UK Parliament

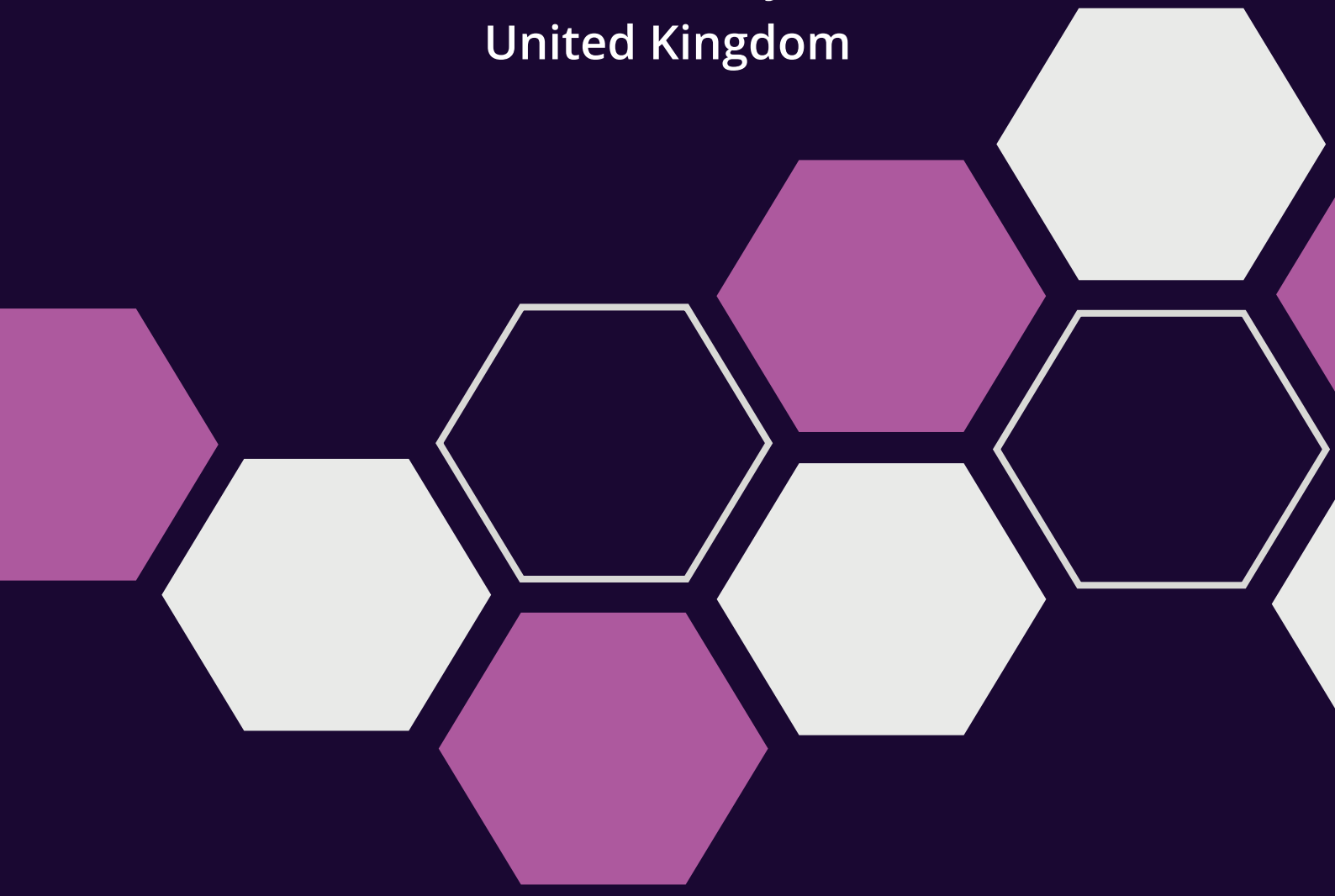
COMMONWEALTH PARLIAMENTARY ASSOCIATION UK

CYBERSECURITY WORKSHOP

OFFICIAL REPORT

24 - 27 February 2020

United Kingdom



IN PARTNERSHIP WITH

Foreign & Commonwealth Office

Ministry of Justice

COMMONWEALTH UK CHAIR-IN-OFFICE 2018-20

UNIVERSITY OF OXFORD

CONTENTS

EXECUTIVE SUMMARY	**3**
ABOUT CPA UK	**4**
MEET THE TEAM	**5**
INTRODUCTION	**6**
WORKSHOP OVERVIEW	**7**
DELEGATE BREAKDOWN	**8**
LIST OF DELEGATES	**10**
OUTCOME AND OUTPUTS	**11**
OUTPUT 1	**12**
OUTPUT 3	**16**
NATIONAL CYBERSECURITY STRATEGIES	**18**
DELEGATE FEEDBACK	**20**
CONCLUSION AND NEXT STEPS	**23**

EXECUTIVE SUMMARY

On behalf of the CPA UK Executive Committee, I would like to thank you for your participation in our Cybersecurity Workshop. Your attendance was particularly valued given the unprecedented global circumstances during which the workshop took place.

Through a combination of interactive exercises, expert panel sessions and peer-to-peer exchanges, we aimed to equip participants with the knowledge, tools and connections required to strengthen cybersecurity legislation within their own jurisdictions and to be confident leaders in this cutting-edge and rapidly expanding policy area.

The workshop was designed to provide a balance between theoretical and practical sessions, allowing participants to draw upon their own experiences of legislating and scrutinising in the field of cybersecurity in order to share best practice and establish mutual priorities and commitments going forward.

During an intense few days of learning, we covered a wide range of topics, from human rights and digital ethics to governmental cyber structures and the Internet of Things. We would like, in particular, to thank our partners, the Foreign and Commonwealth Office, the Ministry of Justice and the University of Oxford, for providing world-leading insights on these topics.

This report provides an overview of the sessions covered during the workshop, and situates them within the workshop outputs. It also presents the valuable feedback you provided and affirms our committment to implementing these in future programmes.

Once again, thank you for participating in this workshop. I do hope you found it an interesting and worthwhile experience.

Jon Davies
CPA UK Chief Executive Officer

ABOUT CPA UK

CPA UK'S STRATEGIC OBJECTIVES ARE:

1. To strengthen parliamentary democracy
2. To link Westminster with the Commonwealth
3. To set and demonstrate high performance standards

The Commonwealth Parliamentary Association (CPA) is the professional association of all Commonwealth parliamentarians, an active network of over 17,000 parliamentarians from 185 national, state, provincial and territorial Parliaments and Legislatures.

CPA UK is located in and funded by the UK Parliament. We support and strengthen parliamentary democracy throughout the Commonwealth by bringing together UK and Commonwealth parliamentarians and offcials to share knowledge through peer to peer learning. We focus on key issues including women in parliament, modern slavery, financial oversight, security and trade.

For more information, please visit our website at **www.uk-cpa.org** or our Twitter account: **@CPA_UK.**

VISION

Our vision is to help facilitate inclusive, representative and transparent Commonwealth Parliaments, fully effective in enforcing the accountability of the executive and representing the interests and concerns of the electorate.

PURPOSE

To learn from and strengthen Commonwealth Parliaments to deliver effective oversight, scrutiny and representation.

CPA UK is also the secretariat for the CPA British Islands and Mediterranean Region, organising activities in support of the Commonwealth Women Parliamentarians network. We also works to strengthen the Commonwealth Association of Public Accounts Committees in its core objectives.

CPA UK continues to work in partnership with a multitude of national and international organisations for mutual benefit; including the Commonwealth Secretariat, World Bank, United Nations Development Programme (UNDP), United Nations Environment Programme (UNEP), Organization of American States (OAS) and the UK Government.

MEET THE CPA UK TEAM

JON DAVIES

CHIEF EXECUTIVE

RUTH POPE

HEAD OF MULTILATERAL PROJECTS TEAM

ELORM HALIGAH

PROJECTS AND PROGRAMMES MANAGER, MULTILATERAL PROJECTS TEAM

VICTORIA BOWER

DEPUTY HEAD, MULTILATERAL PROJECTS TEAM

ELLEN BOIVIN

PROJECT ASSISTANT, MULTILATERAL PROJECTS TEAM

RAHEL KIBRU

PROJECT ASSISTANT, MULTILATERAL PROJECTS TEAM

MATTHEW HAMILTON

MONITORING AND EVALUATION MANAGER

MARK SCOTT

COMMUNICATIONS MANAGER

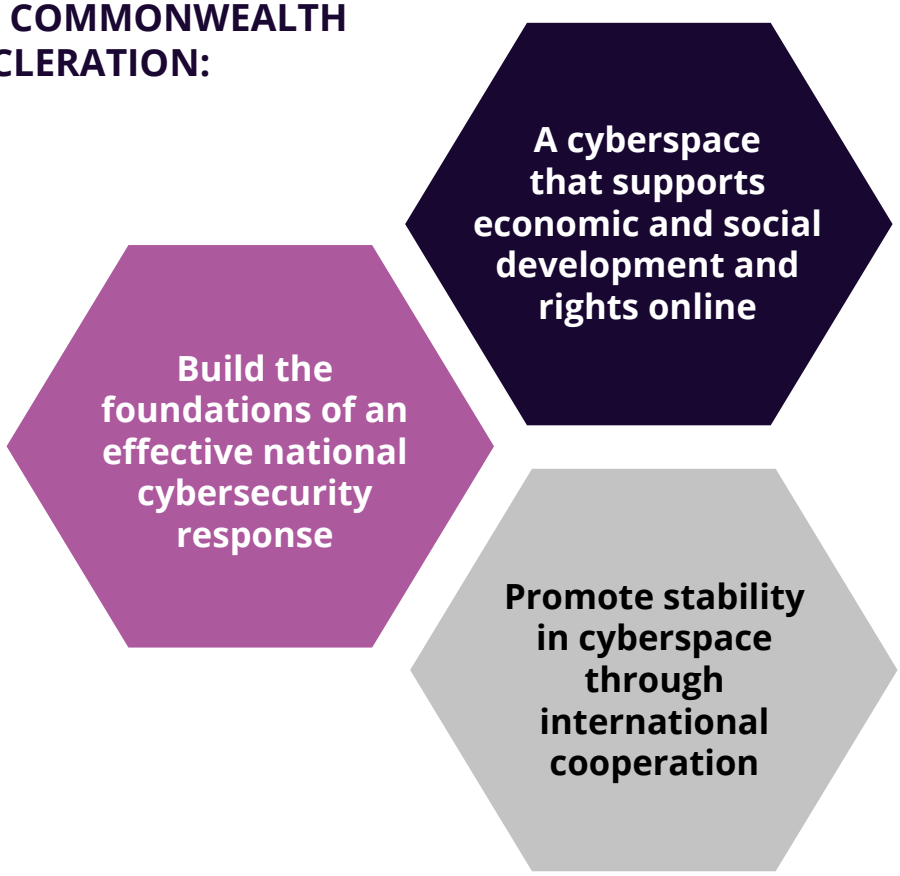
INTRODUCTION

The Cybersecurity Workshop, delivered in partnership with the Ministry of Justice, the University of Oxford and the Foreign and Commonwealth Office, was developed to enable Parliamentarians from across the Commonwealth to build their capacity to legislate and scrutinise on cybersecurity issues.

The workshop provided a unique opportunity for participants to share international and regional best practice, whilst considering ways in which Commonwealth Parliaments can support each other in combatting cybercrime and developing cybersecure legislation.

The objective of the workshop was to explore and support the delivery of the commitments in the 2018 Commonwealth Cyber Declaration*, including raising awareness of current cybersecurity threats and challenges. Participating delegates had a range of profiles, from newly elected parliamentarians to committee members as well as shadow and national ministers with cybersecuirty portfolios.

*THE 2018 COMMONWEALTH CYBER DECLERATION:



SOURCE:
https://thecommonwealth.org/sites/default/files/inline/Commonwealth-Cyber-Declaration.pdf

WORKSHOP OVERVIEW

CPA UK welcomed 25 commonwealth parliamentarians to London for the Cybersecurity Workshop. Delegates from all regions of the Commonwealth and the UK Overseas Territories convened for the three-day programme held across Westminster and Oxford.

On the first evening of the Workshop, delegates heard from cybersecurity and legal experts from the Ministry of Justice and Chatham House, who gave an overview of recent cybersecurity developments within a judicial and legal context. Delegates were then given the opportunity to join world-leading academics at the University of Oxford to learn about the importance and impact of strong links between policymakers and researchers. Amongst the vast range of topics covered were sessions on national cybersecurity capacity, the future of cyberpolitics and digital ethics. Parliamentarians were also able to share their national progress in cyber protection, learning about Malta's 'five pillar approach': policy, legislation, risk management, culture and education, and Ghana's National Cybersecurity Bill expected to pass later this year.

With part of the programme held at the Houses of Parliament, delegates were able to hear from UK Members of Parliament and representatives from the National Audit Office on the role of committees in providing effective scrutiny of national cyber policy. Looking closely at the work of the UK Public Accounts Committee, delegates were given guidance on the role of parliamentarians in delivering oversight on complex and technical matters around cybersecurity.

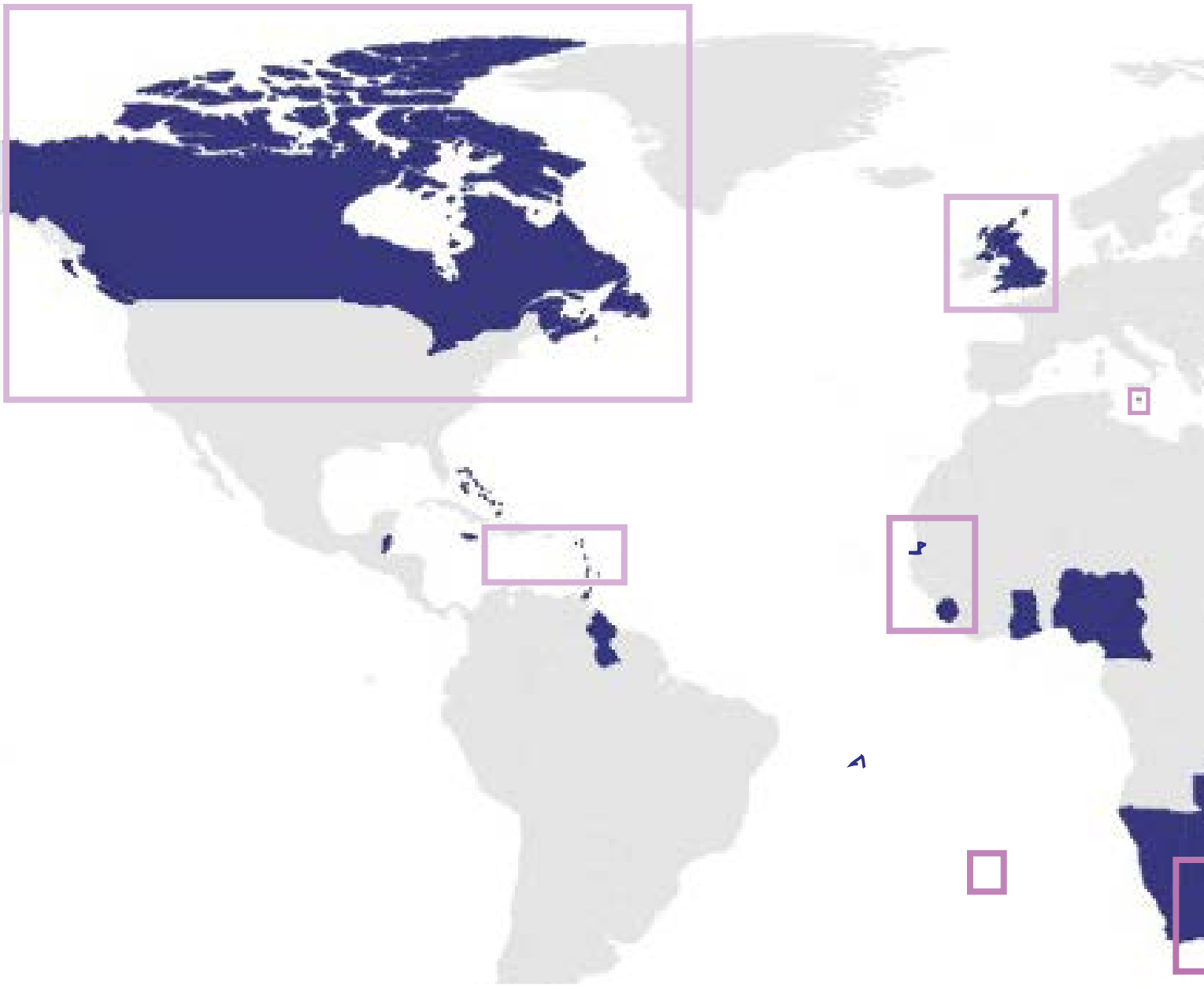
On the final day, delegates were welcomed to the Foreign and Commonwealth Office by Lord Ahmad of Wimbledon, Minister of State for the Commonwealth, whose key message outlined the importance of international cooperation in the fight against cyber-threats. The day also included speakers from the Home Office and the Cabinet Office who gave participants a detailed insight into the UK's cybersecurity structures and their current capacity.

With the fast-changing nature of technology and the huge potential for innovative policy solutions across the globe, delegates were keen to continue the valuable exchange of information through future programmes, in order to ensure Commonwealth parliaments are able to respond effectively to the challenges around cybersecurity.

"SHARING BEST PRACTICE ACROSS THECOMMONWEALTH helps to strengthen cyber defences while respecting and getting the balance right when it comes to freedom of expression**."**

Lord Ahmad, Minster of the Commonwealth

DELEGATE BREAKDOWN



PARTICIPATING LEGISLATURES

8 National Parliaments
3 Subnational Parliaments
1 Crown Dependency
1 UK Overseas Territory
1 Provincial Legislature

DELEGATE NUMBERS

25 Parliamentarians
14 Legislatures
14 male
11 Female

LIST OF DELEGATES

PARLIAMENT OF BANGLADESH
Mr Kazi Nabil MP
Mrs Khadizatul Anwar MP

LEGISLATIVE ASSEMBLY OF THE PUNJAB, PAKISTAN
Ms Syeda Uzma Qadri MPA
Mr Zahid Akram MPA

LEGISLATIVE ASSEMBLY OF THE CAYMAN ISLANDS
Ms Barbara Conolly MLA
Mr Kenneth Bryan MLA

NEW ZEALAND HOUSE OF REPRESENTATIVES
Mr Andrew Falloon MP

STATES OF JERSEY ASSEMBLY
Deputy Judy Martin
Deputy Scott Wickenden

PARLIAMENT OF SIERRA LEONE
Hon Rugiatu Kanu
Hon Musa Lahai

JAMAICA HOUSE OF REPRESENTATIVES
Mrs Ann-Marie Vaz, MP, JP
Mr Fitz Jackson, MP

PARLIAMENT OF GHANA
Hon Catherine Afeku
Hon Emmanuel Kwasi Bedzrah

PARLIAMENT OF SAINT LUCIA
Hon Hermangild Francis
Hon Ernest Hilaire MP

PARLIAMENT OF MALAYSIA
Hon Noraini Ahmad
Hon Shamsul Iskandar Mohd Akin

PARLIAMENT OF KENYA
Hon William Kisang MP
Hon Millie Odhiambo-Mabona MP

PARLIAMENT OF MALTA
Hon Silvio Grixti
Hon Therese Comodini Cachia

PARLIAMENT OF PAKISTAN SINDH
Mr Ghanwer Ali Khan Isran MPA

AUSTRALIAN CAPITAL TERRITORIES LEGISLATIVE ASSEMBLY
Mr Michael Pettersson MLA

PARLIAMENT OF TASMANIA, AUSTRALIA
Ms Madeleine Ogilvie MP

PARLIAMENT OF NEW SOUTH WALES, AUSTRALIA
Hon Scott Farlow MLC
Mr Guy Zangari MP

OUTCOME AND OUTPUTS

Our desired outcome was for Parliamentarians from across the Commonwealth to develop capacity in order to more effectively legislate, scrutinise and deliver oversight in their respective jurisdictions in relation to cybersecurity. The outputs for the CPA UK Cybersecurity Workshop are set out below.

The following pages of this report outline some of the session highlights, dividing them according to Outputs 1 and 3. Please note Output 2 has been excluded as it is a consistent thread throughout the whole workshop.

OUTPUT 1:

Parliamentarians will have a deeper understanding of international cybersecurity policy frameworks.

OUTPUT 2:

Parliamentarians will build a network of colleagues from across the Commonwealth that will share good practice on cybersecurity issues.

OUTPUT 3:

Parliamentarians will have enhanced technical skills and improved capacity to scrutinise and hold government to account on cybersecurity issues.

OUTPUT 1

TECHNOLOGICAL REVOLUTION AND INTERNATIONAL RELATIONS

Speaker: Professor Lucas Kello, Associate Professor of International Relations, Director of the Centre for Technology and Global Affairs

We were delighted to welcome Professor Lucas Kello to our Oxford programme to explore the phenomenon of technological revolution within the international system. Professor Kello was particularly keen to address some of the contemporary challenges of adapting security strategy and policy to new technologies of conflict.

The session began by looking at the historical development of technology during periods of conflict (for example the use of tanks). The speaker emphasised the multitude of conflict-oriented computer systems, such as nuclear systems, that still remain vulnerable to manipulation by hostile forces despite operating outside the visible internet. The speaker highlighted various examples of recent cyber-attacks that threatened the stability of the international system, such as the 2014 'Sony Pictures' attack poignantly described by Barack Obama as "not as an act of war but an act of cyber-vanadalism."

Professor Kello went on to outline the various debates surrounding the accuracy of predicting cyberthreat levels. Is the risk of cybercrime on both an individual and institutional level exaggerated by governments? Professor Kello made it clear that we should not underestimate the potential consequences of a threat just because there is no immediate or visible threat to life; a cyber-attack has the potential to have significant financial and social effects. This is why, in the UK, cyberthreats are classified as Tier 1 – "of the highest priority for national security."

During the discussion that followed, one delegate suggested that 'an act of war' should be redefined to cover cyber-attacks, highlighting the impact of cyber interference in the US presidential elections. Lucas Kello introduced the concept of 'unpeace' as a means of describing the relationship between international actors in an ongoing state of cyber-warfare. Kello described 'unpeace' as a state that is neither war nor peace; where there is not enough physical destruction to constitute a conflict, yet there is too much harm being done for peace to exist.

Delegates ultimately agreed with Lucas Kello's conclusion that international law is yet to formulate the required mechanisms to handle situations of cyber-conflict. The crucial importance of academia and research was highlighted, as was the importance of legislatures working together to ensure that national and international law effectively counters cyberthreats.

LAW AND CYBERSECURITY

Speaker: Professor Rebecca Williams, Professor of Public Law and Criminal Law, Faculty of Law, University of Oxford

In her informative session on law and cybersecurity, Professor Rebecca Williams asked delegates two questions: how can the law best respond to cybersecurity threats, and how can we optimise the effectiveness of the law as a tool for accountability and deterrence?

Rebecca Williams began the session by looking at the creative ways in which the UK has tried to deal with cybercrime within the limitations of existing law, for example through using counterfeiting legislation. She introduced the case study of the Computer Misuse Act 1990 (CMA) as an early attempt by the UK Government to deal with cybercrime in response to the need for new legislation.

Several notable problems with the CMA were highlighted, including its overlap with existing legislation, and the very real risk of overcriminalisation. That is, the law does not protect those whose are legitimately employed to hack into computer systems and find gaps to report back to organisations – under the law this would still be considered digital trespass and therefore illegal.

Delegates were able to take away several key messages from this session. Firstly, within criminal law there are some advantages to avoiding technology-specific legislation, as cyber offences can simply be included in existing legal frameworks. A significant advantage of this is that judges and prosecutors already have an in-depth understanding of existing laws and can therefore use them more effectively.

Secondly, policymakers must let technology lead the law. It is more effective for legislatures to work backwards from what is technically possible at a given time, and then design laws accordingly. During the development of cybersecurity policy, it is important to think about the entire legal process, from educating judges on a law's application and explaining the law to juries, to reaching a final conviction.

Delegates came away from this session with an enhanced understanding of the differences between successful and unsuccessful ways of developing laws in response to the challenges of new technologies.

OUTPUT 1

LOOKING BACK: THE COMMONWEALTH CYBERSECURITY PROGRAMME 2018 - 2020

Speakers:
Matthew Moorhead, Acting Head, Office of Civil and Criminal Justice Reform, Commonwealth Secretariat
Esther Naylor – Research Assistant, International Security Programme, Chatham House
Michael Potter, Head, Commonwealth Cybersecurity Programme, FCO

At the 2018 Commonwealth Heads of Government Meeting, the Commonwealth Cyber Declaration was signed. Through this, all countries unanimously committed to take action on cybersecurity between 2018 and 2020. The declaration is the world's largest and most geographically diverse inter-governmental commitment on cybersecurity cooperation. This session took a look at the progress made across the Commonwealth since the declaration was made.

Our first speaker Matthew Moorhead focused on the Commonwealth Heads of Government Meeting (CHOGM) in which 54 countries developed and signed the Commonwealth Cyber Declaration, which included commitments to economic and social developments in cyber, and to promote stability in the cyber realm.

The Commonwealth Secretariat has worked on various projects in support of the Declaration, including a project focused on building cyber capability in Kenya, Namibia and The Gambia to develop cybercrime legislative reforms. The Secretariat have also initiated a programme focusing on training for judges, investigators and prosecutors in the delivery of effective prosecution for cybercrimes. Matthew Moorhead emphasised the importance of this training for the continuation of capacity building.

Other programmes mentioned during the session included a committment to the strengthening of international networks and transnational cooperation in the field of cybersecurity, and a focus on enhancing election processes across the Commonwealth.

The second speaker, Esther Naylor, began by discussing Chatham House's work in creating a network of diverse experts to look at capacity building and the identification of gaps in legislation across regions.

The priority of Chatham House is to improve cyber policy by increasing the knowledge around cybersecurity both at a citizenry level and within legislatures. These programmes come under three pillars akin to the Declaration:

1. **Supporting economic and social rights online**
2. **Building the foundations of an effective national cybersecurity response**
3. **Promoting stability in cyberspace through international cooperation.**

Finally, Michael Potter shared the achievements of the FCO Cyber Programme, including increased national reviews for identifying areas for improvement and establishing a better intersection between civil society and legislatures.

Several important lessons were learnt during the delivery phase of the FCO Cyber Programme. These included the power of establishing and maintaining networks to share best practice, the need for increased awareness of the Declaration, and the need to have a better understanding of progress in cyber policy across other regions. These sentiments were echoed by several delegates.

Delegates gave feedback on progress around the Declaration within their national contexts. Comments focused on the suggestion that analogue is still the safest model for holding elections, the issue of varying resources across the Commonwealth in implementing the Declaration, and the need for a portal with presenting the different laws adopted.

One delegate inquired about the evaluation of these programmes and the Declaration. The speaker responded that this is currently being reported on and will be reviewed at the next CHOGM.

OUTPUT 3

A PRACTICAL GUIDE TO CYBERSECURITY AND HUMAN RIGHTS IN ACTION

Facilitated by: Sheetal Kumar, Senior Programme Lead, Global Partners Digital

Global Partners Digital (GPD) works with governments to make policy spaces and processes more open, inclusive and transparent. They hold the secretariat for the Freedom Online Coalition, a partnership of 31 governments working to advance internet freedom. Through this session, GPD provided an overview of the links between cybersecurity, cybercrime and human rights, before providing participants with the skills to effectively analyse cybersecurity and cybercrime legislation from a human rights perspective.

Sheetal Kumar opened the session by emphasising there is a mutually reinforcing relationship between cybersecurity, cybercrime and human rights and that cybersecurity legislation and policy should be underpinned by human rights and democratic values. In highlighting a just few of the harms posed by the internet, the speaker and delegates referred to fake news, bullying, organised crime, identity theft, fraud, discrimination, data protection, child sex exploitation.

The speaker went on to discuss the need to ensure that legal definitions of cybersecurity should not lose the human dimension and should preserve the integrity and confidentiality of information. She also emphasised the importance of developing a policy landscape inclusive of human rights, in which all stakeholders are engaged and key human rights principles are included.

The two areas of rights that could be most at threat by cyber policies are the right to privacy and freedom of expression. In ensuring cybersecurity measures do not violate privacy, legislatures can enact strong data protection laws and promote digital literacy.

One delegate raised concerns around the ability of companies to collect personal data and use website tracking. They asked how data protection legislation should apply in such cases, particularly considering companies usually operate beyond legislative jurisdiction. The speaker responded by saying that strong data protection legislation should protect citizens rights and impose obligations on those who gather data.

Sheetal Kumar raised the question of whether freedom of expression could be infringed upon, or impacted upon negatively, in situations where websites have been shut down or free speech limited as a result of a cyberattack. In response, a delegate asked how to draw the line between giving up civil liberties and encouraging use of technology? The speaker highlighted the importance of legislation in being able to balance both.

Reference was made to the three-part test used by GPD to ensure that legislation respects human rights. The test makes it clear that any cybersecurity measures implemented by a country must:

1. **Have a basis in law**
2. **Pursue a legitimate aim**
3. **Be necessary and proportionate**

Towards the end of the session, delegates were given a piece of cybersecurity legislation to analyse. Amongst some of the key human rights issues identified were; the exclusion of 'all knowingly' and 'intentionally' from sections of the text, the unclear penalty for committing the offence, and the general lack of clarity around particular definitions leaving the legislation open to varied interpretation.

INTERNET 101 (INTERACTIVE)

Speaker: Douglas Taylor, Foreign and Commonwealth Office

It was a pleasure to welcome Douglas Taylor for a very interactive, conversational session looking at the different components and mechanisms of the internet and how they operate.

The session began by looking at the history of the internet, which - according to the speaker - was orignally a centralised network that gradually became decentralised. The internet therefore, is not one single entity but constitutes a resiliant hierarchy of individual networks.

The speaker made a clear distinction between the internet and the World Wide Web, the latter dating back to the 1990s when it was developed as a way to store data and link together bodies of text to present them in browsers.

Douglas Taylor went on to discuss the existance of the deep web, the contents of which are not indexed by standard web search-engines. This unindexed web, which also includes the 'dark web', cannot easily be accessed and is therefore commonly used by anonymised criminals to carry out ilicit activities. The speaker also highlighted some lesser-known ways that the deepweb can be used, including by human rights advocates in authoritarian regimes where internet blocks are in place restricting communication.

The concept of the 'internet of things' (a system of interrelated computing devices connected to the internet, such as mobile phones or smart household applicances) was also a key topic of discussion. It was identified that there is a need to ensure these devices are secure and protected, otherwise they are at risk of being corrupted.

The utility and importance of this session was widely acknowledged by delegates who agreed that the information and core definitions provided by Douglas Taylor are crucial in helping legislators to understand how cybersecurity works on a larger scale.

NATIONAL CYBERSECURITY STRATEGIES

We have put together a sample list of cybersecurity strategies from some of the countries that were present at the workshop, based on what is available, as this was a common request from delegates. The links are embedded in the country title below.

AUSTRALIA

BANGLADESH

CAYMAN ISLANDS

GHANA

JAMAICA

KENYA

MALTA

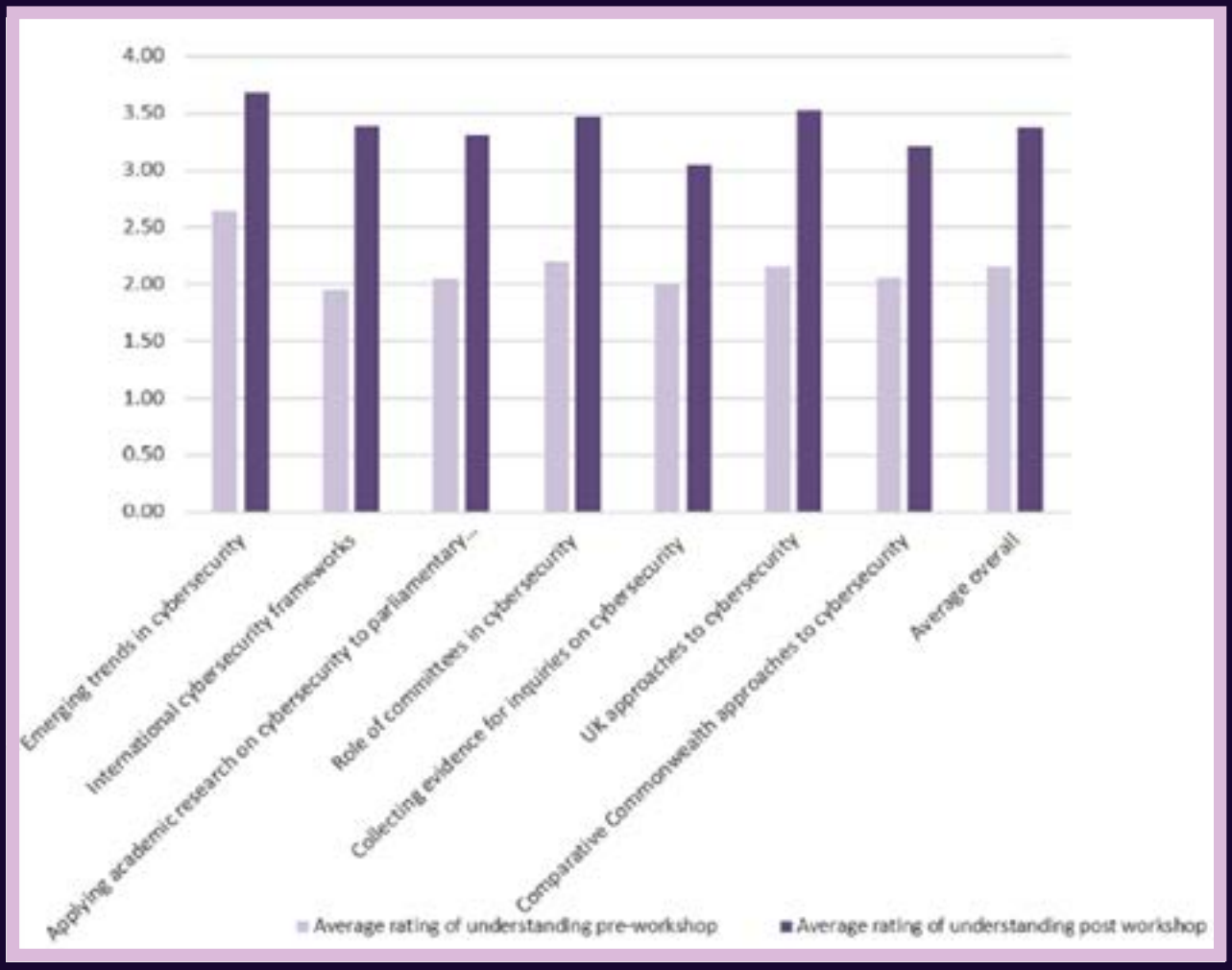
NEW ZEALAND

SIERRA LEONE

JERSEY

DELEGATE FEEDBACK

As part of the workshop's monitoring and evaluation process, delegates were asked to complete pre- and post-workshop assessment forms to measure how effective the workshop had been in raising their level of understanding on cybesersecurity related topics. The graphs below show that the average level of delegate understanding substantially increased across the board as a result of the workshop.



100%

of the participants said the workshop either met or exceeded their expectations

95%

of participants said the workshop was relevant to their role

"I am now fully equipped to critically discuss and analyse issues relating to cybersecurity. I came with limited knowledge and now have a wealth of experiences to take back."

"I now have a greater understanding of cybersecurity and how human rights and economic opportunity depend on it."

"The workshop has made me more cognizant of the dangers and opportunities of the internet, especially in the development of small nation states."

As part of the post-workshop assessment form, delegates were asked how they would apply their learning and knowledge gained during the workshop on return to their respective parliaments. A small selection of responses are highlighted below.

CONCLUSION

The CPA UK Cybersecurity Workshop was successful in providing a learning platform for Parliamentarians across the Commonwealth to develop their capacity to more effectively legislate, scrutinise and deliver oversight in their respective jurisdictions in relation to cybersecurity.

With security being one of CPA UK's core thematic areas, we cannot understate the importance cybersecurity has to play in parliaments across the Commonwealth. There was a unanimous desire expressed by participating parliamentarians to ensure that they contribute to the effort to educate young people in their jurisdictions on this ever-expanding area. A committment was made by all to help in driving forward this agenda in the years to come.

Since CPA UK's last cybersecurity workshop held in 2017, we have seen many major developments in the field played out on the global stage. Particularly as this workshop took place during the time of the Covid19 global outbreak, we are increasingly seeing the importance our cyberspace has to play as not only a carrier of news, but also as a provider of alternative working solutions for citizens in the wake of such events. This conveys the importance of holding forums like this regularly, to provide a platform for legislators to keep up to date and remain well equipped to play their role in upholding a safe cyberspace.

NEXT STEPS

Based on exchanges throughout the few days and feedback from the delegates, we have seen that there is appetite for in-country and regional working groups pertaining to cybersecurity to be set up, in order to continue to uphold the pledges made in the 2018 Commonwealth Cyber Declaration. CPA UK will conduct follow up conversations with all delegates six months after the workshop to gauge the impact it has had upon the development of their capacity to legislate and scrutinise within cybersecurity.

Moreover, we will ascertain at that point if any legislatures need support to take this work further and will see how we at CPA UK can assist. We also plan on holding a Security Conference within the next year. Dates are, of course, yet to be confirmed due to the current Covid19 pandemic. Once the finer details are established, we will notify your respective parliaments.

CPA UK
Westminster Hall | Houses of Parliament | London | SW1A 0AA
T: +44 (0)207 219 5373
W: www.uk-cpa.org
E: cpauk@parliament.uk