

UK cyber support will help the Commonwealth stand up malign regimes

- Foreign Secretary will announce £15m funding to help Commonwealth countries defend themselves against cyber-attacks.
- Liz Truss will tell Foreign Ministers at a meeting in Rwanda today [24 June] that the Commonwealth has a vital role to play as a counterweight to malign actors.
- Cyber a top security challenge for Commonwealth countries, with attacks in cyber-space and threats to sovereignty and freedom on the rise across the world.

The UK is providing a £15 million package of support to Commonwealth countries over the next three years in the face of the growing threat from cyber-attacks.

The Foreign Secretary hopes to boost Commonwealth nations' resilience to rising threats in cyberspace, empowering the bloc to defend themselves.

Cyber is among the top security challenges that Commonwealth countries face today, with 87% of organisations having experienced an attempt to exploit their existing vulnerabilities in cyberspace.

The Foreign Secretary will tell Foreign Ministers during a meeting today at the Commonwealth Heads of Government Meeting (CHOGM) in Rwanda that an expanded Commonwealth, united behind its shared values is a vital counterweight to the growing threat of malign activity.

She will say that alongside other networks like the G7 and NATO, the Commonwealth can and should play a vital role in challenging autocratic regimes and advancing freedoms around the world.

The UK's renewed package of cyber support for the Commonwealth will involve sharing cyber deterrence expertise, building insights into understanding threats, assessing capability and governing effectively to enable agile responses.

And it will support the voices of smaller countries to ensure that we are, collectively, able to stand up as a powerful voice behind our shared values of sovereignty, democracy and good governance in cyber space.

Foreign Secretary Liz Truss said:

In an increasingly geopolitical world the Commonwealth is a vital

and expanding alliance united behind values of democracy, human rights and sovereignty.

The Commonwealth are collectively taking action to bolster our resilience and security, including in cyberspace, to stand up against autocratic regimes that challenge our freedoms.

Russia's invasion of Ukraine is a stark warning to us all that our sovereignty and security is increasingly under threat around the world and in cyberspace.

The new UK funding will maximise the influence of every Commonwealth member state in vital international negotiations on cyber governance. It will support the voices of smaller countries to ensure that we are, collectively, able to stand up as a powerful voice behind our shared values of sovereignty, democracy and good governance in cyber space.

Tailored projects with Commonwealth countries will work to empower smaller states and a Commonwealth Cyber Governance network will bring together experts from across the organisation, in addition to increasing in-country cyber attaches and UN Women-in-Cyber Fellows.

Collectively, it will make it harder for malign states to meddle in domestic cyber space across the Commonwealth.

The last CHOGM was held in the UK in 2018, with the UK now handing over the chairing role to Rwanda.

Background

- [Check Point Software's 2022 Security Report](#) showed that 87% of organizations have experienced an attempted exploit of an already-known, existing vulnerability.
- The UK made cyber security and resilience a priority for the whole Commonwealth during its period as Chair-in-Office in the last four years. Since CHOGM 2018, every member state has taken steps to improve their cyber security competence and capability. A Commonwealth statement in 2020 called for greater coordination on cyber security and the 2018 Commonwealth Cyber Declaration, agreed by all member states, has strengthened an inclusive and rights-based cyberspace that supports economic and social development.
- UK funding has helped civil society groups in Belize, Kenya, Sierra Leone and Ghana to engage with national governments and contribute toward national cyber security strategies.
- Ransomware has become the most significant cyber threat facing the UK this year, with reports of attacks having more than doubled since 2020.