

Cyber Declaration

Third Pillar

- Promote stability in cyberspace through international cooperation

- ▶ Recognising the importance of international cooperation in tackling cybercrime and promoting stability in cyberspace, we:
 - ▶ Commit to the establishment of effective and proportionate domestic cybercrime and cybersecurity frameworks that take into account principles in existing international instruments, acknowledging the evolving tactics of cybercriminals and the transnational nature of cybercrime. Commit to use national contact points and other practical measures to enable cross-border access to digital evidence through mutually agreed channels to improve international cooperation to tackle cybercrime.
 - ▶ Commit to work towards common standards, harmonised legal approaches and improved interoperability, including through the use of Commonwealth model laws; and commit to considering the potential for further Commonwealth cooperation in this regard, including the possible coordination of common positions in international fora.

FCO Commonwealth Cyber Security Programme 2018-20

▶ VISION

- ▶ Greater collective cyber security across Commonwealth States with foundations built for effective national response capabilities that support economic, social development and rights online.

▶ OBJECTIVES

- ▶ Governments have increased political will to improve cyber security within the framework of Commonwealth values
- ▶ All DAC listed Commonwealth countries have completed or scheduled cyber capacity reviews.
- ▶ Governments have increased understanding of their needs and good practices they could apply to act on them
- ▶ More Commonwealth countries have cyber national strategies, legislation and CIIP plans • More Commonwealth countries build their capacity to tackle cyber crime in accordance with the Budapest Convention
- ▶ More cyber security cooperation within the Commonwealth and with other international actors
- ▶ More Commonwealth countries include private sector and civil society when developing and implementing cyber policy
- ▶ More opportunities for youth and women to access cyber security training and skills
- ▶ 95% of Commonwealth countries benefit from programme activity

Cyber Crime Projects

Commonwealth Secretariat

```
graph LR; A[Commonwealth Secretariat] --- B[Strengthening of international cooperation in cybercrime investigations]; A --- C[Cybercrime and Electronic Evidence Training for Investigators, Prosecutors and Judges in the Caribbean Region]; A --- D[Cyber resilience review and cybercrime legislative reforms in three pilot countries – The Gambia, Kenya and Namibia];
```

Strengthening of international cooperation in cybercrime investigations

Cybercrime and Electronic Evidence Training for Investigators, Prosecutors and Judges in the Caribbean Region

Cyber resilience review and cybercrime legislative reforms in three pilot countries – The Gambia, Kenya and Namibia

1. Strengthening of international cooperation in cybercrime investigations

- ▶ Strengthening of international cooperation in cybercrime investigations:
- ▶ This project has been developed to bring pan-Commonwealth cooperation in cybercrime investigations ensuring that electronic evidence is both requested and responded to in a timely and effective manner. The Secretariat will be:
 - ▶ Establishing clear focal points for electronic evidence in all Commonwealth Countries consulting existing networks such as the G7, Budapest Convention and UNODC
 - ▶ Run three regional workshops for the focal points to provide training on approached to requesting and receiving electronic evidence in cross border investigations
 - ▶ Develop a working group to examine legal requirements and challenges in obtaining electronic evidence in cross border investigations

2. Cybercrime and Electronic Evidence Training for Investigators, Prosecutors and Judges in the Caribbean Region

- ▶ The Commonwealth Secretariat will help the Caribbean Region deliver more efficient, effective and just prosecution of cybercrime cases.
- ▶ This will be done by strengthening the capacity of 12 investigators, 12 prosecutors and 12 judges from 12 Caribbean countries in order to be better equipped to respond to the threats from cybercrime.
- ▶ Key deliverable for the regional CARICOM IMPACS report.

3. Cyber resilience review and cybercrime legislative reforms in three pilot countries – The Gambia, Kenya and Namibia

- ▶ These three countries have been chosen principally as they are in need of cyber resilience review and drafting of their cybercrime legislation.
- ▶ The Secretariat will be reviewing the cyber capabilities and legislative responses in these three countries. Once this has been they will conduct a review of the legislative gaps.
- ▶ Revised legislation will then be submitted to project countries, containing modern and effective provisions criminalisation, procedural powers and international co-operation.