Cybercrime: Innovative approaches to an unprecedented challenge

David Tait

Cybercrime represents an unprecedented legislative, law enforcement and policy-making challenge. Countries that do not address it risk becoming the weakest link in global cyber security (Westby, 2004). This brief article will discuss the impact of cybercrime internationally, before reviewing the unprecedented responses resulting from this threat.

The definition of cybercrime relied upon throughout will be that advanced in the Commonwealth Expert Group report to law ministers from May 2014 (Expert Report). The report noted that cybercrime includes: ‘(a) offences aimed at computers, computer or communications systems, their users or the data they contain; and (b) more traditional offences committed using these systems, especially if technologies have significant effects on how the crime is committed or investigated.’

This definition is particularly useful not only in providing a clear framework upon which to build understandings of cybercrime, but also by virtue of illustrating the divergence between perceptions of cybercrime and reality. This gulf was aptly illustrated by UK Security Minister James Brokenshire, who observed that: ‘For too long the public’s perception of cybercrime has been a lone bedroom hacker stealing money from a bank account.’ (Brokenshire, 2013)

The changing nature of crime is a key facet of this complex policy area.

The nature of the threat

McAfee estimates the annual cost to the global economy of cybercrime at more than US$400 billion (McAfee, 2014). This is only set to increase as internet connectivity proliferates. Growth is currently being driven by areas with large concentrations of Commonwealth members. Indeed, as noted by Europol, Asia, despite its low internet penetration of circa 27 per cent, provides more than one billion internet users or 45 per cent of the world’s total users. Furthermore, Africa has seen a growth in internet access of 3,600 per cent in the last decade (Europol, 2014: p. 17).

However, it is not merely the growing scale or impact of cybercrime that makes it a unique challenge, but also, a new criminal genus in which the individuality and unique skill-set of each criminal or criminal group results in a high degree of adaptability. Allied with flexibility in communication methods, this allows for the creation of informal networks that can swiftly coalesce around a single task before, equally quickly, dissipating. The effect of this has been the rise of Crime-as-a-Service (CaaS), whereby cyber criminals sell their services to other criminals (Europol, 2014: p. 19). Critically, this significantly diminishes the digital barriers to entry as few technical skills are now required to commit crime via electronic means (Europol, 2014: p. 9).

The global community is confronted by a challenge of unprecedented scale, adaptability and speed, and it is in this context that responses must be understood.

The international response

Despite these hazards, little progress has been made towards forming a unified, international response. In 2010, at the UN’s Crime Congress, the proposal to create a global cybercrime convention failed as a rift developed between Russia, China and certain developing economies, and the USA, Canada and the European Union (Masters, 2010). This was despite the favourable recommendation of the UN Office on Drugs and Crime (UNODC; Harley, 2010). This dispute was multifaceted, and issues of national sovereignty and the fragmentation of the internet and human rights were significant areas of discord. However, so too was the only extant international convention dealing with cybercrime, the Council of Europe’s (CoE) Budapest Convention on Cybercrime (Budapest...
Convention). The position of those who are already members of this convention was that no new treaty was required. However, the convention, which entered into force in 2004, has attracted significant criticism for being too eurocentric, enshrining a developed world bias regarding intellectual property and for being outdated. Importantly, this rift is not limited to national actors. The Budapest Convention has received significant criticism and support from international organisations. Support has been shown by organisations including the Asia-Pacific Economic Cooperation, the European Union, Interpol and the Organization of American States (OAS), while the International Telecommunication Union (ITU) has criticised the eurocentric approach and described the convention as ‘a little dusty’ (Vatis, 2010: p. 218). As a result of these disagreements there is a fragmentation of approaches to governance at an international level.

Alongside these global responses, many international organisations render assistance to national governments in dealing with cybercrime through measures including harmonising laws; capacity-building; and providing operational support. Organisations, such as the Commonwealth Telecommunications Organisation (CTO), UNODC, Interpol, CoE, ITU and OAS, provide capacity-building and operational resources through measures such as legislative drafting and review, training for law enforcement and legal professionals, support for investigations and digital forensics.

The landscape of the international response to cybercrime is well populated, but also confused and contradictory. Although numerous international organisations seek to support their member states, these efforts are not founded upon a single governmental framework at an international level.

The Commonwealth response

The Commonwealth has a distinguished history of working at the critical juncture of information technology and governance. In the 1990s COMNET, a joint initiative of the Maltese government and the Commonwealth Secretariat was established to help realise the transformational potential of information and communication technology for development. COMNET was also designated to lead the Commonwealth Internet Governance Forum (CIGF). The purpose of this initiative is to inform and engage stakeholders on public policy issues relating to internet governance. Alongside this, the Commonwealth Secretariat has continued in its general duties to support the development of rule of law capacity amongst member states.

In 2011 the CIGF consulted on the appetite for a Commonwealth-led initiative on cybercrime. Ultimately, this initiative was mandated by the Commonwealth Heads of Government Meeting (CHOGM) in 2011 for the purposes of ‘improving legislation and capacity in tackling cybercrime and other cyberspace security threats’ (Commonwealth Secretariat, 2011). As a result of consultations the Commonwealth Cybercrime Initiative (CCI) was created in 2011. The role that heads of government believe the Commonwealth should play in this area has continued to develop. At CHOGM 2013 it was noted by the heads of government that: ‘The Commonwealth Cybercrime Initiative and the recent endorsement of its methodology by senior officials of Commonwealth Law
Commonwealth models

The Commonwealth Secretariat provides critical tools to member states in combating cyber vulnerabilities, including the Commonwealth Model Law on Computer and Computer-Related Crime (the Model Law) together with the recently revised Harare Scheme on mutual legal co-operation and the Commonwealth Network of Connected Persons (CNCP).

The Model Law was adopted in 2002 and aims to ensure a high degree of convergence with the Budapest Convention. The law provides the guidance on key legal definitions, offences and procedural law. The Expert Report notes that 22 other Commonwealth countries made use of either the Budapest Convention or the Model Law, illustrating that the Model Law provides a flexible alternative to the Budapest Convention regime. The two systems are wholly compatible save in so far as the Model Law does not deal with mutual legal assistance.

The longstanding Harare Scheme was amended in 2011 to accommodate the challenges posed by electronic evidence and evidence gathering. The revision of the Harare Scheme introduced material on taking evidence or statements through live video link or other audiovisual means; the interception of telecommunications; the interception of transmission data; the disclosure of intercepted material; surveillance; and the provision of subscriber information. Once again, the new provisions of the Harare Scheme closely resemble those of the Budapest Convention (Commonwealth Secretariat, 2014: p. 29).

Finally, the CNCP serves the complimentary purpose of identifying the key contact persons for requests for mutual legal assistance.

Beyond these general forms of assistance, the Secretariat also assists with specific requests. For example, the Expert Report, as endorsed by Commonwealth Law Ministers, included the specific recommendation that ‘each member state develops and maintains an effective national strategy to co-ordinate efforts to prevent and combat cybercrime’.

To this end, in 2014 the Secretariat participated, at the request of the Government of Jamaica and OAS, in efforts to develop such a strategy in Jamaica through advising on models of best practice and attending national validation exercises with key stakeholders. This model of bilateral support mirrors other capacity-building exercises, such as the training of judges, prosecutors and law enforcement officials.

While these efforts deal with emergent problems and developments in the field of cybercrime, they build upon the deep foundations of the Secretariat’s historic role in providing direct assistance to member states in the form of model laws, legislative schemes and capacity-building exercises.

The Commonwealth Cybercrime Initiative

There is a plethora of support offered to countries seeking to combat cybercrime. This presents a significant risk in itself, primarily in the form of duplicated interventions resulting in the squandering of limited resources. The Third Principle of the Paris Declaration of Aid Efficiency, harmonisation, aims to prevent such mistakes and commits donor countries, including many members of the Commonwealth, to ‘work together to reduce the number of separate, duplicative, missions to the field and diagnostic reviews; and promote joint training to share lessons learnt and build a community of practice’ (OECD, 2005: p. 6).

The Commonwealth has uniquely embraced this requirement by developing the Commonwealth Cybercrime Initiative (CCI). The CCI represents a unique attempt to crystallise this commitment to efficacy and collaboration in cybercrime capacity-building. The programme unites 35 international organisations possessing expertise, mandates and resources, including Interpol, OAS, CoE, CTO and ITU, to contribute to multidisciplinary programmes in Commonwealth countries. These organisations form the CCI Consortium.

Upon receipt of a request from a member state, the CCI deploys a mission team including at least one technical and one criminal justice expert, drawn from the consortium members best placed to donate these resources. A gap analysis is then conducted using a specialised CCI checklist (a tool agreed to by all partners) from which a needs assessment report is produced. The outcomes of this report are agreed with the member state, which outlines its priorities and capacities for reform. The consortium is asked to make commitments to meeting these needs, which then form a plan of action for the member state. A strong example of such an approach is in Ghana, where, following a needs assessment in 2013 and under the CCI umbrella, the CTO has embarked on an awareness raising scheme, the Secretariat has begun a review of relevant legislation, the ITU has developed a national Child Online Protection initiative and the UK’s Open University has begun collaboration on two academic centres of excellence at two Ghanaian universities.

This is a unique solution to the problem of scarce resourcing and provides a multitude of routes to assistance. It is predicated on the unique relationship between the Commonwealth, its member states and the international community. This represents a potential model for future multi-stakeholder engagements.

Conclusion

Cybercrime is an evolving area of policy where criminal elements are able, through technological and networking advantage, to far outpace legal frameworks. As such, there has been an explosive growth in both the volume and practices of cybercrime. Difficulties in securing international agreement on governance have resulted in policy fragmentation. Alongside this there is a diversity of support available to states – yet paradoxically limited funding for such work. The exposure of Commonwealth members, together with the Commonwealth’s inherent advantages, has generated bespoke responses to the cybercrime challenge. Through both direct, bilateral assistance to member states and the innovative CCI programme, pragmatic attempts to deal with cybercrime are being promulgated throughout the Commonwealth.
References


DAVID TAIT is a legal researcher with the Rule of Law Division of the Commonwealth Secretariat.