UK Parliament

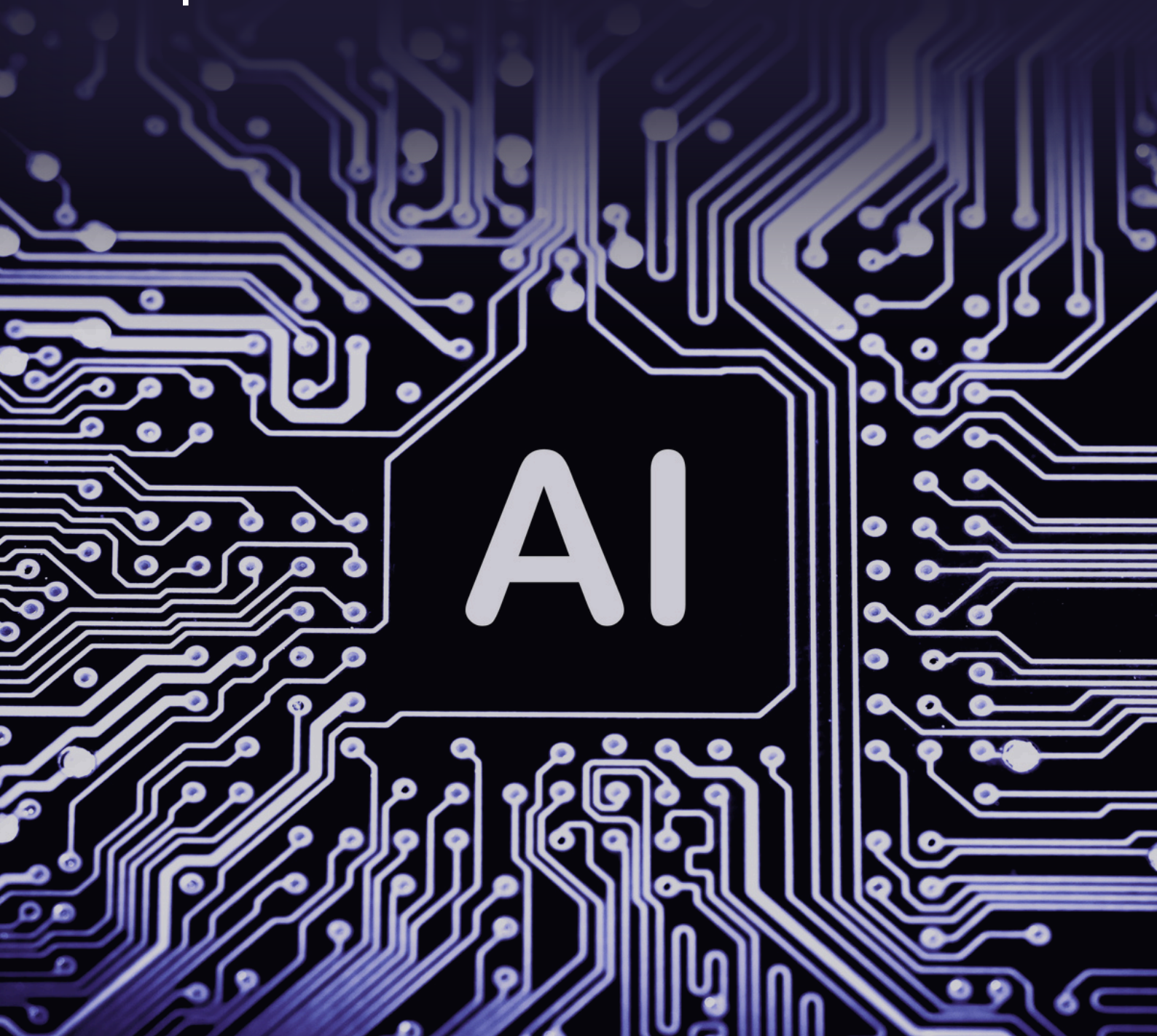
CHATHAM HOUSE

COMMONWEALTH PARLIAMENTARY ASSOCIATION UK

Artificial Intelligence in Security Workshop

28 - 30 January 2025

Report



CONTENTS & OUTCOMES

OBJECTIVE

Delegates will be able to deliver more effective parliamentary oversight and scrutiny of artificial intelligence (AI) and security-related issues.

OUTPUTS

1. Delegates will enhance critical skills to scrutinise AI and security issues.
2. Delegates will expand their professional networks, creating open communication and collaboration with peers to share best practices on AI and security regulation.
3. Delegates will increase their understanding of the opportunities and challenges posed by AI in the context of security.

PROGRAMME OVERVIEW

Members of Parliament from across the Commonwealth participated in CPA UK's AI in Security Workshop, hosted in collaboration with international think tank Chatham House from 28 – 30 January 2025 in the UK Parliament.

CPA UK's first AI Workshop, brought together thirty parliamentarians from fifteen commonwealth legislatures, representing Africa, the Caribbean, Europe, Asia and the Pacific. Delegates gathered in Westminster to discuss the impact of artificial intelligence on security and democracy worldwide.

Throughout the workshop, delegates heard from a wide variety of international expert speakers, from within and outside the UK parliament, addressing the workshop's key themes of AI-enabled disinformation, cybersecurity, defence, and international frameworks for responsible AI governance. Exchanging experiences and sharing ideas, delegates explored strategies to counter emerging threats as well as strengthen democratic resilience in the face of rapidly evolving technologies.

PARTICIPATING LEGISLATURES

Asia-Pacific

Parliament of Malaysia

Parliament of New South Wales, Australia

Parliament of New Zealand

Parliament of Sri Lanka

Africa

Parliament of Eswatini

National Assembly of The Gambia

Parliament of Kenya

National Assembly of Nigeria

Parliament of Sierra Leone

Americas, Caribbean and Europe

National Assembly of Belize

Parliament of Canada

States of Deliberation, Guernsey

Parliament of Jamaica

States Assembly, Jersey

Parliament of Saint Lucia

Parliament of United Kingdom

KEY DISCUSSIONS

AI in Cybersecurity and the Military

Delegates heard from a number of speakers about the increasing use of AI in security and defence, and the risks and benefits this presents. As technology continues to develop at such a fast pace, AI is becoming a new component in defence, with more and more nations leveraging AI for strategic advantage on the battlefield. Warfare is increasingly being driven by digital technology, and it is crucial, therefore, that defence ministries remain flexible and responsive to new technologies. However, this evolution also introduces significant risks and vulnerabilities.

Each new AI capability introduces security risks, especially as developments become more complex and vulnerable to threats. AI will also increase the volume of cyberattacks in the near term, with bad actors often acting more innovatively than governments, using AI to automate and scale cyber threats. This significantly increases the risk of ransomware and phishing attacks, particularly following the rise of cryptocurrency acting as an untraceable currency.

AI is being used in both offensive and defensive cyber operations. On the offensive side, it can facilitate misinformation, phishing and the creation of malicious code. Whereas on the defensive side, AI can help identify and fix vulnerabilities, analyse data and threats more quickly, as well as reduce the workload of skilled cyber experts, allowing them to focus on more complex tasks.

Non-state actors, particularly those without advanced technological expertise, are increasingly utilising AI, leading to more sophisticated disinformation campaigns and cyber threats.

These issues are not limited to technologically advanced states, countries across the commonwealth are facing challenges in keep up with cybersecurity threats. While some have existing legislation, many need updates and further development. Additionally, there remains the unresolved question around who should be responsible for enforcing cybersecurity standards, accountability and support to victims of cyberattacks.

From a military standpoint, AI is transforming the character of conflict. There is a strategic disadvantage in failing to adopt AI, however, there are concerns over ethics. Though AI can be deployed, it does not necessarily mean that it should, and nations should consider whether AI-driven systems and weapons will provide the security and reliability needed on the battlefield. Furthermore, though technology continues to advance, the role of human oversight remains critical. Though AI may enhance decision making, there will continue to be a need for personnel on the ground.

AI in Cybersecurity and the Military

Another key issue when implementing AI in defence is its role in classified data and military intelligence. AI is a useful tool in identifying patterns and analysing vast amounts of information, therefore making it highly useful for intelligence gathering. However, integrating AI into classified information spaces could present significant challenges concerning information security.

At an international level, there is not yet an established UN process governing AI in the military domain. While discussions on autonomous weapons, cyber warfare, and cognitive warfare exist, approaches to AI policy vary widely across regions, with smaller states in particular struggling to keep up with the AI arms race due to resource constraints.

Addressing these challenges requires a proactive and collaborative approach, ensuring that nations not only mitigate risks but also harness AI's potential responsibly and effectively. Firstly, nations could prioritise AI investment, rather than simply reacting to new developments. Playing catch-up can leave countries vulnerable to actors that are more advanced in AI technology. Furthermore, as an international issue, addressing cyber threats requires a coordinated, global response. Commonwealth nations could continue to explore how research and best practices can be shared to improve collaboration and cybersecurity resilience. Finally, nations should continue to recognise the importance of human oversight. Many security failures occur due to simple failures, highlighting the need for well trained personnel and effective intervention strategies. Small businesses and the public must also be equipped to protect themselves, be able to identify bad actors and mitigate threats. Digital literacy is vital, and governments should consider introducing initiatives and programmes to support public awareness.

Disinformation and Democratic Resilience

Through discussions with experts and panellists, delegates recognised the growing threat of AI-generated disinformation and its far-reaching consequences, while also considering potential strategies to strengthen resilience and accountability. The rise of generative AI has made it ever more possible to disseminate misleading information, such as deep fakes and manipulated media, which have been and continue to be used to target individuals worldwide, particularly women. The increase in AI generated disinformation is leading to an erosion of trust in information, where the public are becoming increasingly sceptical of content. Concerningly, this scepticism is not only reserved for AI-generated material; the public are also growing sceptical of legitimate online content, illustrating the growing complexity of verifying the credibility of information and media.

AI-generated disinformation can harm democratic resilience, by targeting key figures and vulnerable groups, such as female politicians, spreading false narratives that influence public opinion. Existing legislation often fails to address AI's role in disinformation, and social media strategies for politicians often prove inadequate as they were designed before the rise of generative AI. A lack of political party codes of conduct on the use, sharing and re-sharing of AI generated content further complicates accountability.

To address the pressing and immediate challenge of AI-enabled disinformation, parliamentarians could consider legislative reform to tackle harmful AI-generated content, such as deep-fakes. Similarly, to promote accountability amongst tech companies, countries could consider agreeing on unified demands to obligate them to address misinformation effectively.

Strengthening the capacity of regulatory bodies is also essential to ensure they are able to effectively combat misinformation, therefore countries should ensure that regulators are provided with sufficient funding, resources and expertise. Finally, to promote democratic resilience, countries should ensure electoral commissions and political parties provide clear guidance for members and politicians on responsible use of social media.

To effectively address the challenges posed by AI-enabled disinformation, policymakers can consider a range of strategic measures, including legislative reforms, stronger regulatory frameworks, and enhanced democratic safeguards.

Key approaches include:

Legislative Reform:
Introduce laws to tackle harmful AI-generated content, such as deepfakes.

Unified Tech Regulations:
Countries could collaborate on shared requirements to hold tech companies accountable for addressing misinformation.

Strengthening Regulators:
Ensure regulatory bodies have adequate funding, resources, and expertise to combat misinformation effectively.

Responsible Political Engagement:
Electoral commissions and political parties could provide clear guidance on responsible social media use for members and politicians.

Digital Colonialism and Power Dynamics in AI

Delegates explored the significant challenges post-colonised states face with data sharing, often highlighting how governments and institutions may not fully grasp its long-term implications. Post-colonised states are unknowingly giving data freely to large tech companies, often without recognising the harmful effects it could cause. It is not possible to know how the data is being used or who is being affected the most. Countries in the global south, and technologically underdeveloped countries are most at risk, and since technology is so fast growing, it is not possible to know the full extent of the harms. The rise of AI is similarly having a detrimental effect on the environment, consuming large amounts of water and energy and land through data centre sites. Low-income countries have been disproportionately affected by this, with many becoming dumping grounds for e-waste. Additionally, the prevalence of digital homogenisation reinforces global reliance on Big Tech from dominant countries, allowing these companies to exert growing influence on government decisions, while disadvantaging smaller nations by limiting their digital sovereignty and economic competitiveness.

Alongside data, labour is flowing from low-income to high-income countries, with digital platforms exploiting labour from low-income nations, while often framing this as a means of promoting development. Although there is the possibility of AI to create new jobs and boost economies, these benefits will be experienced by nations that have already set up the infrastructure. Currently, 66% of Commonwealth nations have no AI strategy, with it often costing between $250,000 - $1.5 million to create a national strategy. However, by the time a strategy is developed, the technology has often already advanced beyond it.

To address and mitigate these challenges, Commonwealth countries could benefit from greater collaboration on this issue, viewing the AI crisis as a global issue rather than developing individual AI strategies. Through collaboration, representing 2.4 billion people, they could strengthen their bargaining power and create more competitive data sets to rival AI leaders and Big Tech. However, for this approach to succeed, mutual trust and transparency among Commonwealth members will be essential.

Furthermore, due to shared and common histories, Commonwealth countries often share similar legal, institutional and governance foundations. In recognition of this, the Commonwealth Secretariat has created a new AI toolkit to support these nations in formulating effective AI strategies. This new tool is able to significantly reduce the time required to draft AI strategies, cutting the processing time down from 9 –12 months to 6 days. By leveraging shared frameworks and fostering collaboration, Commonwealth nations can remain take a unified approach to AI regulation, ensuring they remain competitive while safeguarding their collective interests.

AI Governance and Collaboration

After engaging with experts, delegates recognised the increasing importance of AI regulation as its benefits become more widely acknowledged, while also highlighting the complexities and challenges of establishing effective governance in this rapidly evolving field. In recent years, the global focus has shifted away from focusing on concerns over AI to exploring its potential advantages, however, this evolution highlights the growing need for effective regulation. The challenge lies in the complexity of applying governance to AI, as it appears unlikely that there will be an agreement on regulation that will arise on an international level.

AI present significant opportunities for business innovation and economic growth, however, it is essential that there is regulation present to safeguard data protection and copyright. That said, it is similarly important that regulation does not stifle this growth and limit innovation.

For a system to be properly regulated, AI requires a polycentric governance approach, combining soft law, binding agreements and industry standards. There already exists a number of global soft law instruments focusing on AI, such as OECD AI Principles, G7 Hiroshima AI Process, and the Africa AI Continental Strategy, which allow for quicker agreement among states. However, due to their non-binding nature, there are increasing calls for enforceable legal obligations to ensure compliance and accountability.

A further challenge is the regulation of powerful tech companies, some of which now having significant influence over national governments and being worth more than some countries' GDP. States are obligated to regulate companies in their jurisdiction and ensure they do not create harms. However, as Big Tech continues to gain influence, the likelihood of significant improvements in regulation may vary across different regions.

AI Governance and Collaboration

Certain regions of the Commonwealth face further challenges regarding AI governance, more specifically nations with limited capacity to build AI expertise. Furthermore, for many of these nations, even when the skills are developed, there is often brain drain, leaving countries without a workforce to sustain governance. Additionally, financial constraints can hinder the development of AI, which could lead to some countries being subjected to regulations that are not best suited to their context.

International cooperation has been highlighted as a vital mechanism to support enforceability and compliance. The EU and UN AI offices, BRICS AI working group, UK AI Safety Summit and the Global Digital Compact all represent useful avenues to foster collaboration and promote international dialogue. Though a general global treaty would be difficult to get national buy-in, or would most likely be watered down, global initiatives, regional and domestic law are all key and the Commonwealth has a large role to play in that.

Furthermore, recognising the need for continuous learning as AI evolves, the Commonwealth Secretariat continues to do extensive work in this area, having created a Commonwealth AI consortium in 2023, as well as four AI working groups. They have also established an AI incubator, as well as an AI mega fund to incentivise innovation and introduce infrastructure.

.

While the path towards effective AI regulation will be challenging, encouraging collaboration and continuous learning, as well as adaptable frameworks will be key to ensure that countries are able to balance innovation with the protection of national and global interests

RESOURCES

Strategius AI
AI-Driven Policy Tool – Commonwealth Secretariat

StrategusAI is a governance solution: a model to help policymakers create tailored AI policies. It provides access to expertise, with references and best practices from organisations like the OECD and World Bank, allowing for quick drafting of policies within budget constraints. It allows for customisation, adapting policies to fit local economic, social, and regulatory contexts.

https://strategusai.thecommonwealth.org/

Use of AI in Government
Oral Evidence – UK Public Accounts Committee - House of Commons

Delegates had the opportunity to witness the UK Public Accounts Committee Oral Evidence hearing. This oral evidence session sought to explore how effectively the UK Government have set themselves up to maximise the opportunities and mitigate the risks of AI in providing public services, as well as how they plan to roll out an overarching AI policy across government departments. The session also examined how officials intend to overcome barriers to AI adoption in the public sector, including challenges with legacy IT structures, data access and quality, and AI guidance standards and assurance.

A recording and transcript of the oral evidence session are available on this link:
http://committees.parliament.uk/event/22503/formal-meeting-oral-evidence-session/

Parliamentary Handbook on Disinformation
AI and Synthetic Media - Commonwealth Parliamentary Association and Organization of American States

The Commonwealth Parliamentary Association (CPA) and the Organization of American States (OAS) have developed the Parliamentary Handbook on Disinformation, AI and Synthetic Media. This handbook provides readers with an overview of disinformation, the different forms it can take and the contemporary techniques used to spread it. The handbook also covers the basics of AI and synthetic media, including their applications in, and implications for, democracy.

A recording and transcript of the oral evidence session are available on this link:
http://committees.parliament.uk/event/22503/formal-meeting-oral-evidence-session/

Official Workshop Photographs

View highlights of the workshop through official photograph gallery

MONITORING AND EVALUATION

At the beginning of the workshop, each participant completed a pre-workshop assessment and then completed a post-workshop assessment at the end, evaluating their own level of understanding of the seven areas explored in the programme. The scale of understanding ranged from (1) “None” to (5) “In-depth”.

Overall, participants found that the workshop increased their knowledge in all seven areas, ranging from 53% to 78%, with an average of 65% across all areas, as illustrated in the below chart. Around 76% of participants found the workshop ‘fully relevant' to their role and 24% stated ‘partially relevant’ while no one said ‘not relevant’.