HM Government

CSSF GLOBAL MEL Partnership

Cyber & Tech Security Programme:

Building on a modest investment to design catalytic intent into a new programme

Lead agency / department	FCDO
Type of intervention	Capacity building and using our influence to leverage funding
ODA / non-ODA (2018-22)	ODA: GBP 22.9m; non-ODA: 6.5m

Summary

The Cyber and Tech Security Programme built on the foundations of a modest, short-term, two-year investment during 2018-20, by developing a new 2020-22 programme, where catalytic intent and potential was an inherent consideration in programme design. The focus of this case study is the 2020-22 programme and how the team built catalytic effect into the programme design on the basis of the 2018-20 experience.

As part of the UK's Chair-in-Office of the Commonwealth 18-20 (CHOGM), the 53 member states signed the Commonwealth Cyber Declaration (NB: there are now 54 members, the Maldives re-joined in 2020). HMG supported member states to: review their cyber security architecture; develop legal and policy frameworks; and, more importantly, commit to global norms and standards on cyberspace. By programme closure, this had leveraged funding from other countries and galvanised action from both multilateral and commercial organisations. The scope then widened to address cyber finance, cybercrime and critical national infrastructure.

The new CSSF programme will capitalise on the achievements of CHOGM and on HMG's reputation as a leader in global cyber security; although it is recognised that HMG/CSSF will not deliver significant change on its own, despite being a leading donor for cyber security activities. The programme documents highlight that cyber security is a cross-cutting issue relevant to many HMG country, regional and thematic National Security Strategy and Implementation Groups, as well as to wider critical issues such as the coronavirus pandemic. In order to address these opportunities and challenges, the programme team is taking a rigorous approach to programme design which seeks to both innovate and scale-up investments in building resilience, promoting technology and developing skills through technical expertise with catalytic interventions both at home and abroad. With a view to maximising the opportunities for catalytic effect, this new programme intentionally adopts adaptive MEL techniques at the design stage, to identify opportunities that have the potential to deliver catalytic

HMG seeks to catalyse national and international cyber and resilience capabilities to uphold a free, open, peaceful and secure cyberspace.

ACCELERATING

- Adoption of Commonwealth Cyber Declaration.
- CMMs
- New CSIRT Implementations
- New GFCE memberships
- Budapest conventions sign ups.

UNBLOCKING

- Through International Data Transfers, the project seeks to remove barriers and burdens to the sharing of personal data, while also ensuring its protection, will help the UK facilitate trade with international partners.

BUILDING CAPACITY

- UK capacity building delivers proven development impact
- Demonstrating relevance of cyber security to C 19 based on previous training and relationships.

LEVERAGING

- Harnesses UK strategic influence position as trusted global actor and demonstrates UK thought leadership and investments in relationships
- Working with and through the Commonwealth, as Chair, and Interpol
- Leading the creation of a World Bank Multi Donor Trust Fund, the Chevening Commonwealth Cyber and Tech Alumni Network
- Securing funding from other donors.

change. The project is assessed to have the intent and potential to create all four "catalytic effects".

What have we learned?

The Commonwealth 2018-20 cyber programme was catalytic in that it ignited a series of events which have enabled further change to occur, primarily through capitalising on the enabling conditions, the momentum following CHOGM and the Cyber Declaration, and the relatively limited timescale. It then leveraged further funding to scale up and expand the cyber programme into 2020-22. The catalytic change story includes deliberately programming for catalytic effect through rigorous analysis and MEL tools such as Theory of Change, Theory of Action and progress markers. This approach holds promise for increasing potential catalytic effect.

Global context and timing were ripe:

- During CHOGM 18-20, the political and resource conditions were present for a modest investment to lay the foundations for longer-term change: "*Lasting results outweigh small investment and short timescale*" (PCR SRO response).
- "The [Cyber] Declaration has served as an important reminder of the critical role of cyberspace in connecting all Commonwealth member states together."
- The global awareness of benefits of and threats to a free and open cyberspace continues to grow.
- In the COVID-19 context, support on cyber security became more relevant as global online presence increased.

Capitalising on timeframes:

- The short time span of CHOGM 18-20 galvanized the Commonwealth countries to implement their Cyber Declaration commitments, identify baselines and initiate building skills and resilience. It created relationships and synergies between member states, multilaterals and commercial organisations.
- The initial investment has leveraged further funding and relationships. While the catalytic effect may not yet be fully apparent, it is already clear that "*it was more than the sum of its parts*". Investment is being increased for new programming in 2020-22, with the likelihood of a longer time horizon beyond this point, subject to the comprehensive spending review.

Programming for catalytic intent is possible, but requires honesty:

- *Catalytic intent* built into the design of the programme was embedded in the project from the start; however, *catalytic effect* is not predetermined, and the team is honest about what it is seeking to achieve.
- The team has deliberately and intentionally looked at how to maximise the opportunities through adaptive MEL. They have identified the actor-based change that is business as usual; but have also clarified what they expect to see, what has the potential to be catalytic, and what they would love to see.

The context

CHOGM 18-20 provided the opportunity, political will, and some modest resources to build leadership and momentum to respond to the growing awareness of the serious challenges in cyberspace, and to position the Commonwealth programme alongside other multilateral initiatives. It has provided a launch pad for the CSSF programme to continue to address the wider context of a precarious cyberspace on the basis of the following problem statement: "the benefits, values and opportunities of cyberspace are daily threatened by malicious actors and activity. This is a threat to our values as much as it is to a specific service or system. With global digital transformation, vastly accelerated by the global health pandemic COVID-19, and with old, current

and emerging technologies in every corner of the world, the surface to protect has grown. This increases the risk of instability and potential future conflict."

Hostile actors continue covert behaviour aimed at causing disruption and undermining values (such as democracy and western values); yet governments take insufficient steps to protect their critical national infrastructure. Although cybercrime is one of the fastest growing forms of transnational crime faced globally, thought leaders and influencers do not pressure or advocate for change and there is limited discussion about cyber security.

Worldwide, from 2019–2023, approximately $5.2 trillion in global value will be at risk from cyber-attacks. 10.5 million records are lost or stolen every month—438,000 every hour—and a single large-scale attack can trigger $53 billion in economic losses. The COVID-19 crisis has further underlined the need for investments in cyber security resilience. Cyber-attacks against the healthcare sector are up 150% since January 2020, with cyber criminals targeting everything from testing facilities to hospital IT systems. Citizens and businesses are increasingly reliant on a free, open, peaceful and secure cyber space to adapt to the coronavirus measures imposed by states. Although it is therefore fundamental that states are able to protect internet users from the corresponding increase in COVID-19-related cyber-attacks, citizens and the private sector do not prioritise or take proactive steps to improve cyber security.

The opportunity

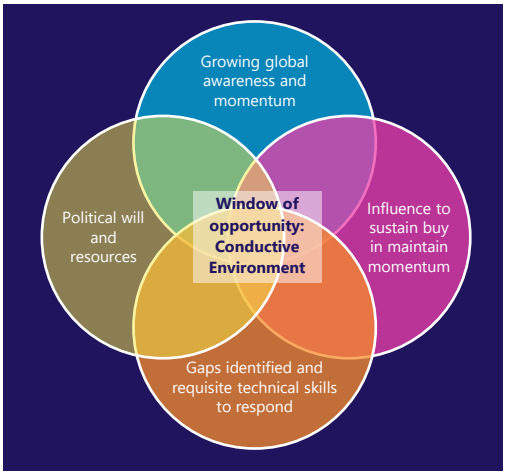
Against such a dramatic context, the cyber security development agenda remains too little advanced. International cyber capacity building has been mainly a national agenda, with comparably little cooperation at bilateral and regional levels or with international organisations and NGOs. Unlike other critical areas of development, there is no major or global international fund supporting low- and middle-income countries focused on cyber security programmes and activities.

Despite laudable investments by different donors and through individual initiatives to assist low- and middle-income countries, the magnitude and strategic relevance of the challenges require a cyber security capacity building programme on a different scale than previous efforts. There is a critical need to better define, understand, articulate, structure and roll out this growing agenda in a systematic manner, with clear result expectations that link assessments to technical assistance and to capacity building and training, underpinned with necessary investments in infrastructure and technology.

Following on from the success of the CHOGM cyber security programme, the CSSF Cyber and Tech Programme is positioned to be a driving force for change. A strong partnership between leaders in cyber security—where the UK is well established as playing a leading role as a cyber champion - can be an effective means for transformational and catalytic change. For example, we are working with international organisations, such as the Commonwealth Secretariat, Interpol, and various UN bodies who are equipped with the technical expertise and ability to roll-out long-term development agendas,

Key factors / conditions:

- The main factor was a conducive domestic and international context: CHOGM Cyber Declaration and impact of COVID-19;
- Growing awareness of ever-increasing reliance on cyberspace, and the reality of cyber threats;
- Political will to implement and resource the Declaration commitments;
- HMG influence and leadership to sustain buy-in and maintain momentum through multilateral organisations;
- Identification of gaps and needs, with the commensurate technical skills to respond;



- Sustainability: A programme team taking the time to understand the space and actors, and willing to take risks with a new approach using MEL processes and tools in a rigorous but adaptive way to identify catalytic potential through progress markers.

The programme document for 2020-23 sets out the intent to serve as a catalyst to:

- **Leverage** existing partners and relationships and expand to new ones (from Singapore and Commonwealth to Interpol and World Bank). For example, this means driving the creation of the World Bank Multi-Donor Trust Fund, perhaps the most catalytic intervention, which seeks to increase access to capacity building support;
- **Unblock** barriers to HMG coordination to underpin fusion of HMG cyber activities;
- **Accelerate** coordination between like-minded international partners and donors;
- Overcome international, national and our own limited capabilities through tried and tested approaches to cyber security **capacity building**, expanding on the success of combatting cybercrime and building incident response resilience and creating an overseas network of cyber attachés within HMG.

Further work by the programme team has led to the development of a new MEL system, including a programme Theory of Change and project-level Theories of Action. These were designed using an actor-based change approach which identified the key actors the programme wanted to influence, their interactions, and the changes in behaviour that the programme aimed to influence in a sustainable manner in order to achieve its objectives.

A new Results Framework was also developed, along with graduated progress markers that enable the programme to measure progress at the outcome level. The progress markers articulate what behaviour changes by key actors the programme a) *expects to see*, b) *would like to see*, and c) *would love to see* as a consequence of programme activities. '*Love to see*' behaviours are characterised by transformational change that actors take ownership of, beyond the lifespan of a programme. Hence, the CSSF seed funding, combined with 'beyond boundary thinking', will support the team to design with catalytic intent and consider the multiplier effects of the programme.

The effects

The main catalytic effects of the Commonwealth 18-20 Fund are highlighted below:

- Delivered more than the sum of the parts. The pan-Commonwealth Cyber Programme has strengthened cyber security across the Commonwealth, creating stronger networks to exchange knowledge and expertise, raising understanding of risks, and facilitating civil society engagement.

- Created a focus on cyber security and on a free and open cyberspace. COVID-19 brought this into stark relief. Timing and context played a part in highlighting the threats to a secure cyberspace.
- Became sustainable, through the network of connections that has been established, and the continued sharing of knowledge and expertise between them. Working through the Commonwealth, where a majority of countries are small, there was a shift in their connections and linkages domestically, regionally and internationally in this domain.
- Built understanding of the gap in the ability of small countries to prioritise cyber-tech and security, given pressing demands on scarce resources.
- Achieved complementarity with two other international cyber programmes, the National Cyber Security Programme-International (NCSP-I) and the Prosperity Fund's Digital Access Programme (DAP). The cumulative range of work of the Commonwealth Cyber, NCSP-I and DAP programmes has enabled UK to build trust and strengthen influence in Commonwealth countries.

Accelerating: The adoption, implementation and momentum of the CHOGM 2018 Cyber Declaration galvanised the 53 member states and created synergies with other multilateral cyber initiatives. *"Since 2018, the Declaration has provided a common framework to put cyber security on the agenda of all member states*". The follow-on programme will continue to accelerate the creation and growth of like-minded groups.

Unblocking: Both the Commonwealth 2018-20 and the 2020-22 programme improve the way cross-Government capability is brought together for greater alignment.

Leveraging: The modest investment has harnessed UK influence, and leveraged direct co-funding from other donors, with follow-on 2020-22 funding in international organisations providing an opportunity for significant catalytic potential, particularly in tackling cyber crime.

Building capacity: The 18-20 programme mainly used a capacity building approach to enhance Commonwealth ability to take new political, operational and legislative actions to deliver on their CHOGM commitments. It also furthered the Commonwealth Secretariat's own capacity in this space. In addition, capacity building has demonstrated the relevance of cyber security to COVID-19. The future programme will seek to address limited UK capacity to build a network of cyber officers and attachés, and will support Commonwealth countries to build their capacity through projects that raise the standards of cyber-crime legislation and develop national cyber security strategies in select countries.

Conclusion and lessons

Through the original £5.5 million CHOGM cyber security programme, every Commonwealth member took steps to improve their cyber security competence and capability and build capacity. A range of pan-Commonwealth, regional and national-level activities resulted in stronger networks to exchange knowledge and expertise across a range of actors, including the Bank of England, Microsoft and Citibank; enhanced sharing of threat intelligence and understanding of risks; and a more informed and engaged civil society. With the continuation of the Cyber and Tech Security Programme beyond Commonwealth 18-20, HMG seeks to catalyse national and international cyber and resilience capabilities to uphold a free, open, peaceful and secure cyberspace.

This case story illustrates the importance of political will and momentum that it needed to both serve as a catalyst and to sustain the longer-term change that is sought. It also validates the conceptual framework, whilst highlighting the need for political momentum or a 'champion' to sustain the desired change.

- **Accelerating** and **building capacity** were clear effects of the project in 18-20 and provided a solid platform for intentional programme design for 20-22.
- **Leveraging** and **unblocking** are key elements of the 20-22 programme.

- Catalytic intent is explicit in programme design, as is a sense of realism.

This case story highlights the importance of having a clear intent, formulated by the cyber team through the use of progress markers.

Sources of information

This catalytic change story was shaped and informed through two discussions with the programme lead and the CSSF point of contact.

The case study drew on documentation including: The UK Commonwealth Chair-in-Office report 2018-2020: delivery of Commonwealth Summit commitments; Annual Reviews and the Programme Completion Review of the Commonwealth 18-20 Fund; the Programme Document for 2020-2023, Implementing Partner's reports, and the emerging Theory of Change, Theories of Action and Results Framework.

Main limitations

It was not possible to interview the team that implemented the Commonwealth 18-20 cyber programme, the Commonwealth Secretariat, or the member states to validate the impact of the Cyber Declaration. The analysis of catalytic effect is based on interviews above, with triangulation through document review and discussions with the GMEL Partnership team supporting the cyber programme MEL.