Empowering Commonwealth Countries to Safeguard their Citizens Online

Commonwealth Cyber Security Capacity Building: 2018 - 2022

GET SAFE ONLINE®

www.getsafeonline.org

Foreign, Commonwealth
& Development Office

Those countries that have the capacity and the expertise should be lending and sharing that expertise with others across the Commonwealth. "No one should be left behind" is a phrase we use often for different aspects. But when it comes to cyber, I think it's extremely important, not just in terms of the opportunities, but also the challenges and threats that we face on a daily basis.

Lord (Tariq) Ahmad of Wimbledon,
Minister of State for South Asia and the Commonwealth

Introduction

The internet is the single most transformative and enabling development in modern times, bringing significant economic, social and political benefits.

The internet and digital technologies are powerful catalysts for economic growth and development for all, and the impact of digital inclusion can be profound and wide-ranging. A recent example has been the exchange of medical knowledge, intelligence and technology during the COVID-19 pandemic.

The importance of being able to use the internet with safety and confidence

Legitimate users, however, are not the only ones to benefit from the ongoing increase in digital access, which is outpacing cyber security capability, creating fertile ground for malicious activity online which can be fraudulent, abusive, disruptive or extremist in nature. Threats as varied as abuse, ransomware and attacks on hospitals and critical national infrastructure are commonplace, and cybercrime and other online harms perpetrated in one country can affect users around the world.

Consider that around the 'physical world', every country has a police force … some have more than one. They enforce their countries' laws, maintain order and safety and prevent, detect, investigate and pursue criminal activities. In short, their job is to keep citizens, communities, businesses, infrastructures and governments safe and secure.

Internet users form the largest and most connected community on the planet. However, this community has no police force to enforce laws, maintain order and safety and prevent, detect, investigate and pursue criminal activities.

The Commonwealth Cyber and Tech Programme (and its predecessor, the Commonwealth Cyber Security Programme), facilitated a comprehensive spectrum of activity to better protect internet users.

The Commonwealth Cyber Declaration

Rewind to April 2018 and the Commonwealth Heads of Government Meeting (CHOGM 2018), which took place in London. The then Prime Minister of the United Kingdom, The Rt Hon Theresa May MP, called on Commonwealth leaders to take action and work collectively to tackle the ever-growing cybersecurity threat. This led to the signing of the Commonwealth Cyber Declaration, which sets out the commitments made by all 54 Heads of Government to support a cyberspace that promotes economic and social development, and rights online. These commitments aim to build the foundations of an effective national cybersecurity response and to promote stability in cyberspace through international cooperation.

In support of this groundbreaking initiative, the Prime Minister announced up to £15 million to help Commonwealth countries strengthen their cybersecurity capabilities and help tackle criminal groups and hostile state actors who pose a global threat to security, including in the UK. To date, in excess of this sum has been invested to support implementation of the Declaration. At CHOGM 2022 in Kigali, Rwanda (delayed for two years by restrictions imposed as a result of the COVID-19 pandemic), the Commonwealth has an opportunity to re-commit to the Declaration and continue driving its implementation.

Building capacity

The UK invested £5.5 million through its Commonwealth Cyber Security Programme – administered by the UK's Foreign, Commonwealth & Development Office (FCDO) – to work with low- and middle-income Commonwealth members to carry out national cyber security capacity reviews before the next CHOGM. The Programme funded projects across the Commonwealth to provide technical assistance, training and advice to address a wide range of cybersecurity and cybercrime threats. These include pan-Commonwealth, regional and national-level activities including: a community platform for Commonwealth Cyber Security Incident Response Teams (CSIRTs); provision of free cyber threat intelligence and detection to member countries in the Indo-Pacific and Africa; National Cyber Risk Assessment training in partnership with the UK Home Office; and working with the Commonwealth Secretariat to tackle cybercrime by improving sharing of electronic evidence between member countries.

As a result of these UK-supported activities, partner countries have been able to better protect their critical national infrastructure from cyberattacks; have stronger networks to exchange knowledge and expertise; and benefit from enhanced sharing of threat intelligence, an improved understanding of risks and a more informed and engaged civil society. During its extended term as Chair-in-Office, the UK has continued to support the implementation of the Commonwealth Cyber Declaration, including testing new and innovative projects.

Key achievements

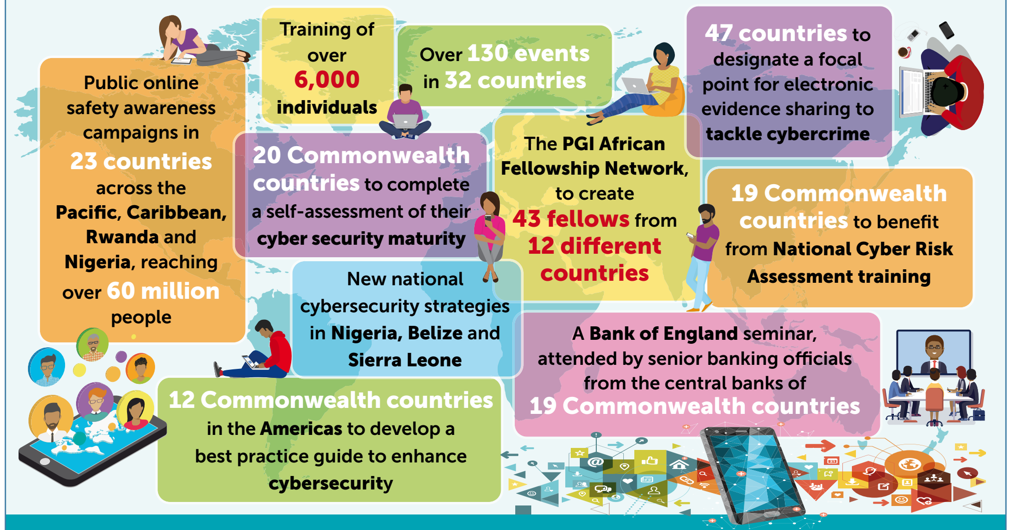
All Commonwealth countries benefitted from the UK's cyber security capacity building activities during the UK's Chair-in-Office. To date, over £15 million has been invested, over 130 events held in 32 countries and over 6000 people trained, all supporting implementation of the Commonwealth Cyber Declaration. Examples include:

- Over 60 million people in the Pacific, Caribbean, Rwanda and Nigeria have benefitted from public cyber hygiene training and are now better able to protect themselves from cyberattacks
- More Commonwealth countries understand their cybersecurity development priorities, including 20 completing a self-assessment of their cybersecurity maturity
- Countries have developed or refreshed their national cybersecurity strategies to better meet the needs of citizens, including Nigeria, Belize and Sierra Leone
- National incident response teams have been strengthened to detect and mitigate against cyberattacks
- 19 Commonwealth countries have benefitted from National Cyber Risk Assessment training
- 12 Commonwealth countries in the Americas have been assisted in developing a best practice guide to enhance cybersecurity
- 47 Commonwealth countries have now designated a focal point for electronic evidence sharing to tackle cybercrime
- 43 cybersecurity leadership Fellows from 12 African countries have been created
- Cross-border cooperation between Commonwealth countries on criminal investigations has improved

Commonwealth Cyber Security Capacity Building: 2018 - 2022

At CHOGM 2018, Government leaders signed **The Commonwealth Cyber Declaration** to support a cyberspace that promotes economic and social development, and rights online as well as building incident response capacity and promoting international stability through co-operation.

Through its **Commonwealth Cyber Capacity building projects**, the UK has supported the Declaration, by investing £15 million to make the internet safer across the Commonwealth to help maintain a cyberspace that is free, open, peaceful and secure. This has enabled:



Public online safety awareness campaigns in **23 countries** across the **Pacific, Caribbean, Rwanda** and **Nigeria**, reaching over **60 million** people

Training of over **6,000 individuals**

Over **130 events** in **32 countries**

47 countries to designate a focal point for electronic evidence sharing to **tackle cybercrime**

20 Commonwealth countries to complete a self-assessment of their **cyber security maturity**

The **PGI African Fellowship Network**, to create **43 fellows** from **12 different countries**

19 Commonwealth countries to benefit from **National Cyber Risk Assessment training**

New national cybersecurity strategies in **Nigeria, Belize** and **Sierra Leone**

A **Bank of England** seminar, attended by senior banking officials from the central banks of **19 Commonwealth countries**

12 Commonwealth countries in the **Americas** to develop a best practice guide to enhance **cybersecurity**

Since 2018, thanks to this investment, every Commonwealth member has taken steps to improve its cybersecurity competence and capability, and build capacity.

Foreign, Commonwealth
& Development Office

COMMONWEALTH
UNITED KINGDOM CHAIR-IN-OFFICE

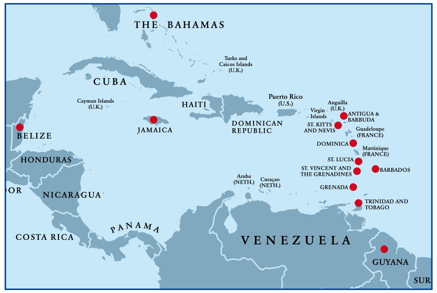
Through the Commonwealth Cyber Security Programme and its successor, the Commonwealth Cyber and Tech Programme, the FCDO has partnered with various implementers to deliver activities. The three case studies below illustrate the range of approaches taken through these programmes.

PREVENT: Improving Cyber Hygiene and Behaviours of Internet Users

The challenge

Cybercriminals, abusers and state-sponsored attackers alike continue to devise more advanced and ingenious ways to operate. There are technological solutions, but these can be successful only in combination with safe user behaviour – good 'cyber hygiene'. With 95% of cybersecurity issues traceable to human error [1], it follows that if human error is reduced, so accordingly is the level of risk.

The approach



As part of the Commonwealth Cyber Security Programme, the FCDO initiated a campaign of online safety awareness for individuals and small businesses in 12 Caribbean countries[2] in partnership with Get Safe Online, a UK-based not-for-profit organisation.

Get Safe Online worked with governmental, non-governmental and regulatory bodies and British High Commissions to determine the main existing and trending cyber vulnerabilities in the 12 countries and the most effective communications strategies to use.

Following this, it created a free to use, easy to navigate website for each country with over 200 pages of online safety advice which is both easy to understand and practical to implement. Get Safe Online worked with local partners to ensure the correct tone of voice, locally relevant look and feel (including imagery) and information – such as the most appropriate links for incident reporting. The partners also assisted in determining the most appropriate topics to highlight on the sites' home pages and in the awareness campaigns which were run with the assistance of a regional PR agency, using social, broadcast and other media and video production to cascade monthly topics. The Caribbean activity went live in April 2019.

In mid-2020, the successful formula was replicated in nine Pacific countries[3] as well as Rwanda.

All benefitted from similar awareness websites and programmes, but with two major additions made possible by increased funding and lessons learned from the Caribbean activity.

GET SAFE ONLINE
Ntibisaba ko winjirirwa n'abatekamutwe bya gihanga kugira ngo wibwe. Zirikana gusohoka (log off) muri porogaramu wakoreshaga cyangwa igikoresho cyawe cy'ikoranabuhanga, buri gihe umaze kohereza amafaranga.
Ku bindi bisobanuro, sura
www.getsafeonline.org.rw
FINANCIAL ONLINE SCAMS
SEIF REMITENS
GET SAFE ONLINE

Eight of the nine Pacific countries involved benefitted from websites, learning resources and media assets translated into indigenous languages alongside the English language versions, enabling further reach and penetration.

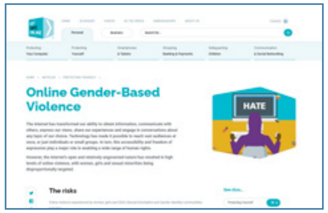
The other significant addition was the establishment of the Get Safe Online Ambassador Scheme established in mid-2020 and rolled out over the following six months to form a unique and highly successful network of local representatives equipped with the training, resources and confidence to go out into their communities – both face-to-face and virtually – to provide online safety advice to groups, schools, businesses and other beneficiaries. Ample and regular support for the Ambassadors is provided directly by Get Safe Online from the UK, which has itself leveraged digital transformation to effectively deliver training and resources online. This has been extended to both an application form for prospective Ambassadors and a request form for awareness sessions going online.

GET SAFE ONLINE | Ambassador Scheme

Naturally, there have been challenges.
The most prevalent have resulted from the COVID-19 pandemic, which at the time of writing is still having a major impact in some of the countries involved. The Ambassadors, and indeed the programme itself, have also continued to deliver in the face of geographical restraints, poor connectivity and natural disasters. Currently, 234 Ambassadors are active in 21 countries.

[1] World Economic Forum Global Risks Report 2022
[2] Antigua & Barbuda, Barbados, Bahamas, Belize, Dominica, Grenada, Guyana, Jamaica, St Kitts & Nevis, St Lucia, St Vincent and the Grenadines, Trinidad and Tobago
[3] Fiji, Kiribati, Nauru, Papua New Guinea, Samoa, Solomon Islands, Tonga, Tuvalu, Vanuatu

The campaign has also been ideally placed to provide guidance on local and regional issues such as online gender-based violence, remittance fraud and pyramid schemes, as well as an independent voice on COVID-19 vaccine misinformation, disinformation and fake news across all of the countries in which it runs.



Online Gender-Based Violence

The risks

The outcome

Over 50 local and regional partnerships were established across the Commonwealth. More than 3,000 social media posts were pushed out and the websites received a total of over 1.9 million visits. In surveys conducted over the period of the programme in the 22 countries involved, internet users said they practised digital hygiene habits 33% safer than they had prior to the inception of the programme. 89% of people who had visited a Get Safe Online website reported that they were better able to manage online risks. In all, 60 million internet users around the Commonwealth have been reached.

> *"Over the past few months, we have observed an increase in the number of discussions relating to online safety, this has been attributed to the content that was shared by your team and other efforts by the ministry. On behalf of our team, I would like to thank you immensely for affording us this opportunity."*

Public Sector Modernisation, Department of Public Service, Government of Saint Lucia

> *"Through this effort, we have been able to reach out to many communities including Central, Western and Northern Division to be able to provide tips and ideas to stay safe online.*
> *We have been able to have a greater reach which has brought about a better way to connect to people."*

Online Safety Commission, Fiji

> *"We are proud of the good work of Get Safe Online ambassadors here in Rwanda.*
> *The Get Safe Online Rwanda education infographics really are amazing."*

Ministry of ICT and Innovation, Rwanda

Commonwealth online safety awareness campaign

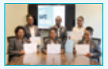
As part of this initiative, **Get Safe Online** has provided free, easily accessible online safety awareness campaigns for individuals and businesses in the Caribbean, Pacific and Rwanda with:

22 individual Get Safe Online websites, eight also translated into the indigenous language

Nobody wants malware, except cybercriminals. Get the full story from Get Safe Online.

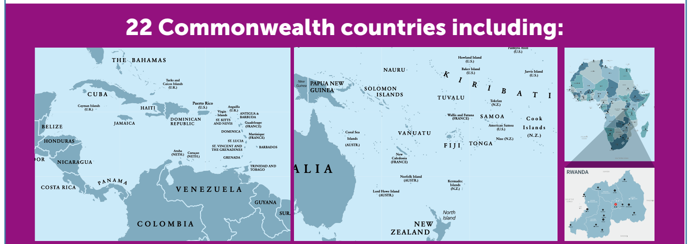
Local, engaging PR campaigns – from social media to TV and radio to billboards

Development of strategic partnerships with in-country government bodies and relevant associations



Implementation and operation of a **Get Safe Online Ambassador Scheme** to empower individuals to help spread online safety messages in their own countries

22 Commonwealth countries including:



Antigua & Barbuda, Barbados, Bahamas, Belize, Dominica, Fiji, Grenada, Guyana, Jamaica, Kiribati, Nauru, Papua New Guinea, Rwanda, Samoa, Solomon Islands, St Kitts & Nevis, St Lucia, St Vincent and the Grenadines, Tonga, Trinidad & Tobago, Tuvalu and Vanuatu

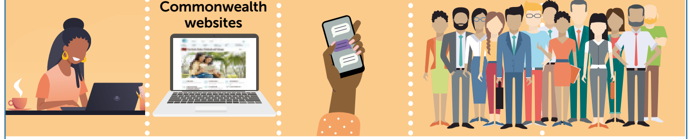
Over **60 million** individuals reached

Over **1.9 million** hits on the Get Safe Online Commonwealth websites

More than **3,000** social media posts

234 Get Safe Online Ambassadors

Over **50** partnerships



Improvement in users' digital hygiene habits:

An average improvement of 33% in digital hygiene habits

Managing online risks:

89% of people who had visited a Get Safe Online website reported they were more able to manage online risks.

Thanks to this investment from the UK's Foreign, Commonwealth & Development Office, individuals and small businesses in 22 countries across the Commonwealth have become safer online.

GET SAFE ONLINE

www.getsafeonline.org

Foreign, Commonwealth & Development Office

COMMONWEALTH UNITED KINGDOM CHAIR-IN-OFFICE

PREPARE:
Capacity Building – Responding to Incidents

The challenge

Every country with access to the internet needs to have strong cybersecurity to ensure users trust digital systems and services. Understanding the risks and being able to respond to them builds confidence within national and international communities, which is especially important for winning foreign investment and trade. At the beginning of 2018, a number of low-and middle-income countries in the Commonwealth had limited national cyber security incident response capability.

The approach

As part of the UK's commitment to maintaining a free, open, inclusive and secure cyber space, the FCDO partnered with the Singaporean Government and a commercial consortium, consisting of Torchlight Group as lead, Protection Group International and Venues & Events, to support governments in developing this important capability. By bringing people together and providing technical advice, the objective was to support public and private sector bodies in the participating Commonwealth countries develop and mature their own national cyber incident response capabilities.

Three regional events were held for African, Caribbean, and Asia Pacific Commonwealth countries, enabling locally tailored and open discussions on shared issues and experiences. Each event consisted of a three-day programme of workshops, forums and keynote speeches delivered by cybersecurity experts. National delegates received tailored support with countries of less mature incident response capability receiving guidance on how to establish these frameworks. States with mechanisms already in place received support on refining and improving them.

A final event brought groups together to discuss standards and best practices. Delegates from these countries also enjoyed continued access to subject matter experts through a dedicated advisory service which operated through to February 2020. The final workshop, hosted in London, was attended by representatives from 29 out of the original 40 participating Commonwealth countries. Three subsequent phases were implemented by Torchlight Group, focusing on incident response capacity development, information sharing and the building of a community of national Computer Security Incident Response Teams (nCSIRTs) across the Commonwealth.

Delivered entirely online under global pandemic conditions, a carefully designed schedule of events engaged public and private national, regional and international organisations to support the community. Activities covered the full range of nCSIRT services, addressing subjects including strategic planning, legal frameworks, cyber hygiene campaigns, equality, diversity & inclusion and tactical implementation. This series of webinars, seminars, mentoring and multi-national cyber exercises, backed by a secure online information exchange platform, provided multiple forums to share best practice, promulgate interoperable standards and assist Commonwealth countries in addressing the key issues in developing incident response capabilities.

The outcome

Each phase has built on the previous, with feedback from the community gathered and acted upon, increasing the level of engagement in the last phase of online events by 300%. Sustainability is a critical factor, and all learning materials are available to the community in a secure web-based platform on an ongoing basis.

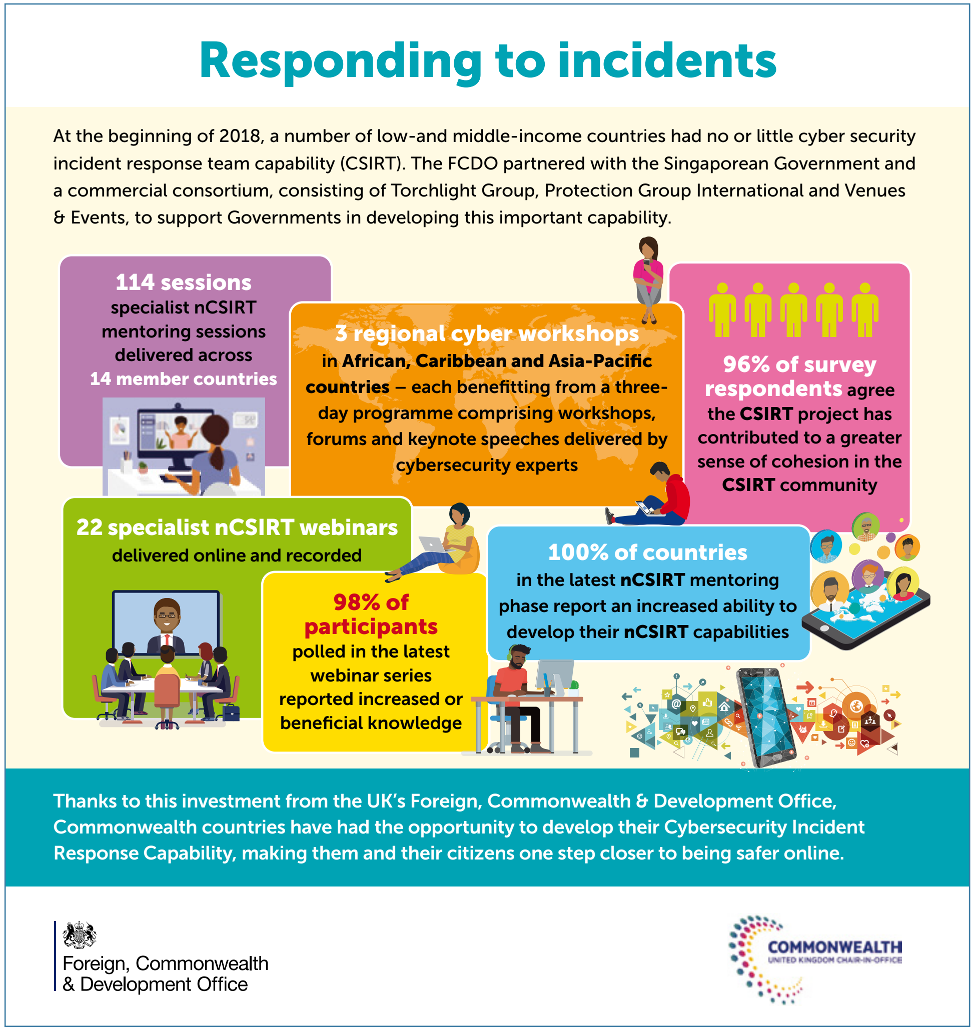
The community has also drawn on its own interest and inputs, with nCSIRTs across the whole range of maturities sharing their experiences in webinars and international development seminars alongside inputs from external, international and regional partners who all have a part to play in the community's collective journey to self-reliance.

114 specialist nCSIRT mentoring sessions have been delivered across 14 member countries, with three regional cyber workshops also taking place. 22 specialist nCSIRT webinars have been delivered online and recorded. Three multi-nCSIRT cyber exercises have also been completed. The latest phase has seen eight specific contributions on human rights and equality, diversity and inclusion.

98% of participants polled in the latest webinar series reported increased or beneficial knowledge. 96% of survey respondents agree the CSIRT project has contributed to a greater sense of cohesion in the CSIRT community and 100% of countries in the latest nCSIRT mentoring phase report an increased ability to develop their nCSIRT capabilities.

> *"The programme has helped with the strategic vision for the CSIRT, we have a clear understanding of where we want to go and have benefitted from an overview of the frameworks available to assist."*

> *"The mentoring has really improved our understanding of what needs to be done next within our environment. It has put everything into context, providing great knowledge and insight."*



Responding to incidents

At the beginning of 2018, a number of low-and middle-income countries had no or little cyber security incident response team capability (CSIRT). The FCDO partnered with the Singaporean Government and a commercial consortium, consisting of Torchlight Group, Protection Group International and Venues & Events, to support Governments in developing this important capability.

114 sessions specialist nCSIRT mentoring sessions delivered across **14 member countries**

3 regional cyber workshops in **African, Caribbean and Asia-Pacific countries** – each benefitting from a three-day programme comprising workshops, forums and keynote speeches delivered by cybersecurity experts

96% of survey respondents agree the **CSIRT** project has contributed to a greater sense of cohesion in the **CSIRT** community

22 specialist nCSIRT webinars delivered online and recorded

98% of participants polled in the latest webinar series reported increased or beneficial knowledge

100% of countries in the latest **nCSIRT** mentoring phase report an increased ability to develop their **nCSIRT** capabilities

Thanks to this investment from the UK's Foreign, Commonwealth & Development Office, Commonwealth countries have had the opportunity to develop their Cybersecurity Incident Response Capability, making them and their citizens one step closer to being safer online.

Foreign, Commonwealth
& Development Office

COMMONWEALTH
UNITED KINGDOM CHAIR-IN-OFFICE

PURSUE:
Enabling Effective Investigation and Prosecution of Cybercrime and Promoting International Cooperation

The challenge

In our technology-driven world in which the internet knows few borders, international cooperation in cybercrime investigations is critical. However, while an increasing number of Commonwealth countries have programmes and legislation in place to improve resilience and tackle cyber threats, a focus on prevention alone is unlikely to be effective. Alongside this, traditional methods of policing, gathering and interpreting evidence and prosecuting cases needed to evolve to ensure that cybercrimes can be dealt with effectively across entire criminal justice systems.

Against this background, the FCDO provided funding to the Commonwealth Secretariat's Cyber Crime Unit to implement projects aimed at tackling cybercrime and promoting international cooperation across the Commonwealth.

The approach

To promote better use of electronic evidence in cross-border criminal investigations, a series of workshops and exercises was held, looking at cybercrime as not simply a matter for law enforcement, but part of a shared challenge affecting different parts of the criminal justice system. The project brought stakeholders together from across the Commonwealth and provided an environment in which shared solutions to key issues could be developed. For example, law enforcement officials from areas such as the police, drug enforcement and anti-money-laundering were asked how they would go about collecting and analysing evidence that might be on a computer or mobile device, while prosecutors, magistrates and judges discussed the utility of different types of evidence.

Better cooperation in criminal investigations was also an ambition with the expansion of the Commonwealth Network of Contact Persons (CNCP) to improve electronic evidence sharing. Live role-playing scenarios were held at three regional events in Barbados, South Africa and Australia, to provide a forum for key contacts in Commonwealth countries to test their collaboration skills. A virtual exercise was also held to test those skills were embedded by the electronic evidence training.

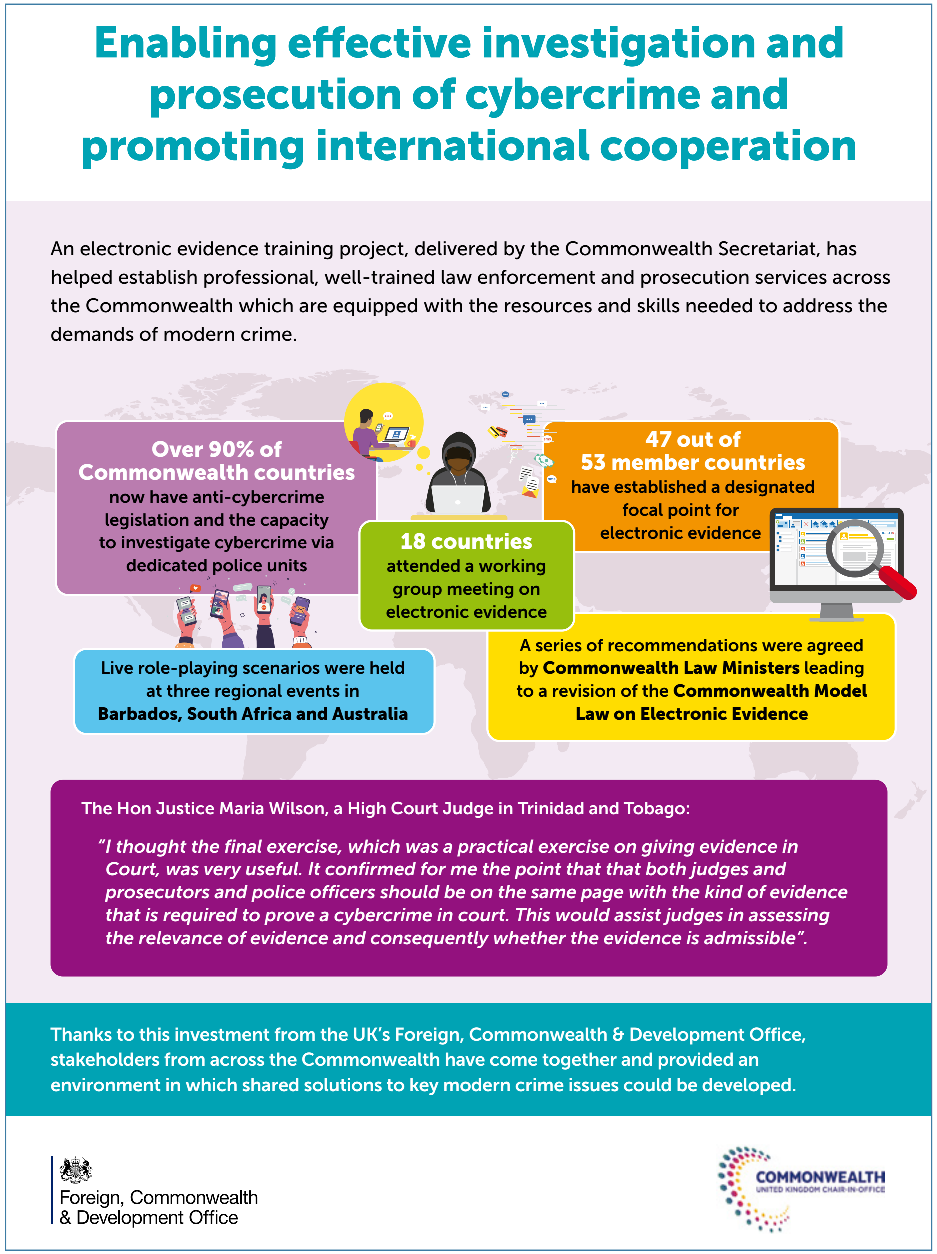
The outcome

The electronic evidence training project has helped establish professional, well-trained law enforcement and prosecution services across the Commonwealth, which are equipped with the resources and skills needed to address the demands of modern crime. The Hon Justice Maria Wilson, a High Court Judge in Trinidad and Tobago stated:

> *"I thought the final exercise, which was a practical exercise on giving evidence in Court, was very useful. It confirmed for me the point that that both judges and prosecutors and police officers should be on the same page with the kind of evidence that is required to prove a cybercrime in court. This would assist judges in assessing the relevance of evidence and consequently whether the evidence is admissible".*

Over 90% of Commonwealth countries now have anti-cybercrime legislation and the capacity to investigate cybercrime via dedicated police units. Most countries are working on developing strategic and implementation plans. The project has also led to the establishment of a designated focal point for electronic evidence for 47 out of 53 member countries.

18 countries attended a working group meeting on electronic evidence, sharing information and knowledge around the latest developments in their countries, as well as challenges and good practice in the implementation of laws on electronic evidence. A series of recommendations were agreed by Commonwealth Law Ministers leading to a revision of the Commonwealth Model Law on Electronic Evidence.



Enabling effective investigation and prosecution of cybercrime and promoting international cooperation

An electronic evidence training project, delivered by the Commonwealth Secretariat, has helped establish professional, well-trained law enforcement and prosecution services across the Commonwealth which are equipped with the resources and skills needed to address the demands of modern crime.

Over 90% of Commonwealth countries now have anti-cybercrime legislation and the capacity to investigate cybercrime via dedicated police units

18 countries attended a working group meeting on electronic evidence

47 out of 53 member countries have established a designated focal point for electronic evidence

Live role-playing scenarios were held at three regional events in **Barbados, South Africa and Australia**

A series of recommendations were agreed by **Commonwealth Law Ministers** leading to a revision of the **Commonwealth Model Law on Electronic Evidence**

The Hon Justice Maria Wilson, a High Court Judge in Trinidad and Tobago:

"I thought the final exercise, which was a practical exercise on giving evidence in Court, was very useful. It confirmed for me the point that that both judges and prosecutors and police officers should be on the same page with the kind of evidence that is required to prove a cybercrime in court. This would assist judges in assessing the relevance of evidence and consequently whether the evidence is admissible".

Thanks to this investment from the UK's Foreign, Commonwealth & Development Office, stakeholders from across the Commonwealth have come together and provided an environment in which shared solutions to key modern crime issues could be developed.

Foreign, Commonwealth & Development Office

COMMONWEALTH UNITED KINGDOM CHAIR-IN-OFFICE

Looking forward

During its extended term as Chair-in-Office, the UK has continued supporting the implementation of the Commonwealth Cyber Declaration, including testing new and innovative projects. The UK continues to work with multilateral institutions, particularly those responsible for technology standards, in support of a free, open, peaceful and secure cyberspace, while raising the cost of state-sponsored hostile activity. As it hands over Chairmanship of the Commonwealth to Rwanda, it stands ready to support colleagues in Rwanda and across the Commonwealth to keep building on the significant progress made since 2018 to increase collective cyber security capacity. For more information, visit: www.gov.uk/government/collections/cyber-security-capacity-building-in-the-commonwealth-2018-to-2021

Programme implementers

Over the period of the Programme, the FCDO has worked with various implementers, leveraging their experience and expertise to ensure the most effective programme delivery whilst maximising value, and would like to take this opportunity to thank them for their valuable contribution.

This report was made possible through the support of the Foreign, Commonwealth & Development Office. The opinions expressed do not necessarily reflect the views of the UK Government.

GET SAFE ONLINE

www.getsafeonline.org

Foreign, Commonwealth & Development Office

COMMONWEALTH
UNITED KINGDOM CHAIR-IN-OFFICE