is not always seen as a risk that needs to be mitigated at every level. This is exposing countries to significant cyber risks, with the potential for damaging impacts on their economies.
- Lack of cybersecurity strategies, coupled with the need for more training, were identified as the main reasons why existing cybersecurity measures are partially failing. In addition, cybersecurity measures need to be revised and updated regularly, considering the changing nature of the threats. This is not necessarily the case in most Commonwealth countries.
- Although investment in cybersecurity measures and adopting good practices do not result in complete protection from cyberattacks, they do help governments and the private sector to build more resilience. This allows them to better prepare for, and recover from, potential and eventual attacks.
- The cybersecurity skills shortage in Commonwealth countries – especially in smaller countries – is acute, and is exacerbating the challenge of strengthening cybersecurity. As part of its Commonwealth Cyber Programme, the FCO has been leading projects aimed at bridging this skills gap, including training and education-based activities directed towards the smaller countries and island states of the Commonwealth.

Recommendations

- In view of the disproportionate impact that cyberattacks have on small and medium-sized enterprises (SMEs), it was suggested that more efforts should be directed at supporting SMEs in building their cybersecurity capabilities and increasing their resilience. Such efforts must be incentivized by both governments and the private sector.
- The Budapest Convention5 can, at a minimum, be used as a point of reference when developing cyber legislation in Commonwealth countries. The Convention has already helped shape and

influence several instruments at the Commonwealth level, such as the Commonwealth Model Law on Computer and Computer Related Crime.\textsuperscript{6}

- Net neutrality is important, and should be maintained throughout the Commonwealth to promote a free and open cyberspace in which all companies, irrespective of size, can carry out their business.

**Session 2: Supporting Social Development**

This session explored the role that digital opportunities and inclusion can have in encouraging social development throughout the Commonwealth, as well as the risks that an unsecure cyberspace may present.

**Key discussion points**

- The sustainability of cybersecurity projects beyond their present life cycle raises serious concerns. The commitment of governments as well as other stakeholders such as SMEs and local businesses is crucial for building better cybersecurity that supports social development.

- Strengthening the cybersecurity of elections is a common priority for Commonwealth countries, even if, depending on the level of digitization from country to country, the threat might differ. In less digitized countries with limited or no computerized electoral infrastructure, the main threat arises from disinformation campaigns. In more digitized countries, the cybersecurity of the electoral infrastructure itself is at risk. Disinformation campaigns pose a serious concern to these countries as well.

- The constantly evolving nature of technology presents challenges for legislators in keeping laws up to date, in allowing these laws to play their role in protecting victims from cybercrime, and in creating a deterrent effect.

**Recommendations**

- Successful cybersecurity initiatives and practices will have to be built with respect to national and cultural contexts and differences, avoiding a ‘one size fits all’ approach.

- To take account of the issue of cultural and regional variances throughout the Commonwealth, it was suggested that more comprehensive efforts should be geared towards promoting national ownership of projects implemented in recipient countries.

- Countering the potential for electoral disruption arising from cyber vulnerabilities will require consideration on a country-by-country basis. A discussion should also take place at the Commonwealth level to determine what types of action can be taken collectively to respond to extraterritorial incidents of electoral disruption.

- Raising awareness of the ongoing projects that support social development through existing networks should be a priority, to avoid duplication of efforts and to explore opportunities for cooperation where possible.

Session 3: Supporting rights online

This session included a presentation of the current legal landscape in the Commonwealth and commonalities with international approaches. There was also a presentation on an inclusive, value-based approach to cyber policymaking in the Commonwealth that also tackles the issue of rights online.

Key discussion points

- While it is generally acknowledged that same rights that are protected offline should also be protected online, most international conventions and declarations often include broad language and commitments when addressing the issue of rights online.
- The lack of specific legislation addressing online rights in the Commonwealth is contributing to complacency regarding the issue of supporting rights online.
- To address the current deficit in the Commonwealth of tangible measures in support of rights online, there is a pressing need for a cybersecurity policy landscape that is informed by human rights considerations, and that fosters the development of laws and policies that respect human rights online.
- At present, there is no central point of information on national cybersecurity strategies. Such a resource could be a very useful tool for Commonwealth countries to incorporate respect for online rights as they develop their own cyber strategies.

Recommendations

- Establish a working group to review the current Commonwealth Model Laws and suggest changes that would reflect a better protection of human rights online.
- Encouraging further cooperation among project implementers and with external organizations should be prioritized as a critical tool in achieving the objective of supporting rights online, through the exchange of knowledge and expertise on best practices.

Final remarks

There was unanimous agreement that opportunities, on an ongoing basis, for project implementers to convene and share experiences, learn about each other’s projects and provide one another with information on upcoming activities will be vital throughout the course of the programme. The synergies created since the initiation of ISD’s project have been very useful. Implementers are now aware of different initiatives under the FCO Commonwealth Cyber Programme, and this allows them to explore cooperation opportunities. The importance was emphasized of implementers sharing information and materials with one another, to promote linkages and avoid duplication of efforts.

Other good practices that were emphasized during the closing session included considering the sustainability of projects beyond their life cycle. The ‘know your audience’ approach was also repeatedly identified for the successful implementation of projects under the Declaration.

The sustainability of projects should be considered by implementers at every stage. This is critical to ensuring that positive work and practices continue beyond the life cycle of the Commonwealth Cyber Programme. This will ultimately lead to improvements in cybersecurity throughout the Commonwealth.

Finally, it was noted that while this workshop focused specifically on the first pillar of the Declaration — *A cyberspace that supports economic and social development and rights online* — the conclusion of the
workshop 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 future activities as well.

Chatham House plans to convene the second workshop at the beginning of 2019. This meeting will be held at the beginning of 2019 and will focus on the second pillar of the Declaration: *Building the foundations of an effective national cyber security response.*
Annex: Workshop 1 Agenda

Cybersecurity in the Commonwealth: Supporting Economic and Social Development and Rights Online

Chatham House, 4 October 2018

09:00–09.30  Tea and coffee

09:30–10:30  Welcome, introductions and context

10:30–11:45  Session 1: Cybersecurity in the Commonwealth: Supporting Economic Development

11:45–12:15  Coffee break

12:15–13:30  Session 2: Cybersecurity in the Commonwealth: Supporting Social Development

13:30–14:30  Lunch

14:30–15:45  Session 3: Cybersecurity in the Commonwealth: Supporting Rights Online

15:45–16:00  Final Remarks

16:00–16:15  Coffee break

16:15–17:30  Session 4: Practical session

In this closed session, implementers will discuss progress, highlight achievements, impediments in relation to their projects under the cyber programme and will update each other on their upcoming activities with the aim of exploring synergies and collaboration opportunities.

1 (1) Recognise and support cyberspace as an enabling environment to promote investment and intra-Commonwealth trade in goods and services through open markets, the free flow of information, innovation, and fair competition.

2 (2) Commit to promote interoperable and global technical standards, through appropriate consultative processes involving industry, academia, governments and other relevant stakeholders, recognising that standards should be open, foster security and trust and not act as barriers to trade, competition or innovation. (3) Highlight the importance of common standards and the strengthening of data protection and security frameworks, in order to promote public trust in the internet, confidence for trade and commerce, and the free flow of data. (6) Commit to limit the circumstances in which communication networks may be intentionally disrupted, consistent with applicable international and domestic law.

3 (7) Recognise that without cybersecurity citizens are at risk of crime or exploitation, and commit to strengthening legislative, social and educational measures that protect the vulnerable. (8) Recognise that access to information and digital literacy can be a powerful catalyst for economic empowerment and inclusion, and commit to take steps towards expanding digital access and digital inclusion for all communities without discrimination and regardless of gender, race, ethnicity, age, geographic location or language. (9) Emphasise that enhanced digital inclusion of young people in the Commonwealth can contribute in a positive way to their education, social engagement and entrepreneurship.

4 (4) Acknowledge the importance of tolerance, respect for diversity, and understanding in cyberspace. (5) Affirm that the same rights that citizens have offline must also be protected online.