Commonwealth Parliamentary Cybersecurity and Cybercrime Project

Asia-Pacific Regional Workshop for Parliamentarians

25-28 July 2016
Parliament of Queensland

Workshop Closing Report

#Cyberparl

Organization of American States
More rights for more people

QUEENSLAND PARLIAMENT

The Commonwealth

COMMONWEALTH PARLIAMENTARY ASSOCIATION UK

Contents

Project Overview

The Commonwealth Parliamentary Association UK (CPA UK) - working in partnership with the Organization of American States (OAS), the Commonwealth Secretariat and with the support of the Parliament of Queensland - delivered the Asia-Pacific Regional Workshop on Cybersecurity and Cybercrime for Parliamentarians over the period of 25 - 28 July 2016.

This workshop was one of three regional workshops delivered by CPA UK and its partners as part of the Commonwealth Parliamentary Cybersecurity and Cybercrime Project. The project is being funded by the Foreign and Commonwealth Office (FCO) Cybersecurity Capacity Building Programme.

The Commonwealth Parliamentary Cybersecurity and Cybercrime Project comprises of:

- Asia-Pacific Regional Workshop on Cybersecurity and Cybercrime for Parliamentarians, Brisbane, Australia, 25-28 July 2016
- Caribbean Regional Workshop on Cybersecurity and Cybercrime for Parliamentarians, Officials and Ministers, Washington D.C., USA, 17-20 October 2016
- Africa Regional Workshop on Cybersecurity and Cybercrime for Parliamentarians, Windhoek, Namibia, 21-25 November 2016
- A Cybersecurity Day, 31 March 2017, as part of CPA UK's International Parliamentary Conference (IPC) on National Security, London, UK, 27-31 March 2017

One of the project's main output, the International Parliamentarians' e-Handbook on Cybersecurity and Cybercrime, is to be launched at the IPC in March 2017.

Parliamentary participants of the Asia-Pacific Regional Workshop

Workshop Aim & Objectives

Aim

The aim of the workshop is to improve the awareness of Commonwealth parliamentarians (and officials and ministers) to implement, scrutinise and promote cybersecurity within their respective countries.

Overview

The project encouraged parliamentarians, ministers and senior officials to:

- Help nations develop and implement robust cybercrime legislation
- Support the delivery and implementation of National Cybersecurity Strategies
- Promote the adoption of robust cybersecurity standards around the world
- Strengthen the application of international law and norms of behaviour

Desired Outputs

- Cybercrime and cybersecurity curriculum and materials for senior parliamentarians
- Map key international stakeholders to participate in projects, develop and maintain a multistakeholder network and develop partnerships with host parliaments
- Increase knowledge and engagement by Members of Parliament on cybersecurity and cybercrime, through three regional workshops in Asia, Africa and the Caribbean between July and October 2016
- An E-handbook launched at the International Parliamentary Conference
- A one-day conference on cybersecurity as part of the CPA UK International Parliamentary Conference on National Security

Workshop Overview

The Asia-Pacific Regional Workshop was attended by parliamentarians from the Australian State Legislatures of New South Wales, Northern Territories, Queensland, South Australia and Western Australia, as well as from Bangladesh, the Cook Islands, Fiji, Kiribati, Malaysia, New Zealand, Niue, Pakistan, Samoa, Solomon Islands, Sri Lanka, Tuvalu and the United Kingdom.

The workshop programme comprised of plenary and interactive breakout sessions; a networking lunch co-hosted with the Australian Cyber Security Network (ACSN) and UK Trade and Investment (UKTI); as well as an interactive committee hearing exercise.

Over the course of 3.5 days, delegates had the opportunity to hear from experts and fellow parliamentarians to discuss the role of parliaments and parliamentarians in:

- Formulating, scrutinising and reviewing legislation related to cybersecurity and cybercrime;
- Developing holistic National Cybersecurity Strategies;
- Strengthening regional and international partnerships with regards to cyber-related threats and priorities;
- Promoting collaboration across public and private sectors;
- Engaging and working with civil society to develop awareness of cyber threats;
- Addressing some of the challenges faced in relation to the development and financing of cybersecurity infrastructure.

Parliament of Queensland, venue of the Asia-Pacific Regional Workshop

Acknowledgements

CPA UK and its partners thank the following organisations for their support in the development of this workshop (in alphabetical order):

1. Anti-Phishing Working Group (APWG)
2. Attorney-General's Department, Tonga
3. AusPost
4. Australia Cyber Security Research Institute
5. Australian Cyber Security Centre
6. Australian Cyber Security Network
7. Australian Federal Police (AFP)
8. BAESystems
9. British High Commission, Canberra
10. CERT Australia
11. Children's e-Safety Commission, Australia
12. Commonwealth Cybercrime Initiative
13. CPA Australia Region Secretariat
14. CPA Pacific Region Secretariat
15. Deloitte
16. Department of the Prime Minister and Cabinet, Australia
17. Elemental Strategy
18. International Cyber Policy Centre
19. Internet Corporation for Assigned Names and Numbers (ICANN)
20. Microsoft
21. National Australia Bank
22. National Security College, Australian National University
23. NATO Cooperative Cyber Defence Centre
24. Parliament of Australia
25. Parliament of Queensland
26. Queensland Police Service
27. Queensland University of Technology
28. Quintessence Labs
29. Senscia
30. Sunshine Coast Innovation Centre
31. Symantec
32. UK Trade and Investment (UKTI), Brisbane
33. UNICEF
34. UniQuest UQ
35. Your Digital File

Special thanks must also go to Lorraine Cherney, Melanie Williams and Galih Imaduddin for taking time out of their studies to act as the workshop's summary writers, and whose output has contributed to this report.

Delegate List

Australia, Queensland	Hon. Tim Mander MP
Australia, Queensland	Hon. Di Farmer MP
Australia, New South Wales	Hon. Natasha Mclaren-Jones MLC
Australia, Northern Territories	Hon. Matt Conlan MP
Australia, South Australia	Hon. Vincent Tarzia MP
Australia, Western Australia	Hon. Kate Doust MLC
Australia, Western Australia	Hon. Martin Aldridge MLC
Australia, Western Australia	Hon. Nick Goiran MLC
Bangladesh	Hon. Mahmud-Us-Samad Chowdhury MP
Bangladesh	Hon. Md. Israfil Alam MP
Bangladesh	Hon. Talukder Md. Yunus MP
Cook Islands	Hon. Mona Ioane MP
Cook Islands	Hon. Tutai Tura MP
Cook Islands	Hon. Teokotai Gifford MP
Fiji	Hon. Balminder Singh MP
Fiji	Hon. Ratu Sela Nanovo MP
Kiribati	Hon. Ioteba Redfern MP
Kiribati	Hon. Pinto Katia MP
Kiribati	Hon. Dr Kautu Tenaua MP
Kiribati	Hon. David Christopher MP
Kiribati	Mr Kairo Tetaake
Malaysia	Hon. Datuk Wira Haji Ahmad Hamzah MP
Malaysia	Hon. Datuk Liang Teck Meng MP
Malaysia	Hon. Dr Mohd Hatta MD Ramli MP
New Zealand	Hon. Dr Shane Reti QSM MP
Niue	Hon.Talaititama Talaiti MP
Niue	Hon. Puletama Puletama MP
Pakistan National Assembly	Hon. Ghulam Rasool Sahi MNA
Pakistan National Assembly	Hon. Maiza Hameed MNA
Samoa	Hon. Aumua Isaia Lameko MP
Samoa	Hon. Faumuina Asi Pauli Wayne Fong MP
Samoa	Hon. Ili Seiefano Taateo Tafili MP
Solomon Islands	Hon. Dr Derek Situa MP
Sri Lanka	Hon. Niroshan Perera MP
Sri Lanka	Hon. Malith Jayathilanke MP
Sri Lanka	Hon. Vijitha Herath MP
Tuvalu	Hon. Otinielu T Tausi MP
United Kingdom	Rt Hon. George Howarth MP
United Kingdom	Hon. Shabana Mahmood MP

Day One
Monday 25 July 2016

Official Opening - Introduction to Cybersecurity & Cybercrime

The Speaker of the Parliament of Queensland, Hon. Peter Wellington MP opened the workshop. He summarised that the key theme of the discussions to be held throughout the week was the concept of cyber threats, and how constituents were left vulnerable to them. He explained that the workshop speakers would define and examine criminal activity within cyberspace and how it specifically affected the Asia-Pacific. The introduction concluded with Speaker Wellington thanking the organisers for providing a platform for such an important issue and wished the workshop participants a fruitful and engaging week.

Cyber Threats Part 1: Cybercrime

The session chaired by the **Hon. Tim Mander MP** from Queensland established and provided a broad overview of the type of **criminal activities that occur within cyberspace**. Specifically it covered: fraud, espionage (both private and corporate), paedophilia, child exploitation and ransom. It also examined the tools that facilitate these crimes - such as ransomware, the dark web, crypto currency, and encryption - before providing an insight into how these issues might be addressed and the different approaches that might be needed both nationally and internationally. The session also looked at the impact of various legal and technical system aspects and how parliamentarians can be a part of cyberspace and the movement to counter cybercrime.

Brian Fletcher, Director of Government Affairs for Australia-Pacific, Japan and Korea at Symantec, focused on breaking common myths surrounding cybercrime and cybersecurity. Common myth #1 was regarding the perception that cybercrime is different to other kinds of crime; Mr Fletcher countered this by stating that whilst the nature of cybercrime was complex, essentially it was just another crime committed in a different way. Common myth #2 was that cybercrime is difficult to enact, which Mr Fletcher dispelled by giving examples of simple "phishing" techniques. Finally, Common myth #3 believed that only big businesses were affected by cybercrime; this was proven incorrect with stats showing that small-to-medium enterprises were increasingly being targeted as a result of a complacent attitude to their cybersecurity capabilities. Mr Fletcher utilising Symantec's threat report[1], used the rest of his presentation to highlight the main targets for cybercriminals (the banking and finance sectors), give a profile of the modern-day cybercriminal (who can be anyone from a bedroom hacker to a member of a fully professional cybersyndicate) and provide prominent case studies of companies that had been affected by cybercrime.

Commonwealth Parli
Association UK
CPA UK
Advancing parliamentary democracy from the heart of Westminster
HON. TALUKDER MD YUNUS MP

Brian Fletcher addressing delegates on the myths of cybercrime

Detective Superintendent Glyn Lewis, National Coordinator, Cyber Crime Operations for the Australian Federal Police (AFP), focused on the localisation of the threat, how it specifically related to Australia and the Asia-Pacific and the measures the AFP were taking to address the threat. Mr Lewis asserted that the cybercrime threat in Australia had evolved and was ever-growing. With this in mind, he stated that the AFP had increased its commitment to the Australian Cyber Security Centre (ACSC) and was working with both high- and low-classified information. Describing the fight against cybercrime as a "team sport", he went on to state that the AFP's role was to operate under Commonwealth law, and as such it was able to apply relevant state and territory legislation. Mr Lewis summarised by stating that the Queensland Government itself had been the target of significant threats, including attacks such as bomb threats on schools. There were also cases where government departments had been hacked and ransoms demanded. This reinforced the notion that cyber-related threats were very real and closer than perceived by most people.

Cyber Threats Part 2: Online Threats Against Children

This session looked at the international and national threats facing children and what steps had been taken in the areas of law enforcement and education to mitigate these risks.

Hon Niroshan Perera MP, State Minister of National Policies and Economic Affairs for Sri Lanka, opened the session by providing some insight into his exposure to the issue in his home country. He stated that whilst Sri Lanka is a developing country, it is also a rapidly expanding one and therefore faces new challenges with the increasing amount of citizens - including children - gaining access to the internet via home computers, mobile phones and internet cafes.

UNICEF's Afrooz Kaviani Johnson, working for the organisation's East Asia and Pacific Regional Office as a child protection consultant, stated that every parliamentarian present needed to play a vital role in helping to prevent the exploitation of children online. She said that whilst the internet provided unprecedented opportunities for children to learn, play and interact, it also had implications for children's safety with exposure to new forms of risk and harm via cyberspace and new forms of digital technology. Offenders would oftentarget countries with limited legal frameworks in place, where the ability to enforce them was low and the likelihood of identification was also low. She stated that, whilst it was important to protect children from online threats, this shouldn't be at the cost of undermining their ability or rights of access to and use of the internet; children should be empowered online. To finish, Ms Johnson emphasised that what was happening online to children was a reflection of society at large and of what they faced offline in their schools, homes and communities. Parliamentarians held the power that these children lacked, and as such, should grasp the opportunity to make a positive and lasting impact on children's lives and their communities.

The session concluded with a presentation from **Andree Wright, Acting Children e-Safety Commissioner from the Commonwealth of Australia**, who provided a comprehensive overview of Australia's leading national organisation for child safety. Ms Wright opened by saying that traditionally the area of crime relating to child sex offences had been dealt with differently. This presented challenges in addressing the shift in these crimes to the internet and technology. As a result, the Australian Government decided that they wanted a national hub for cybersecurity and the protection of children - a hub where people could go if a child was being cyber-bullied or exploited. For this reason, the Office of the Children's eSafety Commissioner (OCEC) was created. Since the organisation was created in July 2015, it had completed more than 11,000 investigations. Many of these cases were related to child pornography; the most shocking fact being that 92% of images involved children who were primary school aged children or younger (5 – 12 years old) and 6% were under the age of 5. As one of its outputs, the OCEC set up an "In Hope Hotline"[2],a hotline used by more than 50 countries to report inappropriate content and have it removed from the internet. Closing her presentation, Ms Wright referenced an old saying - "It takes a village to raise a child" - in emphasising OCEC's work on making the internet a safer place for Australian children.

[1] Symantec - 2016 Internet Security Threat Report, https://www.symantec.com/security-center/threat-report?inid=globalnav_scflyout_istr
[2] In Hope CyberReport Hotline, Australia, http://www.inhope.org/gns/our-members/australia.aspx

Cyber Threats Part 3: Cyberactivism

Should online political activism be viewed as a threat/attack? How should the Snowden effect or other online protests be tackled? How can security be balanced with freedom of speech, privacy and public protests? What is the Asia-Pacific context? This session, chaired by **Hon Matt Conlan MLA from the Australian State Legislature of the Northern Territories**, sought to answer these questions.

The first member of the panel was **Dr Monique Mann, a Lecturer at the School of Justice, Faculty of Law from Queensland University of Technology**, whose main areas of research were police technology and surveillance. She depicted an escalating technology arms race between government and activists; this cat and mouse game had been described as "crypto war". Describing the origins of cyber activism as lying in the activities of "cyber punks" in the 1980s, she explained that the creation of The Onion Router (TOR), proxy Virtual Private Networks (VPNs) and websites such as WikiLeaks were originally created to provide publically available encryption services centred on the right to privacy - but that from these largely benevolent reasons encryption had developed to present many nefarious implications. She mentioned that cyberactivists primarily protested against the perceived injustice of surveillance against the public - for example, organisations such as Anonymous launched attacks as a form of protest.

The second panellist was **Angela Daly, also Lecturer at the School of Justice, Faculty of Law from Queensland University of Technology**. She began by questioning the term "Cyberactivism", and disgreed that it was largely framed as a threat, when it largely concerned just online activism in political spheres. She explained that it could range from benign to illegal or questionable political activities online, and focused on the positive elements that cyberactivism could bring - such as promotion of human rights, privacy, freedom of expression and freedom of association. However, she clarified that it was important to note that these rights were not absolute and could be restricted in certain circumstances; part of cybersecurity should be part of securing these rights for our citizens. She argued that it was parliamentarians' duties to facilitate the ability to not be defrauded whilst also protecting the public's ability to interact in positive online political participation.

Day Two
Tuesday 26 July 2016

Session 4: Building an Open, Safe and Stable Cyberspace

The opening session of day two focused on the challenges facing the development of a safe and robust cyberspace. It focused on what had been achieved so far on international and regional levels; what the successes and failures were; the impact of issues on small states and how to ensure effective internet governance.

Dr Tobias Feakin, Director, National Security Programs, Head of International Cyber Policy Centre at the Australian Strategic Policy Institute, commenced the discussion by discussing the concept of cyber maturity and how it could be improved. He defined cyber maturity as pertaining to the governance, financial cybercrime enforcement, military application, digital economy and business, and social engagement of a given country. Describing the Asia-Pacific region as the focus of these strategic shifts, he stated that there was opportunity in the region - but not without its pitfalls. After describing each of these areas in more detail, he listed a number of international organisations that were leading the way in promoting regional cyber maturity, such as the Association of Southeast Asian Nations (ASEAN), the UN Group of Governmental Experts (UN GGE) and Interpol.

The second panellist, **Peter Cassidy, Secretary General of the Anti-Phishing Working Group**, discussed in detail the emergence of phishing attacks and the rationale needed for industry stakeholders to immediately react to attacks - particularly with regards to the security of financial institutions. He stated, in simple terms, that industry needed to collectively respond to attacks

- and that it had been already forced to do so, as law enforcement simply hadn't had the resources needed to respond to threats effectively. Making it less lucrative and more difficult for aggressors to target institutions would be more effective, as they would eventually be dissuaded from attempting attacks in the first place. He likened predicting cyber attacks as something akin to predicting the weather, and success in mitigating these issues must be achieved through an automated process through machines programmed to recognise and fight such attacks proactively. Finally, he stressed the need for the public to be part of the solution - they should be empowered to become more resilient actors ensuring they participate in their own safety. He used the example of cybersecurity awareness programs, such as Stop-Think-Connect[3].

Champika Wijayatunga, Regional Security, Stability, Stability and Resiliency (SSR) engagement Manager for the Asia Pacific Internet Corporation for Assigned Names and Numbers (ICANN), discussed the work of ICANN. Formed in 1988 as a non-profit body, ICANN's purpose was to keep the internet secure and stable. He described it as an organisation that worked through a multi-state model, with many actors working together. He listed the maintenance of DNS (Domain Name System), IP Addresses as functions that ICANN coordinated, mentioning that these could be attacked through the hijacking of IP addresses and domain names; therefore the key thing would be to keep these identifiers safe and secure. The key take away, he said, was that developing threat awareness, threat response and trust-based collaboration would be important in maintaining internet security.

Session 5: Conflicts in Cyberspace

Session 5 focused on the concept of cyber-warfare and its characteristics. Its aim was to provide examples of attacks and threats, both real and perceived; the "Asia-Pacific context"; and the role of parliamentarians - as well as civil, military and private stakeholders - in this field.

Hon. Mahmud–Us-Samud Chowdhury MP, Member of the Parliamentary Standing Committee on the Ministry of Defence, Bangladesh, chaired the session, but also gave a brief rundown of the critical nature of IT infrastructure in national parliaments. Using his native Bangladesh as an example, he stressed the importance of keeping relevant software and hardware updated to minimise security risks. The Commonwealth, he argued, should become even stronger in the face of such pressing global issues.

[3] https://www.stopthinkconnect.org/

Hon. Maiza Hameed MNA, Pakistan questions members of the panel

The first speaker, **Mari Kert-Saint Aubyn, Senior Analyst for the Law and Policy Branch of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE)**, gave a presentation with the objective of providing an overview of what NATO CCDCOE did with regards to international law creation. One of 18 sectors of excellence providing policy advice to the North Atlantic Treaty Organisation (NATO), the CCDCOE's mission was to enhance the organisation's cyber defence and security capabilities. Amongst other resources, this included the newly updated Tallinn Manual 2.0[4] which gave an overview of the legal frameworks for cyber operations; explored the possibility of total "Cyber War" using case studies (including past conflicts in Georgia and Ukraine); and defined what a "cyber attack" actually is. She claimed that the most pressing issue for nations was to state clearly what their own positions on cyber-related international law were - otherwise there would be the risk of several, conflicting interpretations.

The latter half of the session was led by **Dr Ewan Ward, Director of CERT (Computer Emergency Response Team) Australia** - Australia's national computer response team. He provided deep insight into the kinds of risk governments and organisations were exposed to, and how they could manage these potential threats. In particular, he underlined the importance of instilling a cybersecurity culture in the workplace, and reiterated the need for individuals and organisations to be more involved in the security of their cyber communities.

Session 6: National Cybersecurity Strategies

This session focused on the importance of countries creating their own national cybersecurity strategies. **Hon. Dr Derek Sikua MP, Leader of the Independent Group Solomon Islands**, chaired the session and commenced the discussion by raising the following questions: Why is it important to create a consolidated national strategy for cybersecurity? What constitutes a good cyber strategy? What will we need to do to ensure national buy-in to the process?

Mari Kert-Saint Aubyn returned to discuss the work that NATO CCDCOE had done in the area of researching effective models and frameworks for successful national cybersecurity strategies - particularly its National Cybersecurity Framework Manual. She underlined the critical nature of cooperation between state and non-state actors, such as academia, ICT providers and private companies. Using her native Estonia as an example (indeed the first country to ever develop a national strategy), she described how 99% of businesses used the internet and 21% of enterprise turnover came from e-Commerce. She also insisted that strategies must be country-specific; of the 17 Asia-Pacific nations that created their own cybersecurity strategies, four of them developed more detailed and tailored second generation strategies that differed vastly from the original iterations. Australia was a good example of this.

[4] NATO CCDCOE - Tallinn Manual, https://ccdcoe.org/tallinn-manual.html

Hon. Aumua Lameko MP addresses delegates on the situation in Samoa

Sandra Ragg, Assistant Secretary for Cyber Policy at the Office of the Cyber Security Special Adviser, Department of the Prime Minister and Cabinet, Commonwealth of Australia, outlined how the Australian Government developed its new cybersecurity strategy[5], which was announced in April 2016. She noted how cyber policy had recently been moved to fall under the remit of the Office of the Prime Minister, in recognition of the centrality of the issue, but also stressed the importance of consulting and collaborating with the private and public sectors. It was important to do this in order to gain an appropriate context of what the country needed and this became reflected in the strategy itself, which developed from one based solely around threat to one that included opportunity – advancing and protecting national interests online whilst preparing jobs for the future. Further key points that she raised included a greater need for information sharing between the government and private sectors; developing industry lead guidance on best practice for cybersecurity to help SME's and the need to be "cyber smart" in working with the education sector to promote careers and skills regarding cybersecurity.

Session 7: Legislating for Cybercrime

The afternoon's session focused on the issue of developing robust yet fair legislation to tackle cybercrime and to promote good cyber hygiene.

Shabhana Mahmood MP, UK Parliament, chairing the session, highlighted her work on the UK's Draft Investigatory Powers Bill Joint Committee and the need for balancing security and privacy concerns. She described the constant challenge of creating a robust but transparent piece of cyber legislation, coupled with significant public resistance to the idea of police and government surveillance. She believed that the key take away from the UK's experience was that there was a need for a consolidated piece of legislation.

Alison Evans, Legislation Practice Lead, Senscia (representing the Commonwealth Cybercrime Initiative), provided insights on the process of drafting legislation and gave tips for parliamentarians who were involved in the construction of cyber law, with advice ranging from the strategy stage to the drafting stage. Whilst commenting on the usefulness of the Budapest Convention[6], she noted that the Commonwealth Model of Law could be a more viable form of law for Commonwealth countries to consider as a framework for their own cybersecurity strategies. Discussing the process of turning strategies into law, she stated that policy makers needed to first consider three questions: What is the policy that the legislation is trying to implement? Is a law even necessary to achieve it? Does the statement of policy work as a policy provision? Finally, she stated that a good law needed to follow the "Four Cs" - namely that it needed to be complete, contemporary, congruous and communicative.

Rounding off the session was **'Aminiasi Kefu, Acting Attorney General and Director of Public Prosecutions, Tonga**, who spoke specifically about cybercrime in Tonga and the Pacific and how his office dealt with cybercrime and cybersecurity. He stressed that there were no Pacific-specific issues in particular, as technological developments meant that even the smallest of island nations faced similar issues to larger countries, using the same computers, mobile phones, apps and software. He noted the need for political buy-in to give a priority to cybercrime, and also spoke of the importance of legislators having a good understanding of cybercrime law.

Day Three
Wednesday 26 July 2016

Session 9: Strengthening International and Regional Partnerships

Day three commenced with discussions on the role of international and regional partnerships in securing a safe and prosperous cyberspace. Transnational organisations, neighbouring countries and multinational corporations were all mentioned as key stakeholders in this field.

[5] Australian Cybersecurity Strategy 2016, https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf
[6] Budapest Convention, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

Hon Tutai Tura MP, Associate Minister of Foreign Affairs from the Cook Islands, chaired the session but also opened the discussion by stating that attempting to address cybersecurity and at the levels required of governments invariably brought its own challenges to the floor. Given its complex nature, he argued that this was an issue that could only be tackled through international cooperation.

Peter Cassidy from the Anti-Phishing Working Group returned to reemphasise that, in the outbreak of phishing and cybercrime, it had become clear that the problem was unique and existing institutions could not do much to respond. He said that partnerships only worked when a precise definition of the role of the various partners was specified, but that this would only happen if there was a precise definition of what cybercrime actually was. Once this had been clarified, it would pave the way for more partnerships, which needed to be formed of states, private corporations such as PayPal, and the public sector.

He was followed by **Dr Tim Legrand, Lecturer at the National Security College at the Australian National University**, whose work was focused primarily on public policy, cybercrime and cyber terrorism. His main question was this - how do we determine best practice between cybercrime and cyber terrorism? He responded by saying that security wasn't going to be achieved through legislation alone, but rather through the combined implementation of programmes by collaboration among related stakeholders. Also noting the transnational nature of cybercrime, he again emphasised that collective security was preferable to siloed, purely national approaches.

Session 10: Building Partnerships with the Private Sector

This session focused specifically on partnerships with the private sector and was chaired by **Hon. Aumuia Lameko MP from Samoa**. He mentioned that cyberattacks were not a new phenomena in Samoa and that only through close cooperation with the private sector would legislatures have the skills and capacity to deal with these threats effectively.

David Masters, Corporate Affairs Manager at Microsoft Australia, who had extensive experience in both the public and private sector, said that he couldn't imagine a discussion about security without discussing cross-sector partnerships. He stated that information sharing across actors was vital yet difficult to implement and maintain correctly. Stakeholders needed to consider what the purpose of the exchange was and who all the actors that needed to be considered were. In particular, considerations needed to be made on what information should be held - especially within the government. Giving an example of how arrangements could be structured, he described one of Microsoft's partnership initiatives, the Microsoft Protection Program, where the company detected vulnerability in its own systems and shared this information with its trusted partners. Microsoft would release this information particularly to antiviral or defence systems so they could patch and protect these prior to the public release of information. In order to make such partnerships work, they needed to be build on trust - something primarily engendered by openness and transparency.

Bevan Jones, Head of National Security/ Government, BAESystems spoke about international services and solutions threat defence for the 21st century. Having worked as a technical engineer on the national broadband network and in cyber defence, he stated that there are only two types of people in the world – those who have been hacked, and those who don't yet know that they have. Reiterating the need for cross-sector partnerships, he offered an overview of the role that the private sector can play, such as delivering training and capability solutions for legislators; this emphasised the importance of being visible to the public, being part of a community and ensuring that different sectors work together. He reiterated that the ramifications of not investing the right time and money would be severe.

Chris Noble from Deloitte finished the session by speaking of the importance of preparedness. He likened the fallout of a cyber attack to the impact that an iceberg could have on an incoming ship. There are obvious costs associated with a cyberattack to both public and private organisations: a loss of clientele, loss of brand image, legal costs, loss of trust, higher insurance premiums. But there are further potential ramifications in that an attack's impact could play out over years with a loss of faith and trust in a company's partner organisations. Consequently, he stated the importance of having the relevant action plans and staff awareness in place. Alongside preparedness, he said, there should also be continuous monitoring and increased vigilance, including the development of early warning systems.

Session 11: Advocacy And Education Increasing Public Awareness

The morning concluded with a wide-ranging discussion, chaired by Malaysia's **Hon. Datuk Wira Haji Ahmad Hamzah MP**, on the role that legislators can play in advocacy and education, to improve and increase the public's awareness of cybercrime.

The first panellist was **David Irvine AO, Chair of the Australia Cyber Security Institute** and the former Director-General of Australia's Secret Intelligence Service. He stated that there are two things that parliamentarians need to keep in mind about cybersecurity - that they need to know what they are talking about, so that they can communicate to the public; and that they should avoid being captured or overwhelmed by the noise of certain interest groups. He also warned against over-legislating, or legislating simply to appease a particular lobby. Ultimately, parliamentarians shouldn't leave the public with just "doom and gloom" scenarios; they as individuals can increase cybersecurity and as such parliamentarians should seek to engage them with the government.

A very moving presentation came from **Dr Cassandra Cross, from the School of Justice at Queensland University of Technology**, who focused on the perspective of victims of cybercrime. Her view was that, in understanding how people were affected by such attacks, parliamentarians could develope a more nuanced approach to policy making and implementing legislation. She made the point that cybercrime was about more than just money, reminding delegates of the impact it had on victims' lives, including mental health, arguing that victims often suffer shame and stigma. She said that people often underestimated the skill of cybercriminals and warned that it was difficult to educate people who didn't think that they are vulnerable to cybercrime. As such, she encouraged delegates to present messages to the public that were authentic and impactful, in the hope that an informed society would approach the concept of cyber threats from a more understanding angle, and also be able to better prepare themselves.

Delegates examine a case study in their breakout groups.

Peter Cassidy contributed to the workshop once more, this time to talk specifically about his "Stop. Think. Connect" awareness campaign on promoting clear messages about online safety and the nature of cybercrime itself. The campaign had already been implemented in three Commonwealth countries - Bangladesh, Jamaica and Nigeria. He criticised the fact that the current state of online safety messaging was fragmented and uncoordinated. He promoted the need for practical and contemporary safety and security messaging, available in many languages and easily modifiable for a particular cultural context.

Session 12: Leadership - Securing Parliaments

The final session of the day focused on the security of parliamentary ICT networks, and the ability of parliaments – and parliamentarians – to withstand cyber attacks.

Chaired by the **Speaker of the Parliament of Tuvalu Hon. Otinielu Tausi MP**, the keynote panellist was **Ian McKenzie, Assistant Secretary of the ICT Infrastructure & Services Branch at the Parliament of Australia**. He started the session off by describing the kinds of threats that parliaments and parliamentarians face: hacktivist infiltrations; cybercrime (conducted for monetary gain); cyber espionage (conducted usually for political gain); cyber-attacks (including leaking sensitive information into the public domain); and full scale cyber warfare.

Mr McKenzie gave an overview of the types of scenarios, ranging from an attack by a bedroom-based cyber attacker, right through to full-scale cyber warfare. Some of the particular threats he highlighted included phishing, macros, USB keys, network scanning and malware on mobile devices.

He also made the key point that hackers generally target people rather than computers, and therefore it is vital for parliamentarians and their staff to be fully educated and engaged in the cybersecurity process, and not just the IT department.

Day Four
Thursday 28 July 2016

Select Committee Hearing

The day began with one of the highlights of the workshop, a Select Committee exercise, giving delegates the opportunity to put into practice some of the themes they had discussed during the week.

The session, chaired by the UK's **Rt Hon. George Howarth MP** allowed for the exploration of scrutiny techniques using a case study from a fictional country in the Asia-Pacific region. Delegates questioned two witnesses – **the Head of Security and Operational Governance at the National Australia Bank, Nicholas Scott**, and legislative drafter **Alison Evans from Senscia** – on their work related to cybersecurity and cybercrime.

Participating delegates were divided along government and opposition lines, and all Members asked pertinent and probing questions to try and ascertain useful information.

Following the committee hearing, Members debated a recommendation.

A feedback session then allowed delegates to discuss learning outcomes, including the need for good background information, and the importance of tough questions, particularly from opposition Members.

Session 13: Scrutinising Security

The morning concluded with a session on the role of scrutiny, chaired by the Deputy Speaker of the Legislative Assembly of Queensland, **Hon. Di Farmer MP**, who noted that the workshop provided an ideal forum to share ideas, as different parliaments have different methods of scrutiny.

The first speaker, **Hon. Dr Shane Reti QSM MP** from New Zealand gave a highly engaging presentation of how important it was for parliaments to ensure scrutiny, given the ease by which hackers can operate. He gave some practical examples – using fellow delegates – to show how easy it is for scams such as phishing to occur.

He was followed by the **Rt Hon. George Howarth MP** who gave an interesting overview of his longstanding membership of the UK's Intelligence and Security Committee. He pointed out the importance of working cross-party, noting that every report that the committee has produced has been agreed unanimously, without the need for a vote.

Mr Howarth concluded with the comment that, in a democracy, it is not only possible but essential that parliamentarians have oversight and scrutiny of the work of security agencies.

Break-out Sessions: Part 3

To look further at the role of oversight and scrutiny, delegates took part in another group breakout session to look closely at a cyber-related case study.

World Café on e-Handbook

At the end of the workshop, delegates participated in a "World Café" session to discuss learning outcomes. These will provide an invaluable resource for the e-handbook to be produced as part of the project.

To formally close the workshop, we were delighted to welcome **Hon. Derek Sikua MP from the Solomon Islands**, who paid tribute to all those who had participated in the workshop.

The workshop committee hearing in the Queensland Legislative Assembly

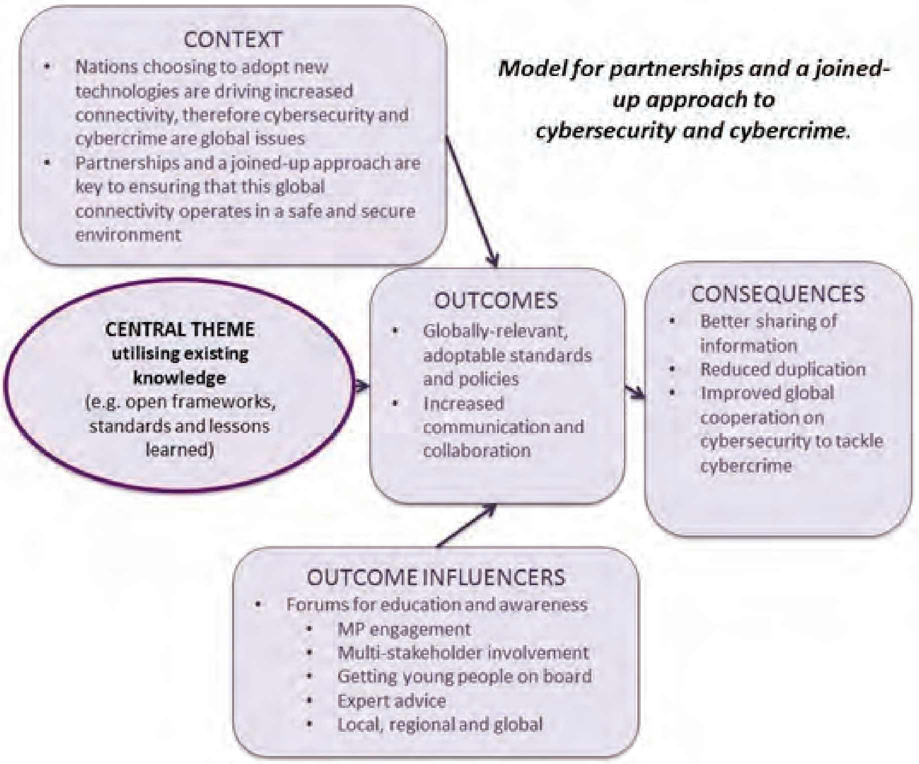
Networking Lunch - Key Outputs

On Wednesday 27 July a networking lunch was held in the Premier's and Speaker's Hall of the Queensland Parliament with the support of UKTI. It was an opportunity for delegates to network with a range of representatives from the private sector and academia to examine mechanisms for joint working across the cybersecurity sector.

Key themes that emerged from the discussion at the networking lunch included the importance of partnerships, as well as ensuring a joined-up approach to cybersecurity and cybercrime. Participants recognised the fact that technological advancement drives increasing interconnectedness, which therefore makes cybersecurity a truly global issue. The need for a global response to the challenges of cybersecurity was underlined, with a particular focus on information sharing. The importance of developing regional and international partnerships with industry and other nations was also highlighted.

Participants highlighted that a "huge range of knowledge" in relation to cybersecurity already exists, including through open frameworks, standards and lessons learned. Many discussions therefore revolved around the central theme of leveraging and reusing the knowledge that already exists.

It was established that an outcome of leveraging and reusing this existing bank of knowledge would be the possibility of influencing forums for education and awareness. These would lead to increased communication and collaboration, as well



Model for partnerships and a joined-up approach to cybersecurity and cybercrime.

CONTEXT
- Nations choosing to adopt new technologies are driving increased connectivity, therefore cybersecurity and cybercrime are global issues
- Partnerships and a joined-up approach are key to ensuring that this global connectivity operates in a safe and secure environment

CENTRAL THEME
utilising existing knowledge
(e.g. open frameworks, standards and lessons learned)

OUTCOMES
- Globally-relevant, adoptable standards and policies
- Increased communication and collaboration

CONSEQUENCES
- Better sharing of information
- Reduced duplication
- Improved global cooperation on cybersecurity to tackle cybercrime

OUTCOME INFLUENCERS
- Forums for education and awareness
  - MP engagement
  - Multi-stakeholder involvement
  - Getting young people on board
  - Expert advice
  - Local, regional and global

as ensure globally-relevant standards and policies. These outcomes in turn should result in enhanced information-sharing, a reduction of duplication, and improved global cooperation on cybersecurity to tackle cybercrime.

Other emergent themes were:

- **Encouraging information sharing between parliaments and governments internationally – for example sharing legislative frameworks, good practice, standards and benchmarks**
  1. Identify existing networks and key players to make the best use of what is available
  2. Consider the need for cross-jurisdictional bodies to maintain dialogue and/or information sharing
  3. Challenges exist around making sharing secure and allocating time and resources to facilitate sharing

- **Building partnerships between parliaments, governments, industry, academia and civil society**
  1. Aim for continuity of people and actors involved in partnerships and forums to build strong links and informed communities
  2. Partnerships with industry are key – governments should focus on outreach to industry and involve them in legislative and/or other consultations
  3. Encourage collaboration and partnerships across Asia and the Pacific
     - A "Pacific forum" could be particularly relevant, with Pacific island nations sharing very similar challenges in acting individually as small states
  4. Collective development of benchmark standards and frameworks – legislatures are more likely to implement something if they've contributed to it

- **Awareness raising at national or constituency level, for example with national campaigns, community forums and local or national 'champions' to lead and raise awareness**
  1. Social media was regarded as a particularly cost-effective method for engagement with a wide reach and impact

- **Youth engagement, particularly in improving partnerships and outreach work with schools and universities**
  1. Investment in schools
     - Cybersecurity made part of the curriculum – children can then educate parents and families
     - "Hackathons" in schools – interactive learning
  2. Technology seen as a key area of growth, with job opportunities for young people. This should be linked to an increased focus on teaching relevant technical skills

- **The role of Parliaments in promoting cybersecurity to the national agenda**
  1. Select committee inquiries, research, reports and recommendations – improving the quality of debate and legislation on cybersecurity
  2. Parliaments could advocate for the role of Government Chief Information Officer
  3. Parliamentary interest groups to foster cooperation, sharing and networks
  4. Challenges identified in parliaments being able to keep up with technological innovation

Final Programme

Day 1 - Monday 25 July 2016

Setting the scene: An introduction to threats in Cyberspace

Undumbi Room, level 5 of the Parliamentary Annexe, Parliament of Queensland

TIME	SESSION
11:15 - 11:45	*Participant Registration*
12:00 - 13:00	*Networking Lunch - Premier's / Speaker's Hall, Parliament of Queensland*
13:00 - 13:30	**Welcome, About the Project & Housekeeping** What is the Commonwealth Parliamentary Cybersecurity and Cybercrime Project? Explanation of the programme and role of participants. What are the aim, objectives and outcomes? Chair: Rt Hon. George Howarth MP, *UK Parliament* Facilitator: Matthew Salik, *Deputy Head of Conferences & Projects, CPA UK*
13:30 - 14:30	**Official Opening - Introduction to Cybersecurity & Cybercrime** What is cybersecurity and cybercrime and where does it sit within the conventional security discourse? Who are the key actors? What steps have been taken to combat actual and perceived threats? How does cybersecurity relate to the developed and less developed world, what different approaches are needed? What is the role of parliamentarians in implementing, scrutinising and promoting the cybersecurity agenda? *Video Messages from the OAS and Commonwealth Secretary-Generals* Chair: Rt Hon. George Howarth MP, *UK Parliament* Speaker: Hon. Peter Wellington MP, *Speaker of the Legislative Assembly, Parliament of Queensland*
14:30 - 15:15	**Cyber Threats Part 1: Cybercrime** What criminal activities occur in cyberspace (fraud, Dark Web, piracy, crypto currencies, ransomware, corporate espionage and paedophilia) and how can they be tackled? What are the international, regional and national challenges and how can parliamentarians fight cybercrime? How can technical, legal and network complexities be overcome? What is the Asia-Pacific context? Chair: Hon. Tim Mander MP, *Shadow Minister for Police, Fire and Emergency Services and Shadow Minister for Corrective Services, Queensland, Australia* Speaker: D. Supt Glyn Lewis, *National Coordinator, Cyber Crime Operations, Australia Federal Police* Speaker: Brian Fletcher, *Director, Government Affairs Australia-Pacific, Japan and Korea, Symantec*

TIME	SESSION
15:15 - 15:30	*Tea/Coffee - 5th Floor Colonnade*
15:30 - 16:15	**Cyber Threats Part 2: Online Threats Against Children** Young people can be the most active online users and the most technologically astute, however they are frequently the group most at risk. Children are all too often at the mercy of cyber bullying, online predators, and inappropriate content. This session will look at the international and national threats facing children and what steps have been taken in the areas of law enforcement and education to mitigate these threats. Chair: Hon. Niroshan Perera MP, *State Minister of National Policies and Economic Affairs, Sri Lanka (tbc)* Speaker: Afrooz Kaviani Johnson, *Consultant - Child Protection, UNICEF East Asia and Pacific Regional Office* Speaker: Andree Wright, *A/c Children e-Safety Commissioner, Commonwealth of Australia*
16:15 - 17:00	**Cyber Threats Part 3: Cyberactivism** Should online political activism be viewed as a threat/attack? How should the Snowden effect or other online protests be tackled (Anonymous, hacktivism, freedom of information, etc)? How can security be balanced with freedom of speech, privacy and public protests? What is the Asia-Pacific context? Chair: Hon. Matt Conlan MLA, *Deputy Speaker of the Legislative Assembly, Northern Territories* Speaker: Dr Monique Mann, *Lecturer, School of Justice, Faculty of Law, Queensland University of Technology* Speaker: Dr Angela Daly, *Lecturer, School of Justice, Faculty of Law, Queensland University of Technology*
17:00 - 17:15	*Transfer to reception*
17:15 - 18:30	Welcome Reception hosted by the Deputy Speaker of the Legislative Assembly, Parliament of Queensland, Hon. Di Farmer MP *Stranger's Dining Room, Parliament of Queensland*

Day 2 - Tuesday 26 July 2016

Implementation & Legislation

Undumbi Room, level 5 of the Parliamentary Annexe, Parliament of Queensland

TIME	SESSION
09:00 - 10:00	**Session 4: Building an Open, Safe and Stable Cyberspace** How can we build a safe cyberspace? What has been achieved so far at an international and regional level? What are the successes and failures? What infrastructure and capacity is needed? How to ensure internet governance is effective? How does this impact upon small states as opposed to large nations? Chair: Hon. Natasha Mclaren-Jones MLC, *Government Whip, New South Wales* Speaker: Dr Tobias Feakin, *Director, National Security Programmes, Head of International Cyber Policy Centre* Speaker: Peter Cassidy, *Secretary General, Anti-Phishing Working Group, USA* Speaker: Champika Wijayatunga, *Regional Security, Stability and Resiliency (SSR) Engagement Manager for the Asia Pacific, Internet Corporation for Assigned Names and Numbers (ICANN)*
10:00 - 11:00	**Session 5: Conflicts in Cyberspace** Does cyber warfare exist and if so, what are its characteristics? Example of attacks and threats both real and perceived (espionage, terrorism, sabotage, subversion, propaganda, etc) on an international, regional and national scale. How effective are these attacks in achieving military or political gain? What is the role of parliamentarians, civil, military or private stakeholders? What is the Asia-Pacific context? Chair: Hon. Mahmud-Us-Samad Chowdhury MP, *Member, Parliamentary Standing committee on Ministry of Defence, Bangladesh* Speaker: Dr Ewan Ward, *Director - Brisbane, CERT Australia,* Speaker: Mari Kert-Saint Aubyn, *Senior Analyst, Law and Policy Branch, NATO Cooperative Cyber Defence Centre, Tallinn, Estonia*
11:00 - 11:30	*Tea/Coffee - (Interviews)*
11:30 - 12:30	**Session 6: National Cybersecurity Strategies** Why is it important to create a consolidated national strategy/policy on cybersecurity? Where should it fit within a national security strategy? What constitutes a good strategy? What consultation and scrutiny should be in place and how to ensure national buy-in to the process? Chair: Hon. Dr Derek Sikua MP, *Leader of the Independent Group, Solomon Islands* Speaker: Sandra Ragg, *Assistant Secretary Cyber Policy, Office of the Cyber Security Special Adviser, Dept of the Prime Minister and Cabinet, Commonwealth of Australia* Speaker: Mari Kert-Saint Aubyn, *Senior Analyst, Law and Policy Branch, NATO Cooperative Cyber Defence Centre, Tallinn, Estonia*

TIME	SESSION
12:30 - 14:00	*Lunch - Premier's / Speaker's Hall, Parliament of Queensland* *Including brief 30 minute tour of the Parliament Building*
14:00 - 15:00	**Session 7: Legislating for Cybercrime** Once a strategy is in place how should parliaments go about creating a legal framework and regulation? What constitutes good cyber laws - both mitigating criminality and warfare? What opportunities exist to amend legislation? Examining model legislation and conventions e.g. Commonwealth Model Law on Cybercrime, Budapest Convention, etc. Chair & Speaker: Shabana Mahmood MP, *UK Parliament* Speaker: Alison Evans, *Legislation Practice Lead, Senscia (representing the Commonwealth Cybercrime Initiative)* Speaker: 'Aminiasi Kefu, *Acting Attorney General and Director of Public Prosecutions, Tonga*
15:00 - 15:45	**Breakout Exercise (3/4 Groups)** In split groups participants will undertake a table top exercise examining threats, cybersecurity strategies and legislation.
15:45 - 16:00	*Tea/Coffee - 5th Floor Colonnade (Interviews)*
16:00 - 16:30	**Breakout Exercise Continued (3/4 Groups)**
16:30 - 17:00	**Session 8: Committee Hearing - Briefing for Thursday** This session will outline the aim and objectives, themes, roles and structure of the Committee hearing session on Thursday morning. Facilitator: Pawel Jarzembowski, *CPA UK*
17:00	*Close (Interviews)*

Day 3 - Wednesday 27 July 2016

Representation, Partnerships and Engagement

Undumbi Room, level 5 of the Parliamentary Annexe, Parliament of Queensland

TIME	SESSION
09:00 - 10:00	**Session 9: Strengthening International and Regional Partnerships** From international and regional organisations to neighbouring countries and transnational corporations, the cybersecurity agenda is a global problem requiring global solutions. What role can parliamentarians play in strengthening international partnerships, initiatives, treaties, conventions to strengthen international security and cybercrime prevention? Utilisation of Virtual Networks to build and sustain contacts that could provide assistance, lessons learned, best fit practices, etc. Chair: Hon. Tutai Tura MP, *Associate Minister of Foreign Affairs, Cook Islands* Speaker: Peter Cassidy, *Secretary General, Anti-Phishing Working Group, USA* Speaker: Dr Tim Legrand, *National Security College, Australian National University*
10:00 - 11:00	**Session 10: Building Partnerships with the Private Sector** The private sector is at the forefront of technological development, so how can parliamentarians strengthen partnerships with the government, law enforcement and the wider public sector? How can parliamentarians ensure oversight of private security actors? What best practice and advice can the private sector offer to parliamentarians in building cybersecurity infrastructure and technical capacity? Chair: Hon. Aumua Lameko, *Member, Social Sector Committee, Samoa* Speaker: David Masters, *Corporate Affairs Manager, Microsoft Australia* Speaker: Bevan Jones, *Head of Government/National Security in Australia, BAE Systems* Speaker: Chris Noble, *Partner, Risk Advisory, National Forensic Practice, Deloitte*
11:00 - 11:30	*Tea/Coffee - (Interviews)*
11:30 - 12:30	**Session 11: Advocacy and Education – Increasing Public Awareness** Parliamentarians as representatives can be influential in raising awareness and increasing public education both at a national and local level. What steps and techniques should parliamentarians take in driving the agenda forward? Chair: Hon. DatukWira Haji Ahmad Hamzah MP, *Malaysia* Speaker: David Irvine AO, Chair, *Australia Cyber Security Research Institute* Speaker: Peter Cassidy, *Secretary General, Anti-Phishing Working Group, USA* Speaker: Dr Cassandra Cross, *Senior Lecturer, School of Justice, Faculty of Law, Queensland University of Technology*

TIME	SESSION
12:30 - 14:00	*Networking Lunch with External Stakeholders* Bringing together parliamentarians and representatives from Government, academia and the private sector to examine how to best encourage joint working across the cybersecurity sector. *Premier's / Speaker's Hall, Parliament of Queensland*
14:00 - 15:30	**Breakout Exercise (3/4 Groups)** In split groups participants will undertake a table top exercise examining education, advocacy and representation.
15:30 - 15:45	*Tea/Coffee - 5th Floor Colonnade (Interviews)*
15:45 - 16:30	**Session 12: Leadership – Securing Parliaments** Parliaments are frequently at risk of cyber-attacks, as are parliamentarians individually. What risks exist and what are the dos and don'ts? What are the best parliamentary security procedures and robust data and file management? How can parliaments as institutions show leadership on cybersecurity? Chair: Hon. Otinielu T Tausi MP, *Speaker, Parliament of Tuvalu* Speaker: Ian McKenzie, *Assistant Secretary, ICT Infrastructure & Services Branch, Parliament of Australia*
16:30	*Close*

Day 4 - Thursday 28 July 2016

Scrutiny & Oversight

Undumbi Room, level 5 of the Parliamentary Annexe, Parliament of Queensland

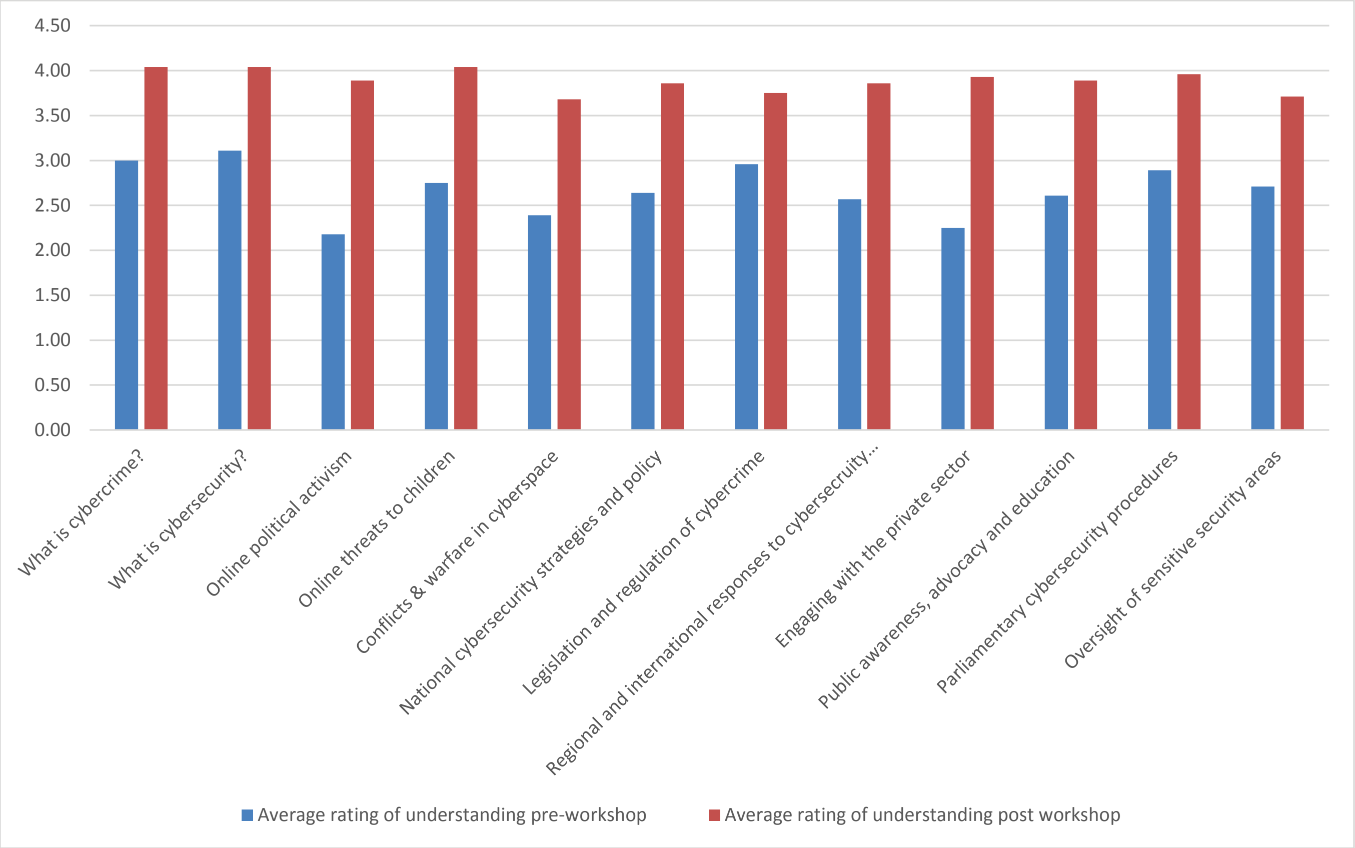
TIME	SESSION
09:00 - 10:15	**Select Committee Hearing** The purpose of this session is to explore scrutiny techniques using a real-life case study from the region. Delegates will act as committee members. They will question witnesses (agency/NGO/private sector) on their work related to cybersecurity and/or cybercrime. Participants will receive a briefing document on the topic to scrutinise during the committee hearing. The session will assist parliamentarians in how to ask open and probing questions and how to ascertain useful and relevant information. The session will conclude with a private sitting for participants to reach a conclusion. Chair: Rt Hon. George Howarth MP, *UK Parliament* Clerk: Pawel Jarzembowski, *CPA UK* Witness: Nicholas Scott, *Head of Security Operational Governance, National Australia Bank* Witness: Alison Evans, *Legislation Practice Lead, Senscia (representing the Commonwealth Cybercrime Initiative)* *Legislative Assembly Chamber, Parliament of Queensland*
10:15 - 10:30	*Tea/Coffee - (Interviews)*
10:30 - 11:15	**Select Committee Hearing – Feedback** This session follows on from the committee hearing. Participants will have the opportunity to share feedback and insights on the previous activity. Facilitator: Pawel Jarzembowski, *CPA UK*
11:15 - 12:30	**Session 13: Scrutinising Security** How can parliaments scrutinise areas that are frequently classified or, in the case of the private sector, commercially sensitive? What existing scrutiny and oversight mechanisms are in place and how effective are they on cybersecurity issues? How can parliaments ensure that strategies and laws can be implemented and enforced? Parliamentarians have a key role in scrutinising spending, so how can parliamentarians ensure adequate funding is in place? Chair: Hon. Di Farmer MP, *Deputy Speaker of the Legislative Assembly, Parliament of Queensland* Speaker: Hon. Dr Shane Reti QSM MP, *New Zealand Parliament* Speaker: Rt Hon. George Howarth MP, *Member of the Intelligence & Security Committee, United Kingdom*
12:30 - 13:30	*Lunch*

TIME	SESSION
13:30 - 14:30	Breakout Exercise (3/4 Groups) In split groups participants will undertake a table top exercise examinining policy oversight and scrutiny of cybersecurity and cybercrime.
14:30 - 15:00	*Tea/Coffee - 5th Floor Colonnade (Interviews)*
15:00 - 15:45	**World Café on e-Handbook** The purpose of this session is to give an opportunity for participants to brainstorm ideas for inclusion in the e-handbook. Through considering a set of questions, participants will identify how parliamentarians can implement and monitor cybersecurity and cybercrime at the national level. Facilitator: Helen Gardner, *CPA UK*
15:45 - 16:15	*Closing Speech & Vote of Thanks* *(feedback forms)*
16:30	*Close*

Monitoring & Evaluation

As part of the workshop's monitoring and evaluation process, delegates were asked to complete pre- and post-assessment forms to measure how effective the workshop had been in raising their level of understanding on cybersecurity and cybercrime topics.

The scoring methodology of the assessment forms is based on a scale of 1 to 5, with 1 signifying little understanding and 5 signifying good understanding. The graph below shows the average understanding of delegates substantially increased across the board as a result of the workshop.



Workshop Outputs

Delegate and Speaker Video Interviews

www.youtube.com/playlist?list=PLmDyxf_tGZUMkIQkNYXrW2Ukd25fFn-Fp

Workshop Photo Gallery

https://www.flickr.com/photos/cpa_uk

How do you intend to use the outcomes of the workshop?

"To lobby for legislation and a strategic framework around cybersecurity. To be more vigilant about loopholes related to cybercrime & cybersecurity when scrutinising government legislation and implementation of policy."

"Engage my Parliament on potential assistance, through a proposed twinning programme, for regional islands to improve their cybersecurity and build multi-national and regional partnerships."

"Make sure the message reaches the office of our leader and our Parliament. The issues must be addressed at the highest level; create a new ministerial portfolio to continue implementation of cybersecurity and cybercrime."

"Raise awareness with MPs, schools and the public; Initiate an awareness-raising programme/ campaign within my party and constituency."

"Share knowledge gained with parliamentary colleagues."

As submitted by delegates in their assessment forms.

Communications Impact

Twitter

Tweet impressions – 70,690
Tweeted – 133 times

The "Top Tweet" was a Tweet about Shabana Mahmood appearing on BBC West Midlands to discuss cybercrime, with 2,679 impressions and 76 direct engagements (Likes or RTs) (.@ShabanaMahmood talking to @bbcwm about how tackling cybercrime is the responsibility of all of us #cyberparl pic.twitter.com/2OtAw9qTnL)

MailChimp

CPA UK's daily briefings were opened by, on average, 56% of people they were sent to. Industry average is 23.7%.

- www.uk-cpa.org/news/cybercrime-asiapacific-regional-workshop--day-1-summary/
- www.uk-cpa.org/news/cybercrime-asiapacific-regional-workshop--day-2-summary/
- www.uk-cpa.org/news/cybercrime-asiapacific-regional-workshop--day-3-summary/
- www.uk-cpa.org/news/cybercrime-asiapacific-regional-workshop--day-4-summary/

Media Coverage

ABC – Shabana Mahmood live on The World to discuss cybercrime: www.abc.net.au/news/2016-07-27/balancing-privacy-rights-with-security-concerns/7663548

Fiji Times - www.fijitimes.com/story.aspx?id=363905 (Picked up from press release on Fiji Parliament website, which we provided to them)

PoliticsHome (in advance of workshop) - www.politicshome.com/news/uk/home-affairs/policing/opinion/house-commons/77000/david-hanson-mp-security-v-privacy-%E2%80%93

INTERNATIONAL PARLIAMENTARIANS' E-HANDBOOK ON CYBERSECURITY & CYBERCRIME

Commonwealth Parliamentary Association UK (CPA UK) in partnership with the Commonwealth Secretariat and the Organization of American States (OAS), with the support of international parliamentarians and experts, are in the process of designing an e-Handbook for parliamentarians on cybersecurity and cybercrime.

This e-Handbook will combine best practice, case studies, advice, ideas and innovation to assist international parliamentarians in legislating, scrutinising and advocating on cybersecurity and cybercrime.

This e-Handbook will be an essential tool to ensure parliamentarians can support the implementation, oversight, scrutiny and advocacy of cybersecurity.

www.uk-cpa.org/ehandbooks/ehandbook-on-cybersecurity-cybercrime/

Launched in March 2017

About Us

Commonwealth Parliamentary Association

Established in 1911, the Commonwealth Parliamentary Association is a Commonwealth-wide network of some 17000 national, state, provincial and territorial parliamentarians within 180 legislatures in 53 countries. The purpose of the CPA is to strengthen parliamentary democracy within the Commonwealth, providing space for parliamentarians to share, learn, compare and work together to promote Commonwealth values of democracy, the rule of law, human rights, good governance and social and economic development.

Commonwealth Parliamentary Association UK (CPA UK)

CPA UK is one of the largest and most active branches in the CPA community, and delivers a full programme of international parliamentary activities in Westminster and overseas. Governed by an Executive Committee of parliamentarians from all main parties, CPA UK's work includes parliamentary diplomacy and parliamentary strengthening on behalf of the UK Parliament and the wider CPA. Its activities include conferences, seminars, workshops and inter-parliamentary exchanges on parliamentary practice and procedure, policy and issues of international interest and concern.

Our Vision

CPA UK, a first-class organisation, will be a UK parliamentary strengthening partner of choice for the FCO and DfID, delivering high quality, innovative and effective capacity-building programmes that provide value for money

CPA UK, with its reputation of international trust, will be the parliamentary group to which most Westminster parliamentarians wish to contribute to deliver international parliamentary outreach

CPA UK will be a key contributor across an expanding Commonwealth and elsewhere internationally to parliamentary development with a particular reference to parliamentary practice, procedure and the role of parliamentarians in contextualising and implementing policies which contribute to good governance.

Our Mission

CPA UK's mission is to strengthen parliamentary democracy.

Our Work

CPA UK has established a reputation for the design and delivery of high level international parliamentary projects and conferences for parliamentarians, experts, academics and NGOs on a range of development topics. In the last six years CPA UK has run conferences on Sustainability, Energy & Development (2015/6), Growth for Development (2014), the Post-2015 Development Agenda (2013), Gender and Politics (2012), the MDGs (2011), Climate Change (2010) and Peacebuilding: Tackling State Fragility (2010).

In terms of security policy, CPA UK has in the last two years worked bilaterally and multilaterally with the Parliaments of Pakistan, Ghana and Nigeria in addressing the role of parliamentarians in formulating a national security strategy and parliamentary scrutiny of defence and security respectively.

For more information, go to: www.uk-cpa.org

SAVE THE DATE

INTERNATIONAL PARLIAMENTARY CONFERENCE ON NATIONAL SECURITY

WESTMINSTER, LONDON
MONDAY 27 - THURSDAY 30 MARCH 2017

FOLLOWED BY THE

CYBERSECURITY DAY

AS PART OF THE COMMONWEALTH PARLIAMENTARY CYBERSECURITY AND CYBERCRIME PROJECT

FRIDAY 31 MARCH 2017 WESTMINSTER, LONDON

Made possible with the financial contribution of the United Kingdom Foreign and Commonwealth Office

Foreign &
Commonwealth
Office

CONTACT US

Commonwealth Parliamentary Association UK
Westminster Hall | Houses of Parliament | London | SW1AA 0AA
T: +44 (0)207 219 5373
W: www.uk-cpa.org
E: cpauk@parliament.uk

Commonwealth Secretariat
Commonwealth Secretariat | Marlborough House | Pall Mall | London | SW1Y 5HX
T: +44 (0)207 747 6170
W: www.thecommonwealth.org
E: s.haruna@commonwealth.int

Organization of American States
Cyber Security Program - Inter-American Committee against Terrorism (CICTE) | Washington D.C.
T: +1 202 370 4674
W: www.oas.org/cyber
E: cybersecurity@oas.org

Organization of
American States
More rights for more people

QUEENSLAND PARLIAMENT

The Commonwealth

COMMONWEALTH PARLIAMENTARY ASSOCIATION UK