The Commonwealth

Meeting of Commonwealth Law Ministers and Senior Officials

Gaborone, Botswana: 5–8 May 2014

Agenda Item 3(i) **LMM (14)14**

REPORT OF THE COMMONWEALTH WORKING GROUP OF EXPERTS ON CYBERCRIME

Paper by the Commonwealth Secretariat

Background

1. It will be recalled that at their last Meeting in Sydney, Australia, in 2011, Law Ministers considered two presentations on cybercrime in a High Level Ministerial Panel Discussion. The papers underscored the proliferation of digital technology and the convergence of computing and communication devices which have provided a range of opportunities to be exploited for criminal purposes. It was apparent that revolutionary developments in information communication technologies (ICTs) have brought many social, cultural, political and economic benefits. However, equally, these technologies have brought new opportunities for crime and new interests that can be threatened by crime. The meeting heard of legislation, specialist agencies and awareness-raising material developed in Australia, Botswana and Canada among others, noting that the issues were of equal importance to all member countries.

2. There was a sharing of the experiences of many jurisdictions regarding the significant challenges cybercrime presents to national security, to law enforcement, to individuals and to businesses. Ministers noted the existence of a comprehensive international instrument, the Council of Europe's 2001 Convention on Cybercrime, work on which led to the preparation of the Commonwealth draft Model Law on Computer and Computer-Related Crime in 2002, and to regional efforts in West Africa.

3. Ministers resolved to recognise the significant threat cybercrime poses to national security and law enforcement in all countries of the Commonwealth, and mandated the Commonwealth Secretariat to form a multidisciplinary working group of experts to:

- Review the practical implications of cybercrime in the Commonwealth
- Identify the most effective means of international cooperation and enforcement, taking into account, amongst others, the Council of Europe Convention on Cybercrime, without duplicating the work of other international bodies

- Collaborate with other international and regional bodies with a view to identifying best practice, educational material and training programmes for investigators, prosecutors and judicial officers.[1]

4. Pursuant to this, the Legal and Constitutional Affairs Division (LCAD) of the Secretariat, in conjunction with the Governance and Institutional Development Division (GIDD), established a multidisciplinary working group (the Group) comprised of individual experts, academics, representatives of some member countries.[2] These experts have developed legislation and have practical experience, Commonwealth organisations,[3] civil society,[4] and regional[5] and international organisations[6] with remits on cybercrime and related matters, to deliver the mandate. The Group also drew on existing Commonwealth anti-cybercrime expertise in the context of the Commonwealth Cybercrime Initiative (CCI).

5. The Group met five times between January 2012 and May 2013 to explore the various elements of the mandate. After painstaking research and deliberations, the Group produced a comprehensive report (Annex A).

The Working Group's Report

6. The report of the Group is divided into three parts, each addressing one part of the mandate.

7. In its first part, the report from the Group considers the nature of cybercrime and the challenges it poses to member countries. It states that cybercrime poses challenges to traditional law enforcement techniques due to several factors, including: the speed with which offences can be committed; the fast pace at which offending evolves into new forms; and the transnational character of cybercriminal activity. It also notes that cybercrime is a global concern, as the nature of the internet means that an offender in one jurisdiction can target any other jurisdiction. A weak link in the chain at any location threatens all countries.

8. The report finds that the implications of cybercrime in member countries depend on numerous factors, including size, development indexes and national experiences with information and communication technologies. It identifies the general implications of each of these characteristics. For example, small island states may have difficulty training and retaining the specialist staff needed to form a sustainable cybercrime forensics unit. Regional offices may provide the answer to this particular challenge.

9. In its second part, the report recommends that, to tackle cybercrime, the most effective means of international cooperation and enforcement is an effective national, legal regime against cybercrime, combined with effective international cooperation.

10. In considering international cooperation, the Group assessed several formal and informal international and regional instruments based on specific criteria, including: the comprehensiveness of the instrument in addressing the different aspects of an effective cybercrime regime; the practicality and realism of the instrument's provisions; the extent to which the instrument addresses human rights and procedural safeguards; and whether the instrument carries with it relevant support mechanisms. Based on these criteria, the Group

[1] Commonwealth Law Ministers Meeting Communiqué, 2011 paragraphs 17–19.
[2] Australia, Canada, Tonga, South Africa, Singapore and the United Kingdom.
[3] Commonwealth Magistrate and Judges Association (CMJA), Commonwealth Lawyers Association (CLA) Commonwealth Telecommunications Organisations (CTO).
[4] Internet Corporation for Assigned Names and Numbers (ICANN), COMNET.
[5] Council of Europe.
[6] United Nations Office on Drugs and Crime (UNODC), International Telecommunications Union (ITU).

recommends that Commonwealth countries should be encouraged to accede where practicable to the Council of Europe Convention on Cybercrime (Budapest Convention).

11. The Group additionally recognises that there are regional legal instruments and other initiatives on cybercrime at various stages toward completion in several regions containing Commonwealth countries. The Group recommends that, insofar as it is possible to do so without prejudicing other forms of cooperation, Commonwealth countries should consider becoming party to and participating in regional conventions and initiatives on cybercrime, in order to ensure further coordinated action.

12. The Group noted that the Commonwealth Model Law on Computer and Computer-Related Crime is modelled after the Budapest Convention and recommends its adoption by member countries that have yet to develop comprehensive legislation on cybercrime. The revised Harare Scheme is also considered a useful tool for cooperation for member countries to reflect in their national legislation.

13. In considering effective national regimes against cybercrime, the Group recommends that member countries should be encouraged to develop and implement all the components of an effective and adequately resourced response to cybercrime, including: secure infrastructure; appropriate capacity in prevention; investigation; prosecution and in the judiciary; and cooperation between the public and private sectors. The Group identified several international organisations and Commonwealth bodies which provide capacity building and technical assistance in this area. It notes that the Secretariat has a continuing role to play in combating cybercrime, particularly (though not exclusively) through its Commonwealth Cybercrime Initiative (CCI). The CCI operating framework is attached at Annex B.

14. In its third part, the report considers cybercrime training in more detail. The Group found that it would not be feasible to include in its report a comprehensive catalogue of training products, as such a list would inevitably be incomplete and almost immediately out of date. The Group instead proposes a strategic model for training, a training model for the Commonwealth, and practical recommendations for use when conducting cybercrime training. Amongst its key findings are that a basic level of cybercrime training should be provided to all criminal justice actors, and that, given the interconnected strategic elements in combating cybercrime, needs assessments engaging all stakeholders as well as international organisations already involved in-country should precede sustainable responses from training projects.

Developments since SOLM 2013

15. The Working Group’s report was considered by Senior Officials of Commonwealth Law Ministries in September 2013. Senior Officials expressed appreciation for the report and discussed their own jurisdictions’ experiences with cybercrime. They approved the report for submission to law ministers.

16. The Working Group’s report was originally finalised in July 2013 in preparation for SOLM. The following developments in the Commonwealth’s efforts to combat cybercrime, in particular through the CCI, are brought to the attention of Law Ministers for the purposes of recommendation (C) to this paper.

17. Following the bringing of the management of CCI and its budget in the Commonwealth Secretariat, the CCI has made progress in several member countries. Renewed engagement with the government of Ghana has brought about presidential endorsement of the CCI programme in the country. A comprehensive resource and training

needs analysis for the criminal justice system is being conducted in collaboration with the United Kingdom Crown Prosecution Service, and university collaborations have been set up between the countries to develop technical skills. The CCI is working closely with the International Telecommunications Union in Ghana. An official launch for the programme bringing together all stakeholders is scheduled for March 2014.

18. Needs assessment missions have been completed in Kenya and Uganda and the reports shared with the respective governments. The CCI is working closely with the governments to implement the phase two programmes of work. Additionally, upon request from the Ugandan government and with approval from the Kenyan government, a high-level planning meeting is tentatively scheduled for the second quarter of 2014 to bring together senior officials from the six East African Community countries to identify, coordinate and plan initiatives which can be extended regionally. The CCI is working closely with UNODC to plan and facilitate this meeting through the EAC.

19. A needs assessment mission has been completed in Trinidad and Tobago and the phase two programme of work is being developed, with an official launch also planned for the second quarter of 2014.

20. Finally, the strength of the Commonwealth's convening power has been demonstrated by the continued expansion of international partners in the CCI. New Zealand has joined the Executive Management committee and made monetary contributions. The UK DfID, the World Bank, the African Union Commission, the Organisation for American States, the World Economic Forum, Microsoft and Vodafone have joined the Operations Consortium.

21. It is in this context the Commonwealth Heads of Government at their meeting in Colombo, Sri Lanka, in November 2013 noted the CCI and the decisions of SOLM 2013, and called for the provision of assistance to developing countries on their cybercrime issues.[7]

Recommendations

22. Law Minsters are invited to consider and approve the report of the Commonwealth Working Group of Experts on Cybercrime attached at Annex A.

23. Approve the Secretariat's programme of work in tackling cybercrime, including:

- Collaboration with national, regional and international organisations to provide and/or facilitate technical assistance to criminal justice officials and other relevant stakeholders of member countries through the Commonwealth Cybercrime Initiative (CCI), and through the Secretariat's other programmes

- Facilitate the establishment of regional networks to support the efforts of small Commonwealth states to develop and retain the capacity to combat cybercrime

- Establish, in collaboration with other organisations and without duplication of effort, a virtual community on Commonwealth Connects to share information and best practice on cybercrime, and to maintain a database of trainers, training materials and training centres that may be made available to member countries in response to requests for technical assistance

[7] Commonwealth Heads of Government Meeting Communique 2013, paragraph 64.

- Work with course providers in order to create and develop course materials and ‘train the trainer’ courses in fields not covered by existing national, regional or international training courses, having particular regard to the practical needs of small states

- Conduct needs assessments as necessary to facilitate requests for assistance

- Follow the lead of Heads of Government and endorse the Commonwealth Cybercrime Initiative (CCI) methodology in the implementation of the mandate.

Commonwealth Secretariat
Marlborough House
Pall Mall
London SW1Y 5HX

March 2014

The Commonwealth

ANNEX A

COMMONWEALTH
SECRETARIAT

THE COMMONWEALTH WORKING GROUP OF EXPERTS ON CYBERCRIME

REPORT TO COMMONWEALTH LAW MINISTERS 2014

The Commonwealth

GLOSSARY OF ABBREVIATIONS

APWG	Anti-Phishing Working Group
CARICOM	Caribbean Community
CBC	Commonwealth Business Council
CCI	Commonwealth Cybercrime Initiative
CHIS	Children’s Charities’ Coalition on Internet Safety
CHOGM	Commonwealth Heads of Government Meeting
CIGF	Commonwealth Internet Governance Forum
CMJA	Commonwealth Magistrates and Judges Association
COMNET	COMNET Foundation for ICT Development
CPS	Crown Prosecution Service
CSPs	*Communication Service Providers*
CTO	Commonwealth Telecommunications Organisation
CTU	Caribbean Telecommunication Union
DDoS	Distributed Denial of Service
ECOWAS	*Economic Community of West African States*
eNACSO	European NGO Alliance for Child Safety Online
FATF	Financial Action Task Force
G7A	A Group consisting of the Finance Ministers of seven industrialised nations: United States; United Kingdom; France; Germany; Italy; Canada; and Japan
OECD	Organisation for Economic Co-operation and Development
GPEN	Global Prosecutors’ e-Crime Network
HIPCAR	EU-ITU project: Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures
HIPSSA	EU-ITU project: Support for Harmonization of the ICT Policies in Sub-Sahara Africa
IAP	*International Association of Prosecutors*
ICANN	Internet Corporation for Assigned Names and Numbers
ICB4PAC	EU-ITU project: Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries
ICMEC	International Centre for Missing and Exploited Children
ICPO-INTERPOL	International Criminal Police Organization
ICSPA	International Cyber Security Protection Alliance
ICT	*Information and communications technology*
IGF	*Internet Governance Forum*
ITU	International Telecommunication Union
IWF	Internet Watch Foundation
NCA	National Crime Agency
SOCA	Serious Organised Crime Agency
T-CY	Cybercrime Convention Committee of the Council of Europe

UNODC *United Nations Office on Drugs and Crime*

“24/7 network” *Formal or informal network of access-points for rapid assistance in international cybercrime investigations that are staffed on a 24-hour and 7-day week basis.*

The Commonwealth

INTRODUCTION AND EXECUTIVE SUMMARY

The Law Ministers' Mandate and the CHOGM Commitment

1. At the Commonwealth Law Ministers' Meeting held in Sydney from 11 to 14 July 2011, Law Ministers resolved to recognise the significant threat cybercrime poses to national security and law enforcement in all countries of the Commonwealth, and mandated the Commonwealth Secretariat to form a multidisciplinary working group of experts to:

(i) review the practical implications of cybercrime in the Commonwealth;
(ii) identify the most effective means of international co-operation and enforcement, taking into account, amongst others, the Council of Europe Convention on Cybercrime [hereinafter referred to as the Budapest Convention], without duplicating the work of other international bodies; and
(iii) collaborate with other international and regional bodies with a view to identifying best practice, educational material and training programmes for investigators, prosecutors and judicial officers.[1]

The Commonwealth Working Group on Cybercrime

2. In January 2012 the Legal and Constitutional Affairs and the Governance and Institutional Development Divisions of the Commonwealth Secretariat established this Working Group (hereinafter referred to as 'the Group') to work on the Law Ministers' Mandate and present a Report to Law Ministers at their Meeting in Botswana in 2014. As work had already started within the Commonwealth in the context of the Commonwealth Internet Governance Forum (CIGF)'s Commonwealth Cybercrime Initiative (CCI), it was thought appropriate for the Group to draw upon the expertise already existing within the CCI and augment the Group with experts drawn from a number of member states, institutions working in this field, academics, legal professionals and civil society in order to form a truly multidisciplinary group (see Appendix). In seeking to include the widest range of stakeholders, including those who are involved in the establishment and operation of the CCI, it was hoped to capture the widest range of viewpoints to address the matter and produce a balanced report.

3. The Group held its first meeting at the Commonwealth Secretariat on 27 February 2012 to discuss its terms of reference and consider how it would take forward its work and held further meetings in Geneva on 12 and 13 June 2012, and in London on 13 November 2012, 12 and 13 March 2013, and 16 and 17 May 2013.

4. The Group recalled the importance attached to the problem of cybercrime as a national and transnational crime and the work of the Commonwealth Secretariat, the CIGF and other specialised agencies in tackling the issue, and noted that:

(a) in a related paper on the revision of the Harare Scheme relating to Mutual Legal Assistance in Criminal Matters within the Commonwealth (the Harare Scheme), Law Ministers also resolved to adopt a revised and updated Scheme and mandated the Secretariat to develop an associated Model Law and to report to the Senior Officials Meeting to be held in September 2013 on progress in developing this body of work. The updated Scheme includes in its provisions the interception of telecommunications and postal items; covert electronic surveillance; the use of live

[1] Commonwealth Law Ministers Meeting Communiqué, 2011 paragraphs 17-19: Cybercrime.

video links in the course of investigations and judicial procedures; and asset recovery.

(b) In October 2011 following the Law Ministers' Meeting, the Commonwealth Heads of Government, at their Meeting in Perth, Australia:

(i) re-iterated their commitment to improve legislation and capacity in tackling cybercrime and other cyber inspired security threats, including through the Commonwealth Cybercrime Initiative (CCI), which had recently been formed to assist developing countries to develop their institutional capacity in fighting cybercrime through the sharing of expertise from existing resources, with particular focus on the Commonwealth Model Law on Computer and Computer-Related Crime[2] and also drawing from other treaties, conventions (including the Budapest Convention), legal frameworks, toolkits and guidelines; and

(ii) re-iterated their support for the Commonwealth Connects programme which is encouraging greater effort from member countries to harness the benefits provided by technology, through promoting strategic partnerships, building ICT capacity and sharing ICT expertise; encouraged member countries to contribute to the Commonwealth Connects Special Fund[3]; and requested the Secretariat's continued support for the programme.

5. The Group acknowledged the need for:

(a) international co-operation and enforcement, including through the Budapest Convention, and other regional initiatives, and for collaboration to assist Commonwealth member states with capacity building and best practices to deal with transnational aspects of cybercrime;

(b) the Commonwealth to leverage its unique advantages, building on the core competencies of individual Commonwealth agencies;

(c) the Commonwealth Secretariat to ensure that its work does not duplicate but complements the work of other agencies working in the same area and to collaborate more effectively with, and take into account the experience of the Council of Europe and United Nations entities such as the International Telecommunications Union (ITU) and the United Nations Office on Drugs and Crime (UNODC); and

(d) recognition that although the Law Ministers' Mandate is specifically directed to cybercrime and therefore to conduct that requires a crime prevention and criminal justice response, it is also concerned with cyber security and can include threats that are the result of errors and gaps in systems as well as those that are malicious. The Group has addressed its mandate with a primary focus on cybercrime whilst incorporating, as ancillary, several aspects that also contribute to enhanced cyber security.

6. The Group received information relating to the cybercrime laws of Australia, Canada, Pakistan, Singapore, South Africa, Trinidad and Tobago, and the United Kingdom and the

[2] Text available at: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf

[3] A fund established by CHOGM in 2005 to implement activities within the Commonwealth Connects programme.

extent to which they had been influenced by the Commonwealth Model Law and the Harare Scheme, reports from the UNODC and the Council of Europe on the results of their studies and surveys of cybercrime legislation, and from the ITU, the Commonwealth Telecommunication Organisation (CTO), and the CCI.

The Group's Approach, Conclusions and Recommendations

7. The Law Ministers' mandate requires answers to three questions, which though not entirely separate, call for separate responses, and which for the purposes of the Group's Report have been labeled Part 1, Part 2, and Part 3. A summary of the Group's approach, conclusions and its recommendations is as follows.

Part I: Practical Implications of Cybercrime in the Commonwealth

8. Cybercrime at all levels of sophistication poses unprecedented challenges in terms of legislation, law enforcement, and policy-making. 'Cybercrime' is not a defined legal category, but for the purposes of this report 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.

Procedural laws must also deal with the issues raised when digital material is to be relied upon in court, whatever the nature of the offence. International co-operation is facilitated by common approaches to criminalisation and any cybercrime-specific investigative or procedural rules.

9. It is not possible to give accurate figures as to the scale and cost of cybercrime, but there is general agreement that it is a fast growing phenomenon and that, taking indirect as well as direct costs into account, it costs the global economy many billions of US dollars a year.

10. Cybercrime does not respect national boundaries. That creates challenges for the public sector, in terms of legislation and investigative and prosecutorial capacity and reach, and for the private sector, which must address technical vulnerabilities in the systems it designs and operates which sometime straddle many national jurisdictions. The Internet brings criminals together to share information on how to commit crimes and how to avoid detection, adding a new dimension to organised crime. Increasingly, successful attacks are founded on knowledge, co-operation and deals created and shared between networks of individuals and groups. Offenders seek out and exploit any weak links or vulnerable locations.

11. Fast communications mean that offences can be committed very quickly, and that digital evidence of them can be erased equally quickly. Even with the best possible legal measures, the speed of offending is a major challenge for investigators, and the practical implications of this include the need for a high degree of skill, high quality equipment and extensive training. The complexity and speed of evolution of cybercrime makes it essential

that expertise in policy, law, law enforcement, prosecution and prevention not only be developed but also monitored, maintained and updated frequently. To do this efficiently it is important that all countries co-operate effectively, both within the Commonwealth and globally.

12. Commonwealth member states are as much affected by the challenge of cybercrime as other states. The practical implications of cybercrime depend in part on the characteristics of the countries affected, both those from which offenders operate and those in which the effects are felt, and the criminal justice and other capacities of those countries.

13. The following analysis divides countries into four general categories.

(i) The interests of large, developed Commonwealth countries are generally to develop sophisticated capacities for the prevention and control of cybercrime and to co-operate internationally to make them as available as possible.

(ii) The interests of developing countries in general tend to reflect the need to protect technological development from cybercrime, both as a development goal in itself and because cybercrime poses a threat to the use of technologies as a means for the achievement of other development goals. Beyond this, a range of specific interests arise depending on factors such as size and rates of technological or other development, which make individual assessment and the balancing of general and country-specific assistance important.

(iii) In rapidly-developing Commonwealth countries, a major implication of cybercrime is the fact that the development of technology may outstrip the development of the ability to prevent and combat crime, both by public and private sector entities. The major need of rapidly developing countries will usually be assistance in developing crime-control capacity, especially in the public sector.

(iv) Small Commonwealth countries have smaller governance and administrative sectors and they are less likely to have technical and policy experts in academic, private sector and other resources. Infrastructures in small states are more limited, as are the personnel and expertise needed to support them. The difficulties faced by small states are felt in many areas of criminal law or policy, but they pose a much greater challenge in the area of cybercrime.

14. The challenge for small countries is not only to develop law enforcement and preventive capacity but to maintain it on an on-going basis. To do this, special co-operative relationships among the smaller countries and between small and larger countries should be explored.

Part 2: Identify the Most Effective Means of International Co-operation and Enforcement, taking into account, amongst others, the Council of Europe Convention on Cybercrime, without duplicating the work of other international bodies

15. In seeking to identify ‘the most effective means of international co-operation and enforcement against cybercrime’, the Group has considered whether it should limit its enquiry to an examination of international and regional instruments, or whether it should extend it to the improvement of national legislation and capacity building, without which international co-operation and enforcement cannot be effective.

16. As Commonwealth countries cannot enjoy the protection of an effective anti-

cybercrime regime without adequate anti-cybercrime legislation and the capacity to support it, the Group agreed to examine the mandates and activities of organisations working in this field. The object of Part 2 is to assist Commonwealth countries to develop the most effective means of international co-operation and enforcement, an object which can only be achieved by helping them to identify the organisations and tools best suited to improving their legislation and capacity building, including through technical assistance to developing countries. Without, therefore, detracting from the terms of its mandate and its task, the Group has added, as ancillary, to the scope of its work on Part 2 an examination of the capacity-building efforts of organisations and initiatives working in this field together with the minimum standards required at national level on which member countries require assistance.

17. The Group agreed that the best means of international co-operation and enforcement is an effective national criminal justice regime against cybercrime, including appropriate preventive, investigative and prosecutorial capacity, as well as the practical skills needed to manage complex and transnational investigations. The Group recognised the importance of co-operation with the private sector and civil society in this context.

18. International co-operation can be based on a wide range of scenarios depending on the countries and facts in each case. Possibilities range from informal and ad hoc co-operation on a case-by-case basis to the use of multilateral, bilateral or regional legal instruments. The Group was mindful of the larger debate about the merits and demerits of a global legal instrument, but did not believe that this debate should be an obstacle to progress at a more practical level. That said, based on its content and accessibility, the criteria set out in paragraph 2.10 of this report, the Budapest Convention appeared to the Group to be currently the most effective and viable model for Commonwealth member states[4]. The Report also notes the availability of other international legal instruments. The Commonwealth Model Law follows the Budapest Convention and the Group encourages the use of the Commonwealth Model Law and the Harare Scheme in the drafting of their legislation as part of the base level which all Commonwealth countries should achieve.

19. A Council of Europe report on the results of its survey on the 'Implementation of the Budapest Convention and the Commonwealth Model Law on Computer and Computer-Related Crime' which was submitted as a contribution to the work of the Group indicates that four Commonwealth countries are Parties to the Convention, two others have signed the Convention and one has been invited to accede; that 22 other Commonwealth countries made use of the Budapest Convention or the Commonwealth Model Law and/or expressed an interest in becoming a Party; and that, on a preliminary analysis of the available information, 16 Commonwealth countries in addition to those that are Parties have legislation that is largely consistent with the standards of the Budapest Convention. These countries could submit a request for accession. Such decisions and the completion of the ratification process by Canada and South Africa could increase the number of the Commonwealth countries using the Convention as a framework for international co-operation to 22 and the total number of Parties to 57. The Council of Europe has engaged in co-operation activities with 39 out of 54 Commonwealth countries.

20. The Group was kept informed about discussions by the UN open-ended intergovernmental expert group on cybercrime convened pursuant to General Assembly Resolution 65/230, which are on-going. That process has not yet reached any substantive

[4] In view of the continuing work of the open-ended expert group on cybercrime established by the General Assembly, UNODC cannot endorse this statement.

conclusions[5], but it did highlight the range of diverse views among UN member states, and the fact that capacity building and technical assistance was needed in all areas independently of any efforts at the setting of global legal or other standards[6]. There was broad support for capacity building and technical assistance, and for the role of UNODC in that regard.

21. Commonwealth countries should also be encouraged to develop and implement all other components of an effective response both to cybercrime, and to the challenges related to the recognition, collection, preservation and admissibility of electronic evidence in relation to any type of criminal activity. These should include as a minimum:

(a) national strategies for an effective and co-ordinated response;
(b) effective cybercrime prevention including
(c) general awareness raising;
(d) co-ordination of actions by government departments and other agencies;
(e) appropriately resourced and trained criminal justice actors[7];
(f) efficient response systems such as 24/7 networks; and
(g) mechanisms and protocols for co-operating with Communication Service Providers (CSPs) and the private sector as a whole.

Part 3: The Group collaborate with other international and regional bodies with a view to identifying best practice, educational material and training programmes for investigators, prosecutors and judicial officers

22, This part of the Report seeks to establish clear guidelines regarding the levels of training on cybercrime and handling electronic evidence that may be necessary for criminal justice actors. The provision of adequate resources by governments for this purpose is crucial.

23. It is necessary to take into account the different roles and professions of criminal justice actors and any assessment of training needs as well as any sensitivities about the method and context of delivery.

24. The requirements for skills and knowledge range from those at the basic levels, where training should be embedded within routine training programmes, to those at the highest level where specialised training is needed by those tasked with investigating electronic attacks on critical national infrastructure and other targets, as well as those dealing with the analysis and interpretation of electronic evidence. Generally the higher the knowledge level required, the lower the numbers of personnel that need to be trained.

25. The approach to the planning of training recommended by the Group supports and encourages countries to incorporate cybercrime and electronic evidence training within their national programmes drawing on training initiatives and well tested and proven programmes already in existence.

[5] UNODC does not associate itself with this wording. Resolution 22/7 of the United Nations Commission on Crime Prevention and Criminal Justice (2013) expressed appreciation for the work done thus far by the expert group, requested the group to continue its work towards fulfilling its mandate, invited the group, subject to the availability of extra-budgetary resources, to finalise reports of its deliberations and requested to report to the Commission on progress in its work.

[6] UNODC does not associate itself with this wording which is not included in the report on the meeting of the expert group to conduct a comprehensive study on cybercrime held in Vienna from 25-28 February 2013 contained in document UNODC/CCPCJ/EG.4/2013/3.

[7] This term is used in this Report to include investigators, prosecutors, law enforcement personnel, judges and magistrates.

26. The approach recommended requires Commonwealth countries to: (a) examine their legislation in order to assess whether there are adequate provisions for action against cybercrime; (b) examine whether they have sufficient specialised capacity within law enforcement and prosecution offices; and (c) assess the adequacy of training strategies and programmes. Key components of such strategies and programmes should include international co-operation, industry relations and, for example, means of tackling illegal financial transactions on the Internet. Any supportive response project would address deficiencies identified whilst ensuring local responsibility and sustainability beyond the life of the project. Individual governments may well find it necessary to adapt or develop training modules, including training skills development to local conditions.

27. The creation of regional training centres for criminal justice actors supported by the private sector and academia should be considered for the purposes of economies of scale.

28. The report sets out the sequence of the principal main steps to be taken in order to build a comprehensive training strategy. No new training initiatives should be undertaken without these stages being completed. This is accompanied by a more detailed practical approach to training delivery and exchanges of good practice and a list of indicative measures. The importance of specialist networks and co-operation with the private sector to take advantage of their expertise are recognised as important features within a strategy to build capacity to understand and tackle cybercrime.

RECOMMENDATIONS

PART 1

1. The Group recommends all Commonwealth countries to co-operate effectively, both within the Commonwealth and globally, to develop, monitor, maintain and update frequently their expertise in policy, law enforcement, prosecution and prevention of cybercrime.

2. The Group recommends that each member state develops and maintains an effective national strategy to co-ordinate efforts to prevent and combat cybercrime. This may include legislative, judicial, prosecutorial, law enforcement and preventative public sector entities and appropriate private sector entities.

3. The Group recommends the creation of special co-operative relationships among the smaller developing countries as well as between developed and developing countries to build law enforcement and preventive capacity and to maintain it on an on-going basis, for example including the development of regionally-based investigative or emergency response resources, and the sharing or provision of investigators, forensic facilities and similar resources on a case by case basis as needed, and to explore the practical, legal and sovereignty aspects of such arrangements.

4. The Group recommends that Commonwealth countries develop effective prevention strategies in co-operation with the private sector and civil society, having regard to the need for preventive measures to be co-ordinated internationally. Specific elements should include the development and maintenance of appropriate technical security measures, training directed at specific situational threats or risks, and educational and awareness-raising programmes directed at general populations.

PART 2

5. The Group recommends that Commonwealth countries should be encouraged to bring their laws into line with the Commonwealth Model Law and the Harare Scheme (as revised).

6. The Group recommends that Commonwealth countries should be encouraged

(i) to accede, where practicable, to the Budapest Convention[8]; and/or

(ii) where they can do so without prejudicing other forms of co-operation, to consider becoming Party to any regional and/or international cybercrime conventions and participating in other initiatives to ensure co-ordinated action against cybercrime.

7. The Group considers that there is no immediate need to revise the Commonwealth Model Law, but given the rapid evolution of cybercrime, some supplementation may in future be judged necessary.

8. The Group recommends that Commonwealth countries should also be encouraged to develop and implement all other components of an effective and adequately resourced response to cybercrime, and the challenges related to the recognition, collection, preservation and admissibility of electronic evidence in relation to any type of criminal activity.

9. The Group recommends that the Commonwealth Secretariat should in managing the Commonwealth Cybercrime Initiative and in its more general work on such matters as money-laundering and terrorism, without unnecessarily duplicating effort, continue its role in the development of capacity within the Commonwealth to combat cybercrime, and continue to collaborate with other international and regional organisations to provide and/or facilitate technical assistance in this field to member states.

10. The Group recommends that Law Ministers should follow the lead of CHOGM in

[8] In view of the continuing work of the open-ended expert group on cybercrime established by the General Assembly, UNODC cannot endorse this part of the Recommendation.

endorsing the Commonwealth Cybercrime Initiative and should ensure that their colleagues in government are aware of it and should, as appropriate, facilitate its work.

1. **The Group recommends that the Commonwealth Secretariat, in collaboration with other organisations and without duplication, should establish a virtual community to share information and exchange views, and a repository of best practices and lessons learned.**

PART 3

12. The Group recommends that all Commonwealth countries be encouraged to incorporate cybercrime and electronic evidence training within their national training programmes for criminal justice actors.

13. The Group recommends that Commonwealth countries should be encouraged to follow the model recommended within the Report and follow the steps and adopt the measures listed in order to achieve an effective training strategy supported by relevant educational material and good practice.

14. The Commonwealth Secretariat should take a lead on cybercrime and electronic evidence training of criminal justice actors by

(a) maintaining up-to-date information (in conjunction with other international organisations) about existing training products that may be available to Commonwealth countries from third party, national and international organisations;

(b) making use of the Commonwealth Connects platform to maintain a database of existing regional and international training courses and centres and available materials that can be accessed or distributed in response to requests from national governments, judicial or law enforcement bodies;

(c) maintaining similarly a database of trainers and training providers that are qualified and able to support training activities for criminal justice actors in Commonwealth countries; and

(d) working with training course providers, including those experienced in training the judiciary in the Commonwealth, such as the Commonwealth Magistrates and Judges Association, in order to create and develop course materials and training of trainers courses in fields not covered by existing national, regional or international training courses especially where gaps have been identified and where further capacity building is required.

(e) Training institutes should consider involving academic and private sector experts in the design of their programmes and the development of training material.

IMPLEMENTATION

16. Bearing in mind the seriousness of the practical implications of cybercrime and the urgent need for the commitment of adequate resources, the Group strongly recommends that member states contribute the resources needed for the implementation of the foregoing recommendations.

PART I: PRACTICAL IMPLICATIONS OF CYBERCRIME IN THE COMMONWEALTH

> 'It has no capital, no airport, and only 1400 people who call it home, but the tiny isle of Tokelau has become the cybercrime centre of the world. A new report by an international group tackling internet scams has confirmed that Tokelau, a New Zealand territory, has more malicious registrations under its '.tk' domain name than any other domain except '.com'. These fraudulent web addresses are used for phishing, where emails are sent to random web addresses in an attempt to steal banking information and other personal details…' *Sydney Morning Herald*, 28 April 2011.

The Effects of Cybercrime

1.1 Countries at all stages of social, economic and technological development are experiencing the effects of revolutionary developments in information and communications technologies. Many effects are plainly beneficial. Families and commercial enterprises enjoy easy and rapid communication across the world. There is greater awareness (and hopefully better understanding) of other nations and cultures. But equally there are new opportunities for crime and the creation of new interests that can be threatened by crime. The increasing sophistication and speed of computer systems, and the convergence of information and communications technologies, enhance the capacity of technological change to benefit society, but also provide opportunities for those who seek to exploit the same capacity for criminal purposes.

1.2 Cybercrime at all levels of sophistication poses unprecedented challenges in terms of legislation, law enforcement, and policy-making. Law makers have to define and criminalise it. They have to craft provisions which facilitate the investigation and prosecution of cybercrime but also apply human rights norms in new and untested contexts. Their aim must be to provide stable national legal platforms for the international co-operation that is critical to effective national and international responses to the problem.

1.3 Law enforcement agencies have to acquire and maintain high degrees of technical sophistication and conduct high-speed international investigations without losing sight of the need to respect national sovereignty and fundamental rights.

1.4 Governments need to develop national strategies that include essential participants from outside the criminal justice community and from the private sector, and to find ways to co-operate with one another as never before.

The Nature of Cybercrime

National definitions

1.5 'Cybercrime' is not a defined legal category, but a label that has been applied to a range of illicit activities associated with information and communications technologies and computer networks. For the purposes of this report, it includes:

(a) a core cluster of criminal offences covering conduct that is harmful to computers, computer or communications systems, such as hacking, distribution of malware[9], DDoS (Distributed *Denial of Service) attacks, and other forms of interference with data or systems; and*

[9] Various forms of hostile or intrusive software including computer viruses, ransomware, worms, Trojan horses, rootkits, keyloggers, dialers and spyware.

(b) more traditional offences committed using these systems, especially if technologies have significant effects on how the crime is committed or investigated; these will include stalking, criminal copyright infringement, money laundering and fraud. This category may be perceived differently from country to country, depending on policy decisions about whether to criminalise the underlying conduct at all, and often, minor differences in policy or legislative strategy. So, for example, some countries have created specific 'computer fraud' offences, while others have either relied on ordinary fraud offences or made minor legislative adjustments to ensure computer fraud is included in them.

1.6 The technologies affect the ways in which crimes are committed, but they can also affect the broader contexts of psychological, social, economic and deterrence factors that influence offending patterns, and some pre-existing forms of criminality have been transformed more than others. A good example of this has been the evolution of the production of and trafficking in "child pornography" or images or other content derived from the sexual exploitation of children. The scope of the problem has expanded enormously as a result of technologies which make it easier to produce and disseminate the illicit materials to a global audience with less risk than pre-digital offending, and which place more distance between consumers and abused or exploited children. During the same period, many of the same factors have contributed to an even larger expansion in the making and dissemination of "erotic" or "pornographic" content, which is not considered as illicit or criminal in many countries. The resulting de-stigmatisation of "pornography" in general has led to pressures to re-label "child pornography" in terms which focus less on a digital commodity that might be legal or illicit depending on what it depicts, and more on the underlying evil of the sexual exploitation of children that is an element of both its creation and dissemination. The concept of "child pornography" or "exploitation materials" is still reflected in international legal instruments, the Commonwealth Model Law, and the laws of many countries because of the need to establish specific and distinct criminal offences relating to child-abuse and the creation, possession and/or dissemination of illicit materials.

1.7 Computer technologies have become so ubiquitous that they are now used to organise or facilitate almost any form of crime. That does not usually lead governments to treat the offences involved as forms of cybercrime *per se*. Trafficking in narcotic drugs, for example, is not usually regarded as a form of cybercrime, but the Internet can be used for organisational and communications functions as well as to launder proceeds.

1.8 The classification of offences in this way is useful for the development of policy initiatives. However, in reality cybercrime commonly involves criminal activities falling into several categories. For example, distributing malware may be an offence in its own right but is often used to facilitate other offences, such as fraud. This also presents considerable investigatory and evidentiary challenges.

1.9 There can therefore be no clear demarcation between 'cybercrime' and 'non-cybercrime', nor is one required. Whether a country considers a particular problem to be 'cybercrime' for its own purposes often depends on whether it chooses to respond to it as a new problem or simply an old one using new means of commission that requires updating policies and legislation. In this context whether or not a type of criminality is labelled as 'cybercrime' is not as important as whether the response chosen is actually effective at the national level and as a basis for international co-operation. The latter does require a recognition of the full range of issues discussed in this Report, even if a narrower understanding of cybercrime suffices for national purposes.

1.10 Types of criminal activity, which are not regarded as "cybercrime" *per se* often still raise cybercrime issues when considered from the perspectives of evidentiary requirements and law enforcement capacity and training because offenders use the technologies in indirect ways. In scenarios such as the drug-trafficking example above, law enforcement agencies must be able to search computer networks and intercept and read e-mail messages, and investigative and evidence laws would be needed to provide the necessary powers and ensure that seized or intercepted data are admissible as evidence. Whenever digital material forms part of the evidence to be relied on in a prosecution, whatever the nature of the offence, procedural and evidence laws need to make provision enabling its use, and there is a need for training of criminal justice actors in the skills needed to preserve, collect and produce in court electronic or digital forms of evidence.

International co-operation

1.11 International co-operation is facilitated by common approaches to criminalisation and any cybercrime-specific investigative or procedural rules. Complete harmonisation and identical offences are not essential, but the scope and structure of offences need to correspond closely enough to enable criminal justice actors to co-operate effectively, to support formal mutual legal assistance, and to meet 'dual criminality' requirements for extradition and mutual assistance where they apply. The greatest pressure for harmonisation, however, especially in criminal offence provisions, comes from offenders and not from governments. Any new vulnerability or criminal technique spreads quickly once discovered, placing uniform pressures for the development of responses by criminal justice actors and legislators everywhere.

1.12 The major constraints on harmonisation are the policy differences between individual countries with respect to what conduct or content is sufficiently harmful to justify criminalisation and, in the case of content offences, the countervailing application of freedom of expression and other human rights principles. The result is that there is broad international consensus on some offences, especially those that deal with crimes against computer networks themselves and on offences such as computer fraud and the making or dissemination of materials depicting the sexual abuse or exploitation of children, where there was already consensus on the underlying pre-existing crime. There is a lesser measure of agreement on content-related offences: this may reflect national policy differences with respect to such matters as hate speech, blasphemy and harassment.

The Scale and Cost of Cybercrime

1.13 There is no accurate way to measure the number of "cybercrime" offences or occurrences, and as above there are no universally agreed definitions of cybercrime on which to base such a measurement. Cybercrime occurrences are generally some form of interaction between offenders and victims, however, and some indication of the volume and rate of expansion can be inferred from the expansion of the Internet itself. The number of Internet hosts has gone from zero in 1980 to about 908.6 million as of July 2012[10], and the numbers of on-line devices and of users is much higher, especially in developing countries where shared or public-access facilities are more common. This creates an unprecedented pool of potential offenders, victims and interactions. Fraudulent "spam" messages can be

[10] Internet Systems Consortium, Internet Host Count History;
http://www.isc.org/solutions/survey/history. An 'internet host is any computer which is connected to the Internet and has a unique IP (Internet protocol) address. The annual electronic count of such hosts is regarded as a measure of the expansion of the Internet over time but does not necessarily reflect other factors such as the number of people using the Internet, number of web sites or volume of data or communications.

sent at once to millions of recipients, and a "botnet", a network of machines that have been infected with malware, may have thousands, even millions, of machines within its scope.

1.14 A report commissioned by the UK Cabinet Office and published in 2011[11] estimated cybercrime's annual cost to the UK to be £27 billion. That report was greeted with widespread scepticism and seen as an attempt to talk up the threat. It led the UK Ministry of Defence to commission a further study from a group of academics. Their report[12] noted:

> There are over 100 different sources of data on cybercrime, yet the available statistics are still insufficient and fragmented; they suffer from under- and over-reporting, depending on who collected them, and the errors may be both intentional (e.g., vendors and security agencies playing up threats) and unintentional (e.g., response effects or sampling bias).

1.15 The report for the UK Ministry of Defence contains a sophisticated analysis of both direct and indirect costs (including such things as the effect of loss of confidence in systems) and covers many different types of cybercrime. Although the authors warn against any simple totalling of their estimates, the figures in the report suggest an annual cost for the UK which approaches US$20 billion. Global estimates are much harder to make with any degree of accuracy; the authors estimate a global figure in excess of US$200 billion a year.

Cybercrime has no National Borders

1.16 Cybercrime does not respect national boundaries. That creates challenges for the public sector, in terms of legislation and investigative and prosecutorial capacity, and for the private sector, which must address technical vulnerabilities in the systems it designs and operates.

1.17 Cybercrime prosecutions may involve multiple offenders, victims and evidence from many different countries, a fact which can create significant resource and logistical challenges for the law enforcement and prosecutorial agencies presenting cases and for the courts which hear them. Further the offences may be triable in more than one jurisdiction and there may be an issue as to the appropriate venue for the case or cases to be heard.

1.18 The nature of modern technology means that it is not always possible even to say where a cybercrime is committed, in either legal or factual terms. Networks are increasingly being designed to store information in remote or diffuse physical locations and move it around automatically ('cloud computing'), in order to optimise the use of storage and transmission capacity. This confounds conventional approaches to jurisdiction, because in some scenarios it can be difficult to ascertain where information or system users are located. Similarly, the law that applies to evidence before or after it is obtained will sometimes depend on the physical location at which it was obtained or intercepted, and the design of modern networks can make this difficult to ascertain.

Implications

1.19 The transnational aspects of cybercrime also have significant implications for investigation and prosecution. Effective measures to investigate cybercrime and to collect and preserve digital evidence need to be speedy, but criminal justice systems and procedural safeguards are rooted in domestic law and are based on jurisdictional territoriality and national sovereignty. Requests for mutual legal assistance can be notoriously slow and

[11] Detica and Office of Cyber Security and Information Assurance, The cost of cyber crime, February 2011.
[12] R Anderson and others, Measuring the cost of cybercrime (2012), available at http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

even where expedited mechanisms exist they are not always used. Human rights considerations, and the protection of civil liberties, may require judicial authorisation before evidence can be collected. The timescale involved may not meet the operational requirements of cybercrime investigations, especially if several different countries are involved.

1.20 This can create multiple practical challenges for investigators. The procedural requirements that matter most will often be those of another country, which requires close co-operation and access to fast and accurate legal assistance from the country involved. The extent to which human rights and independent judicial oversight are engaged may depend on the nature of the investigation or specific locations or types of information involved, and investigators need to ensure that they neither over- nor under-estimate these. On one hand, where the applicable law permits fast and informal co-operation it is important to use it effectively, but on the other hand where the nature of the co-operation sought does engage fundamental human rights interests it is equally important that they are not circumvented. Information that is on a public website or 'subscriber/traffic data' that only identify parties and locations without disclosing content may be more easily obtainable than the content of communications themselves.

1.21 These challenges are most commonly seen in the context of human rights, but they have national sovereignty and practical investigative aspects, and evidentiary aspects as well. For example, direct investigative measures can interfere with parallel criminal investigations in other countries, and most states reserve the right not to provide assistance where such investigations might be prejudiced. They may not co-operate with or allow the investigation of conduct which they themselves do not regard as criminal. Evidence collected in one country and used in another must often satisfy the legal admissibility requirements of both, and the use of digital evidence sometimes generates forensic challenges not encountered with tangible evidence.

The offenders' view

1.22 The Internet brings criminals together to share information on how to commit crimes and how to avoid detection. Increasingly, successful attacks are founded on knowledge, co-operation and deals created and shared between networks of individuals and groups. The Internet makes it possible for individuals to commit major transnational offences, but the majority of cybercrime represents new dimensions in domestic and transnational organised crime. Not only do networks permit much larger and more transnational organised criminal groups to form, they also permit entirely new organisational structures and relationships to form, challenging both legal definitions and investigative techniques. The technologies have transformed illicit markets by creating whole new digital commodities and transforming others into forms that can be more easily created or trafficked. Both identity-related crime and the creation of and trafficking in images of child abuse are pre-existing forms of criminality that have been so transformed.

1.23 Various forms of malware require much more skill to create than they do to use, which has made them a valuable commodity among offenders and at the same time opened up various forms of on-line crime to a wider and less-skilled body of offenders. The black market in malware is lively and enterprising individuals offer all levels of service for hire. One example is the infamous 'Zeus' application, which spreads from one device to another by various means, directing each infected device to copy specified information such as passwords or financial transaction dates, and return it to locations from which the offenders can retrieve it. In May 2011 the source code for Zeus was leaked online, allowing offenders to download, copy, and modify it for their own purposes. In December 2012, Symantec discovered a criminal selling a complete installation of Zeus for US$250. Illicit consulting services can also assist in setting up “botnets”, which infect computers and allow criminals to hijack and use them for other purposes, for charges that range from US$350-400. The truly idle offender can pay to have services distributed through an existing botnet at US$30 for 20,000 spam emails, or US$525 for 5 hours of DDoS attacks per day for a week[13].

1.24 The transnational nature of the technologies, and of the crimes they facilitate, make it easy for offenders to seek out and exploit any weak links or vulnerable locations. This creates practical challenges in that legislation, law enforcement, prevention and security measures become interdependent, and also that seeking out and closing any vulnerabilities becomes a constant and ongoing task. Any location where law enforcement or security measures are relatively weak can be used by offenders as a base of operations from which to target other, better-protected locations, and this creates a powerful shared incentive for technical assistance and capacity building to eliminate weaknesses that render everyone vulnerable.

1.25 In this context, what matters is not necessarily the perspective of governments, but that of offenders. From their perspective a ‘relatively weak’ or vulnerable ‘location’ may range from a single address, file-server or local computer system to an entire country, and ‘weakness’ simply means choosing whatever digital location offers the easiest illicit access and/or the lowest risk of detection and prosecution. Weaknesses and vulnerabilities may be technological or jurisdictional, and they are ‘relative’ to one another in the sense that, as each specific vulnerability is addressed, another one becomes the ‘weakest link’ in the network and will become a new focus for offenders. No country, company, or individual can be complacent, because security depends on keeping one’s own security measures at the same level as others as well as one step ahead of offenders.

1.26 Technical vulnerabilities are mostly a concern for the private sector, which develops the technologies and operates the networks. For companies individually, the security of products and systems is a key element of competition and commercial success, and collectively there is a shared interest in making the Internet itself safer. In general the fear of crime is bad for business, and cybercrime is no exception.

Cybercrime happens quickly

1.27 Fast communications mean that offences can be committed very quickly, and that digital evidence of them can be erased equally quickly. This presents serious challenges for conventional investigative techniques. In response, the laws of many countries and the Budapest Convention provide ‘fast freeze - slow thaw’ schemes in which investigators may seize, or order the preservation of, digital evidence quickly and then complete the necessary judicial proceedings before it may be accessed and actually examined and read. Even with the best possible legal measures, the speed of offending is still a major challenge for investigators, and the practical implications of this include the need for a high degree of skill and extensive training, and that investigators have equipment which is as fast and powerful as that used by the offenders.

Technology evolves rapidly, and Cybercrime evolves with it

1.28 Information technology evolves very rapidly, and new ways to commit cybercrimes are constantly being developed. For example, as mobile phone usage increases and the technology becomes more sophisticated, criminals seek to target mobile operating systems.

[13] Fortnet Security, Anatomy of a Botnet.

Another example can be found in the use of specialist malware to compromise card readers at ATMs or point of sale. New developments are hard to predict, which makes prevention difficult. Legislative, law enforcement and policy agendas in this context can only be largely reactive, set by a combination of technological change and innovation and new patterns of criminal activity. Although this may be true to some extent for any criminal law policy area, the practical implications are greater for cybercrime because of its global scope, speed and complexity.

1.29 The immediate practical implications of this include the need for constant monitoring of new technologies and forms of cybercrime; for fast reaction to close vulnerabilities and update investigative and prosecutorial capacity; and for greater emphasis on crime prevention. The best way to deal with new vulnerabilities is to identify and close them before they can be misused, and as with prevention in general, this is an area where the private sector plays an important role.

The Need for effective Cybercrime Prevention

1.30 Crime prevention reduces the human cost of offending, and it also reduces or avoids the direct and indirect costs associated with investigation, prosecution, punishment and other reactive measures. These advantages are much more compelling in the case of cybercrime because of the much higher costs associated with investigating and prosecuting the complex, transnational and broad-ranging crimes made possible by information and communications technologies and computer networks. The prevention of cybercrime is complex and generally entails a high degree of collaboration between the public and private sectors at both the domestic and international levels.

1.31 Generally, prevention strategies would include some combination of the following elements:

(a) *Technical security elements* are needed to exclude offenders and make computer systems more difficult to access or penetrate. In general, these should be incorporated into new technologies and systems as they are developed and then maintained to ensure continued effectiveness as the threat of cybercrime evolves. This is primarily a function of the private sector, but governments can play a role in areas such as encouraging the development of appropriate measures and assisting diverse companies in developing common and interoperable security measures.

(b) *Targeted or situational prevention* based on an assessment of specific situational risks by both public and private sector entities is also important. There must be education or training of specific groups to raise awareness of the assessed threat, and as to how it can be reduced or prevented. Situational elements often combine education and technical measures: for example, a company threatened by cyber-fraud may both acquire new security products and train its employees how to use them to detect or prevent fraud.

(c) *Broad ranging public information campaigns* directed at users of technologies are also needed to raise awareness of cybercrime in general and of specific forms of cybercrime as they emerge from time to time. General awareness of the nature and scope of the problem encourages good cyber-security habits among general users, and fosters better understanding of, and co-operation with, law enforcement and other authorities in a shared response to the problem.

Technologies and Networks as ‘critical infrastructure’ and the Rise of ‘cybersecurity’

1.32 In the past decade, information and communications technologies have grown in importance to the point where many states regard them as critical infrastructure and see the need to protect them as a security interest and not just a criminal justice matter. The policy focus moves beyond the protection of individual economic or social interests to the protection of infrastructure which is seen as critical to the functioning of the state itself.

1.33 As a subject, “cybersecurity” is broader than “cybercrime” and focuses more on preventive than on reactive policies. Cybersecurity includes the protection of networks and data from non-criminal threats such as natural disasters or system failures, for example. Cybercrime measures can also be seen as a means to the end of better cybersecurity, in the sense that criminal offences are defined, investigated and prosecuted, to a large degree, based on the need to identify and criminalise conduct which poses a threat to computer users or general populations, and to deter and incapacitate those who would or do engage in such conduct.

1.34 Classification of cybercrime and related activities as a security matter often reflects a combination of an assessment of the risk or probability that an attack will occur and the magnitude of the potential harm were an attack to succeed. Offences against state interests, such as espionage or terrorism offences, will always be regarded as cybersecurity matters, but economic forms of cybercrime will only be included if they either are linked to such offences (e.g. frauds that finance terrorist activities), or are of sufficient magnitude to damage the state’s overall economic stability. There may be special concern if a ‘cyber-attack’ is thought to be launched from another state or if the motivation of the attackers is to gain policy influence or extort policy changes through the commission of crime or the threat of crime. When these interests are engaged, ‘cybercrime’ begins to overlap significantly with concerns about ‘cybersecurity’.

1.35 Specific technologies have become embedded in pre-existing critical infrastructures controlling electrical power, water supplies, air and ground transport, emergency and health services and the like, and increasing reliance on computers and networks for basic communications has made computer networks critical infrastructures in their own right. Disruptive attacks on major banks or securities-trading systems can occur on a scale that damages national economies, and even small interferences with governance functions such as electronic voting systems can have major effects.

1.36 While the different policy foundations of cybercrime and cybersecurity may be fairly clear, the practical implications are less so. Most preventive measures, whether they are technical applications such as firewalls and encryption or training and education of system users, are also labelled as ‘security measures’, and they protect systems, users and countries equally from all threats, regardless of whether they originate with a state actor or a private criminal or whether they are motivated by politics, terrorism or simple greed. Most countries still rely on the adoption and prosecution of criminal offences as a major element of defence and deterrence, even if the interests involved are security interests such as terrorism or espionage.

1.37 The overlap of crime and security policy interests does have a significant impact on how countries react to the issues, both at the policy level and in individual cases. Within states, the perception of cybercrime as a national security issue influences the way in which policies and laws are developed. Internationally, matters are further complicated by the fact that each state may have its own perception of the scope of security interests. States may be less co-operative when dealing with matters of security as opposed to crime more generally. Internationally, whether an issue is labelled as a criminal or as a security matter also tends to have institutional implications, as crime and security mandates tend to be assigned to different bodies.

Practical Implications of Cybercrime in the Commonwealth

1.38 Commonwealth member states are as much affected by the challenge of cybercrime as other states. The practical implications of cybercrime depend in part on the characteristics of the countries affected, including both those from which offenders operate and those in which the effects are felt, and the criminal justice and other capacities of the countries concerned.

1.39 The Commonwealth is notable for the diverse range of member states in terms of culture and technological development. Over half of its citizens are under 25, and the Commonwealth contains some of the world's largest and smallest countries by population and some of its richest and poorest economies. This combination of homogeneity as well as diversity poses some practical challenges in collaborating effectively against cybercrime, but it also provides some significant advantages in making the Commonwealth a potential setting for creative and innovative discussions and policy development, and for specific initiatives such as the linking of smaller states into specific co-operative relationships.

1.40 Broadly speaking, the different implications of cybercrime on Commonwealth member states can be usefully considered in the following groups, based on size and the degree, pace and direction of development.

Implications for developed Commonwealth countries

1.41 Developed member states have a long history of engagement with information and communications technologies and with efforts to prevent and suppress cybercrime. They have the private sector expertise to develop and market new technologies, or the resources to import such expertise, and to incorporate crime-control elements into them, and the public sector expertise to develop and maintain up-to-date laws and law enforcement capacity. For major transnational cases they have greater prosecutorial capacity and resources, which may affect decisions about where to prosecute if jurisdictional requirements are met[14].

1.42 The speed with which new technologies and their criminal misuse evolves poses a major challenge even for their research and development capacity, but beyond this the major domestic interest of such states is to ensure that their laws and law enforcement capacities are adequate and effective at home, and their major international interest is to protect their nationals and national interests by encouraging and assisting other countries to establish and maintain basic laws, law enforcement capacity and preventive security measures.

1.43 Such states have heavily invested public and private resources in applications that can be threatened or compromised by cybercrime or the fear of cybercrime. These include general commercial interests in areas such as e-commerce and the provision of banking, e-trading and other financial services, and many specific commercial interests related to the provision of hardware, software and network or communications services. In the public sector they include quasi-public elements such as the ownership, control and regulation of mass media, telecommunications and other services considered as 'essential' or quasi-

[14] For a useful list of the jurisdictional, legal and practical considerations see Results of the second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity, U.N. document no. E/CN.15/2007/8/Add.2 and paragraph 50.

public in one state or another, and also a range of specific public sector functions. Many developed countries rely heavily on networks for the payment of taxes, maintenance of voting registries, and the maintenance of public-sector identity infrastructures, and these are vulnerable both to the direct effects of cybercrime and the indirect effects and loss of confidence that can be generated by the fear of cybercrime, whether it originates at home or from another state.

1.44 At the level of the Commonwealth and other intergovernmental processes or bodies, the interests of these states are generally to develop sophisticated capacities for the prevention and control of cybercrime and to co-operate internationally to make them as available as possible. In addition to protecting domestic information infrastructure, this is sometimes also seen as a development goal, both to directly address the so-called 'digital divide', and indirectly in the sense that information infrastructure is increasingly used as a means of delivering other forms of sustainable development.

Practical implications for developing Commonwealth countries in general

1.45 In general developing countries are seeking assistance in responding to the challenges of cybercrime, both as an element of broader high-technology strategies and to fill specific gaps or assessed needs. Upgrading a country's national information infrastructure will usually entail some consideration of how to incorporate crime prevention elements, for example, and the same country's legislative or law enforcement institutions may be seeking specific assistance to extend existing criminal law to cybercrime and ensure that new provisions can be adequately enforced and investigated. Unlike some other elements of sustainable development strategies, high-technology elements are usually both a means to the end of development and a development goal in their own right, because the technologies themselves represent a means of delivering development assistance in key areas such as education, commerce, health care, and effective and efficient communications between governments and their populations.

1.46 In general "Internet penetration", or the number of Internet computers *per capita*, in developing countries is lower than in developed countries, whereas the situation with other communications devices such as mobile telephones is quite different and may in some countries be the reverse. Mobile or cell phones have become common in the developing world because the infrastructure is much cheaper and more easily constructed, and this has often allowed these countries and their populations to circumvent obstacles to development.

1.47 Whether or not these differences affect overall levels of cybercrime, they do affect specific crime patterns and the way individual countries perceive and respond to the threat of cybercrime. In developed countries, the focus tends to be more on offences such as fraud and identity-related crimes that target individual victims, whereas developing countries may be more likely to perceive and experience cybercrime as a threat to collective and social interests and to development itself. Countries with smaller economies may also regard it as a more serious threat in proportional terms: a major fraud that represented only a large economic loss in a developed country might threaten the viability or credibility of the financial infrastructure of a developing country.

1.48 It is important to note that each country represents a unique case. The assessment of development levels is complex, and the degree of development in general economic and social terms and in terms of specific areas related to information and communications technologies are to some degree independent of one another and may differ from country to country. Individual countries also base policy not only on their assessment of the *status quo*, but of strategic positions and aspirations. That said, the goal of bridging the 'digital divide' between developed and developing countries has been a central objective of the United

Nations since the Millennium Declaration of the 55th Session of the General Assembly in 2000,[15] and both an end and a means to the end of development in every major intergovernmental organisation since then.

1.49 Bearing in mind that in this context ‘development’ tends to refer more to technological development than more general *indicia* of social and economic development, the overarching objective of developed countries is to assist developing countries in establishing and maintaining up-to-date information and communications infrastructures and the expertise and skills needed to make them self-sustaining, and this is generally true regardless of the relative size or rate of development of the countries involved. As above, this is both a strategic and altruistic development goal and a matter of enlightened self-interest on the part of donors because the resulting capacity supports economic prosperity, good governance and other strategic objectives.

1.50 There are many practical aspects and implications of this, but in the case of cybercrime, the first major implication is that cybercrime has the potential to reduce and even neutralise the development advantages of information technologies for everyone, especially for developing countries. The second major implication is that cybercrime from emerging information societies threatens everyone. Thus, while each country, and its information and communications infrastructure and development, must be assessed individually, countries with expertise and resources have a shared interest with developing countries in bringing all countries up to a level at which everyone is protected from cybercrime.

Practical implications for rapidly developing Commonwealth countries

1.51 This group of Commonwealth member states, exemplified by India, can be characterised not so much by factors such as size or degree of development, but by the pace of development. One significant impact of information and communications technologies has been the opportunities they provide for rapid development, often by allowing developing countries to ‘leap-frog’ over or around barriers that arise in more traditional development strategies. This sort of rapid progress has major advantages, but it also raises some practical implications and concerns about vulnerability to cybercrime.

1.52 One of these is the fact that, as reliance on technologies as the means and goal of national development increases, and as individual use and reliance on the technologies increase, so does the threat posed by cybercrime and the magnitude of the harm it can cause to national development strategies and the major benefits they provide. A developing country attempting to produce and market hardware or software will not be competitive if it falls below international norms and comes to be regarded as a ‘weak link’ in terms of its vulnerability. More generally, internal development strategies based on technologies will generally depend to a large degree on public confidence in them, which can be seriously affected by cybercrime. Developing countries are more vulnerable to a loss of confidence and reputation damage if their products are seen to be vulnerable to attack than developed countries that have the capacity and resources to recover from cybercrime.

1.53 The other major implication of cybercrime for such countries is the fact that, in any rapid transformation, and especially one involving the complexities of modern information technologies and infrastructures, it can be difficult to ensure that the ability to combat cybercrime keeps pace with the development of commercial activities. In fast-emerging economies strong competition tends to see innovation outpace security in the private sector,

[15] See U.N. General Assembly Resolution 55/2, of 8 September 2000 (A/RES/55/2,Annex). See also the annual General Assembly resolutions dealing with technologies, development, globalisation and interdependence, including A/RES/55/212 of 20 December 2000, and most recently, A/RES/67/195 of 21 December 2012.

and the speed of change can outstrip the capacity of the public sector in terms of legislation, law enforcement and training.

1.54 When gaps between the reliance a state places on technology and its capacity to combat cybercrime open up, they can be discovered by offenders anywhere, not just in the country where they arise. This makes fast-developing countries a tempting target for sophisticated offenders elsewhere, as innovative industries create new vulnerabilities, criminal techniques that no longer work against more sophisticated targets may still be viable, and the lesser capacity of local law enforcement provides protection for offenders not only from domestic investigations but transnational ones as well.

Specific practical implications for small developing Commonwealth countries

1.55 Cybercrime poses additional challenges for countries with small populations. Smaller countries are no less exposed to cybercrime than larger ones, but they tend to have fewer resources and smaller law enforcement and other institutions to meet the challenge, and in proportional terms they have to expend more effort and resources than larger countries to obtain the same results. Whether a small country is able to do this depends on other factors. A small country whose economy includes significant elements that would be threatened by cybercrime, such as financial services or international commerce, such as Singapore, may be willing and able to invest heavily in preventive and law enforcement capacity whereas many other small developing countries may not be.

1.56 Developing Commonwealth countries with populations of less than 1.5 million, such as Tonga, face the same general challenges as all developing countries in the need for the resources and expertise to build adequate levels of preventive, investigative and prosecutorial capacity, but they face additional challenges in maintaining that capacity. About one-half of Commonwealth member states fall into this category. For these countries, the problem is primarily one of both human and financial resources. Developing countries with small populations have smaller governance and administrative sectors and they are less likely to have technical and policy experts in academic, private sector and other resources. The development of new cybercrime laws or the conduct of a sophisticated investigation and prosecution is no more or less difficult in Tonga than it is in the United Kingdom, but the latter has large numbers of experts in all of these areas and the former does not. Infrastructures in small states are more limited, as are the personnel and expertise needed to support them. The same general pattern holds true for cybercrime-prevention capacity in the private sector: if service providers are smaller and have fewer subscribers, their ability to establish and maintain in-house expertise and capacity is less.

1.57 Small developing countries face additional challenges in developing and maintaining capacity in most areas of crime prevention and criminal justice because expertise is more difficult to develop and maintain in smaller institutions than it is in larger ones. Once specialised expertise is established in a large police force, for example, it may become largely self-sustaining as new officers brought into a large specialised unit are gradually trained and gain expertise under more senior experts, whereas in a smaller one the only way to maintain expertise may be to send officers elsewhere for the necessary training. These problems face small developing countries in other areas as well, but they are particularly acute in the area of cybercrime because of its speed, complexity, international nature, and the pace at which the technologies and criminal misuse of them is evolving.

1.58 Moreover, the small populations and isolated locations of some Commonwealth countries do not make them any less vulnerable to cybercrime. Indeed, in some respects they may well be more vulnerable to the commission of cybercrime and to its adverse effects; their territories may be used as a virtual base by offenders who are never physically present there. Offending patterns often reflect the fact that criminal conduct can be displaced by strong laws and law enforcement into jurisdictions where the risks are less for offenders, but with physical crimes such as robbery an isolated location makes this difficult. Strict enforcement elsewhere is unlikely to displace much bank robbery to Tuvalu or Tonga, but the same is not true for cybercrime. If small developing countries are not supported in developing and maintaining security and other capacities at levels consistent with other countries, they risk becoming attractive to offenders as a safe haven from which other locations can be attacked, and this provides an incentive for developed countries to provide such assistance and for developing ones to accept it. Smaller, more isolated countries also often rely more heavily on the Internet and communications technologies than larger countries specifically because they are isolated, and this degree of dependence means that the adverse effects, such as a loss of communications, can have much more serious consequences.

1.59 The challenge to small countries is not only to develop law enforcement and preventive capacity but to maintain it on an on-going basis. To do this, special co-operative relationships among the smaller developing countries as well as between developed and developing countries should be explored. Examples might include the development of regionally based investigative or emergency response resources, and the sharing or provision of investigators, forensic facilities and similar resources on a case-by-case basis as needed. The practical, legal and sovereignty aspects of such arrangements need to be explored and the nature of the Commonwealth may make it a useful forum for such consideration.

Recommendations

1. **The Group recommends all Commonwealth countries to co-operate effectively, both within the Commonwealth and globally, to develop, monitor, maintain and update frequently their expertise in policy, law enforcement, prosecution and prevention of cybercrime.**

2. **The Group recommends that each member state develops and maintains an effective national strategy to co-ordinate efforts to prevent and combat cybercrime. This may include legislative, judicial, prosecutorial, law enforcement and preventative public sector entities and appropriate private sector entities.**

3. **The Group recommends the creation of special co-operative relationships among the smaller developing countries as well as between developed and developing countries to build law enforcement and preventive capacity and to maintain it on an on-going basis, for example including the development of regionally-based investigative or emergency response resources, and the sharing or provision of investigators, forensic facilities and similar resources on a case-by-case basis as needed, and to explore the practical, legal and sovereignty aspects of such arrangements.**

4. **The Group recommends that Commonwealth countries develop effective prevention strategies in co-operation with the private sector and civil society, having regard to the need for preventive measures to be co-ordinated internationally. Specific elements should include the development and maintenance of appropriate technical security measures, training directed at**

specific situational threats or risks, and educational and awareness-raising programmes directed at general populations.

PART 2: IDENTIFY THE MOST EFFECTIVE MEANS OF INTERNATIONAL CO-OPERATION AND ENFORCEMENT, TAKING INTO ACCOUNT, AMONGST OTHERS, THE COUNCIL OF EUROPE CONVENTION ON CYBERCRIME, WITHOUT DUPLICATING THE WORK OF OTHER INTERNATIONAL BODIES

The National Dimension

2.1 This part of the Group's mandate speaks of 'the most effective means of international co-operation and enforcement'. The Group is clear that this part of the mandate should not be interpreted as limited to 'international co-operation' in the sense of mutual legal assistance and/or extradition, and similarly that it should not be limited to 'enforcement' in the sense of the enforcement of judgments and penalties issued or imposed in another state. The focus is on effective means by which the international community can meet the challenge of cybercrime, and that requires effective systems to be in place within each state. International co-operation will be most effective if each state has a developed strategy against cybercrime, and the capacity and means to give effect to that strategy.

2.2 Such national systems must have a strategy for preventive work, and adequately trained, skilled and resourced investigative and prosecution agencies and the judiciary. Cybercrime by its nature places especial demands on the technical capacity of state agencies and on their ability to interpret and analyse complex international transactions. The effective discharge of the state's responsibilities will often require close co-operation with the private sector and civil society.

2.3 An example of such co-operation is provided by the United Kingdom's Cybercrime Reduction Partnership which held its first meeting in March 2013. It brings together Government ministers, academics, experts from the IT sector, and law enforcement agencies with the aim of staying one step ahead of criminals by sharing information and raising awareness among businesses and consumers.

The International Dimension

2.4 As Part 1 of this report has emphasised, cybercrime is international in nature. To combat it effectively there must be close co-operation between agencies in different countries. It is often the case that informal contacts between agencies provide the swiftest, most economical and most effective means of co-operation, but more formal methods may have to be used to comply with applicable international obligations to ensure that the procedural requirements of the legal system or systems involved are met. This may be especially true where digital evidence is to be relied upon in court. The effort expended in gathering and preserving digital material may be wasted if it cannot be transmitted from state to state in a form that is both technically and legally secure, or if the laws and procedures of the receiving state do not enable this type of evidence to be admitted and given probative value.

2.5 Digital data can be transmitted or erased by offenders very quickly and from long distances, which creates a tension between investigative needs and procedural safeguards, and when international borders are involved, national sovereignty and comity. On one hand, investigators need to trace, locate and secure digital evidence before it can be moved or erased, but on the other hand, safeguards are needed when investigators in one country are seeking evidence in another. There is a need to ensure that investigators in one country do not unintentionally interfere with or compromise enforcement or investigative measures elsewhere. In general, the more intrusive the investigative measures and the stronger the privacy interests in the data sought or the place where it is located, the more formal and time-consuming the investigative and international co-operation procedures become. Compliance with human rights safeguards may take more time when the request originates in a different country.

2.6 The Group noted the importance of provisions whereby data could be identified or 'frozen' by the requested state and then released to the requesting state once the appropriate safeguards had been applied. The Group also noted the expanding use of ‘24/7’ networks whereby investigators in one state could obtain immediate assistance in another to trace and identify target data, assess its nature and ensure that the appropriate procedures were followed as efficiently as possible. The Group further noted that under-estimation of privacy interests could compromise basic human rights protections and the admissibility of the evidence in one or both of the states involved, while on the other hand, over-estimation of privacy interests could unnecessarily delay investigations by the use of formal channels when they were not needed.

2.7 There are many informal networks within the Commonwealth, such as the Commonwealth Network of Contact Persons. The Commonwealth context, with a shared legal tradition and a common approach to many matters of administration and agency procedures, makes those networks especially effective; within them, there is an easy understanding of requests for help.

Formal instruments for co-operation

2.8 Where more formal procedures are necessary, the requirements for co-operation may be set out in instruments of different types. These include memoranda of understanding between specialist agencies; obligations of co-operation derived from common membership of a regional organisation; instruments such as the Schemes adopted by Law Ministers which have a force that falls short of a treaty; Model Laws that have been adopted by both states concerned; and bilateral treaties and multilateral treaties open to states within a particular region or of potentially global effect.

2.9 In some cases, several modes of proceeding may be available. This is recognised in the text of the Budapest Convention, article 23 of which sets out general principles relating to international co-operation:

> The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Criteria for the selection of instruments

2.10 Although ad hoc arrangements may be very useful, a standing and binding arrangement that can be invoked as required is a very desirable part of the armoury of a state engaged in combating cybercrime. It is possible to set out some criteria to be used in assessing the various instruments that a state may choose to adopt, criteria also relevant to the Group’s task:

(a) the number of Parties, so that a multilateral instrument is to be preferred to a bilateral one especially where the existing or prospective Parties include states with which regular co-operation is likely to be needed;

(b) the comprehensiveness of the instrument in addressing the different aspects of an effective anti-cybercrime regime: the definition of criminal offences; procedural law; and mutual legal assistance and other forms of cross-border legal co-operation;

(c) the practicality and realism of the instrument's provisions: are they adequate to deal with the urgency of many international requests concerning cybercrime; and are they within the capacity of the intending Party;

(d) whether the instrument creates binding obligations on its Parties or is merely aspirational in character;

(e) the extent to which the instrument ensures that human rights and procedural safeguards are addressed;

(f) whether the instrument carries with it support mechanisms, such as those maintained by several international organisations which arrange meetings of Parties enabling those operating the instrument on a day-to-day basis to reflect upon its operation, develop guidelines as to best practice, and perhaps issue agreed statements as to the interpretation of any provisions in the instrument which experience has shown to be unclear.

2.11 Investigators should not necessarily assume that because an offence or investigation involves cybercrime elements, they must use an instrument specific to cybercrime. Instruments dealing with corruption, terrorism, and trafficking in narcotic drugs and psychotropic substances may all be applied to cyber-investigations where the underlying offences meet their respective substantive requirements. While not all cybercrime involves organised crime elements, much of it does, and in any case where cybercrime or other offences are 'serious crimes', 'transnational in nature' and involve an 'organised criminal group' the co-operation provisions of the United Nations Convention against Transnational Organized Crime (the Palermo Convention)[16]can be used if the countries involved are Parties to it. The Convention offences of participation in the activities of an organised criminal group (Article 5) and money-laundering (Article 6) may be particularly useful in scenarios where cybercrime and organised crime coincide. Article 29(1)(h) provides specifically for technical assistance in the techniques needed to investigate cybercrime based on the fact that the technologies are commonly used by organised criminal groups.

The Commonwealth Model Law

Genesis

2.12 The one instrument that has been developed specifically for Commonwealth member states is the Model Law on Computer and Computer-Related Crime, adopted by Law Ministers in 2002[17]. The initiative for the creation of the Model Law came from Law Ministers at their 1999 Meeting in Port of Spain, Trinidad and Tobago. At that Meeting, Law Ministers considered the impact of technology on various aspects of the law and one of the issues

[16] U.N. Convention against Transnational Organized Crime (Palermo Convention), A/RES/55/25, Annex I, in force 29 September 2003, U.N.T.S. 39574.

[17]Text available at:
http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf

highlighted for further consideration was computer crime. Ministers asked that an expert group be convened to consider the content of a model law on the basis of the work (then under way) of the Council of Europe on the Draft Convention on Cyber Crime. Topics that were specifically mentioned for consideration included criminalisation of various forms of computer abuse, admissibility of computer evidence, and investigation of computer-related crime.

2.13 An Expert Group duly prepared a draft Model Law which was considered by Senior Officials in 2001; it took into account a late draft of what was to become the Budapest Convention. Senior Officials decided that the Expert Group should be reconvened to review the draft model law in light of recent developments, in particular the changes made to the text of the Budapest Convention, since the original meeting of the group[18]. With a number of very limited exceptions, principally the omission of forgery, fraud and intellectual property offences from the listed offences, the Model Law is wholly compatible with the Budapest Convention, as indeed was the intention of the Expert Group. However mutual assistance provisions are not in the Model Law, as the Expert Group recommended revisions and additions to the Harare Scheme to deal specifically with cybercrime issues. This led in due course to the preparation of a revised Harare Scheme which was adopted by Law Ministers in 2011.

Contents of the Model Law

2.14 The Model Law is in three Parts. Part I contains in section 3 the important definitions of ‘computer data’, ‘computer system’, ‘service provider’ and ‘traffic data’ (in terms virtually identical to those in article 1 of the Convention) together with an additional definition of ‘computer data storage medium’ (a term not defined in the Convention but used in a number of its provisions). Section 4 of the Model Law deals with the jurisdiction of the enacting state in terms very similar to those of article 22 of the Convention.

2.15 Part II of the Model Law (sections 5-10) is concerned with substantive criminal law and the creation of offences. The offences relate to illegal access, interfering with data, interfering with a computer system, the illegal interception of data, illegal devices and child pornography using a computer system or a computer data storage medium. The provisions in the Model Law correspond to those in articles 2 to 6 and article 9 of the Convention. As already noted, the Model Law does not cover computer-related forgery or fraud (the subject of articles 7 and 8 of the Convention); the criminal law of most if not all Commonwealth member states would in any event criminalise such conduct.

2.16 Part III of the Model Law (sections 11 to 21) deals with ‘procedural law’. It contains provisions as to search and seizure warrants, the obligation to assist the police, recording and access to seized data, the production of data, the disclosure of stored traffic data, the preservation of data, the interception of electronic communications and the interception of traffic data, with provisions as to evidence, confidentiality and the limitation of liability together with the necessary definitions. Although the presentation of the material in the Model Law differs from that in the Convention, Part III of the Model Law corresponds in substance to the procedural law provisions in articles 16 to 21 of the Convention.

The Harare Scheme

2.17 In addition to the Model Law, the Commonwealth has the Harare Scheme. The latest revision of the Scheme was a lengthy process, involving an Expert Working Group meeting

[18] For details of the process, see LMM(02)17.

in 2007, consideration by Senior Officials at their Meetings in 2007 and 2008, consultation with governments with responses from 15 countries[19], a further Working Group Meeting of Senior Officials and Practitioners of Commonwealth countries meeting in January 2010 at which representatives at a high policy-making level from 22 countries attended[20]. After further work by a Drafting Committee and consideration by Senior Officials, the revised Scheme was adopted by Law Ministers in 2011.

2.18 The revision of the Harare Scheme in 2011 introduced material on taking evidence or statements from persons, including through live video link or other audiovisual means (paras. 1(5)(b)) and 14), the preservation of computer data (para. 20), the interception of telecommunications (paras. 22 and 23), the interception of transmission data (para. 24), the disclosure of intercept material (para. 25), surveillance, including covert electronic surveillance (para. 26), and the provision of subscriber information (para. 28). Although there are differences of language, for example 'transmission data' rather than 'traffic data', the provisions of the Harare Scheme correspond to article 27 to 34 of the Budapest Convention which set out mutual assistance procedures to be applied in the absence of applicable international agreements.

Recommendation concerning the Model Law and the Harare Scheme

2.19 The Group, having assessed the Model Law and the recently-revised Harare Scheme, finds that they continue to provide Commonwealth countries with a sound basis for the core provisions of their cybercrime legislation. There is no need at present for the revision of the Model Law. However, the Group recognises that, given the rapid evolution of cybercrime, some supplementation may in future be judged necessary. It would urge those Commonwealth countries which have not already adopted legislation based on the Model Law to consider doing so with a degree of urgency. The Group notes that an expert group convened by the Commonwealth Secretariat is preparing a Model Law to give effect to the revised Harare Scheme with a view to its adoption by Law Ministers in 2014.

2.20 Although the wide adoption of legislation inspired by the Model Law would be of great value at the national level, the international dimension can only be legally secure if it is dealt with in a binding international instrument.

The Budapest Convention

2.21 As noted above, the Commonwealth provisions, in the Model Law and the Harare Scheme, are closely related to the Budapest Convention[21]. The Convention was drawn up by the Council of Europe with the active participation of the United States, Canada, Japan, and South Africa, and was adopted by the Committee of Ministers of the Council of Europe in November 2001. It entered into force on 1 July 2004. The negotiation and adoption of the Convention itself was based on more than a decade of discussions in the UN, G-8, OECD and a range of other European and non-European fora which were also used in various ways as Commonwealth resources[22]. To some extent the typology of crimes and inventory

[19] Australia, Botswana, Cameroon, Canada, The Gambia, Ghana, Isle of Man, India, Jamaica, Malaysia, Montserrat, New Zealand, Singapore, South Africa and the United Kingdom.

[20] Australia, Bangladesh, Brunei Darussalam, Cameroon, Canada, The Gambia, Ghana, Jamaica, Kenya, Malawi, Malaysia, Mauritius, Mozambique, Namibia, Nigeria, Singapore, South Africa, Sri Lanka, Trinidad and Tobago, the United Kingdom, Tanzania and Zambia.

[21] Council of Europe Convention on Cybercrime, C.E.T.S. No.185, in force 1 July 2004. Text available at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm, See also (2002) 41 I.L.M. 282.

[22] For a summary of multilateral efforts prior to the Budapest Convention, see M A Sussmann, "The critical challenges from international high-tech and computer-related crime at the millennium", (1999)9 Duke Journal of Comparative and International Law, 451 at 476-88.

of investigative powers used in the Convention is based on broader international discussions on the nature of the problem, the need for principles which would remain neutral in the face of evolving technologies, and underlying issues such as the balances between the need for effective investigative powers and the need to protect human rights and national sovereignty.

2.22 By June 2013, it had been ratified by 39 countries, signed by an additional 12 countries, and a further 10 countries had been invited to accede. Many other countries including Commonwealth countries have used the Convention as a guide to cybercrime legislation. The Council of Europe believes that at least 140 States have undertaken reforms in recent years or are in the process of reforming laws regarding cybercrime; some 90 per cent of these have made or are making use of the Convention as a guideline or source.

2.23 The Budapest Convention is an open convention, so not limited to States which are members of the Council of Europe. Four Commonwealth countries (Australia, Cyprus, Malta and the United Kingdom) have ratified it, Canada and South Africa are signatories and Mauritius has been invited to accede.

Use especially within the Commonwealth

2.24 A study by the Council of Europe prepared for this Group[23] indicates that twenty-three Commonwealth countries[24] made use of the Budapest Convention and/or the Commonwealth Model Law in the preparation of national legislation and/or expressed an interest to become Party to the Convention. At present, 15 Commonwealth countries[25] seem to have legislation that is largely consistent with the standards of the Budapest Convention and are in a position to seek to accede. If they were to do so, and were Canada and South Africa to complete the ratification and Mauritius the accession process, the number of Commonwealth countries using the Convention as a framework for international co-operation would rise to 22 and the total number of Parties to 56. Nauru, Papua New Guinea, Solomon Islands, Tuvalu and Vanuatu have no legislation in place, but intend to prepare legislation based on the law of Tonga, itself drawing on the Budapest Convention and the Commonwealth Model Law. Information is not available from all Commonwealth countries[26] but only five are known not to have made use of the Convention or the Commonwealth Model Law in developing their national legislation[27].

Recommendation concerning accession

2.25 It is clear that many Commonwealth member states could satisfy the requirements for accession to the Budapest Convention. Should they do so? If the criteria identified above are considered, the multilateral nature of the Budapest Convention, the number of existing Parties, the comprehensive nature of its provisions, its proven practicality, its binding nature, and the existence of a support mechanism in that Parties to the Convention participate in the Cybercrime Convention Committee (T-CY) of the Council of Europe, the Group believes that Commonwealth countries should be encouraged to accede, where practicable, to the

[23] Available at hhttp://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2571_Commonwealth_cy_leg_v21_27Feb%20rev_final_CoE.pdf

[24] Antigua and Barbuda, Barbados, Botswana, Cameroon, Ghana, India, Jamaica, Kenya, Kiribati, Malaysia, Maldives, Mauritius, Namibia, New Zealand, Nigeria, Pakistan, St Vincent and the Grenadines, Samoa, Sri Lanka, Tonga, Trinidad and Tobago, Uganda, and Zambia.

[25] Antigua and Barbuda, Barbados, Botswana, Brunei Darussalam, Cameroon, Ghana, India, Jamaica, Malaysia, New Zealand, St Vincent and the Grenadines, Singapore, Sri Lanka, Tonga, Trinidad and Tobago.

[26] No information is available for Belize, Dominica, Mozambique, Rwanda, St Kitts and Nevis, St Lucia, Seychelles, Sierra Leone, Swaziland, The Gambia, Grenada, Guyana, Lesotho and Malawi.

[27] Bahamas, Bangladesh, Brunei Darussalam, Fiji and Singapore,

Budapest Convention[28].

2.26 This judgment is in line with the support for the Budapest Convention from bodies such as the European Union in its Stockholm Programme[29], and the Financial Action Task Force (FATF)[30]. In 2011, following the meeting of Commonwealth Law Ministers, the 'Quintet' of Attorneys-General from Canada, the United States, the United Kingdom, New Zealand and Australia met in Sydney to develop an action plan to address the significant and growing issue of cybercrime. In their Action Plan to Fight Cyber Crime (2011) they concluded that all Quintet countries should

> 'take steps to become parties to the Convention; consider how the Convention can assist Quintet countries to share information and help to solve practical issues, and promote the Convention as the key international instrument for dealing with cybercrime and use the Convention as a basis for delivering capacity building and awareness raising activities'.

Other international instruments

2.27 The Group is aware of a number of other instruments, proposed or already in existence, which address issues similar to those in the Commonwealth Model Law and the Budapest Convention. Some have, for geographical reasons, no relevance to Commonwealth member states. They include the Agreement on Co-operation in Combating Offences related to Computer Information drawn up in 2001 by the Commonwealth of Independent States (made up of states formerly within the Soviet Union); the Arab Convention on Combating Information Technology Offences of 2010; and the Shanghai Co-operation Organisation Agreement on Co-operation in the Field of International Information Security (2009). The European Union has been active in related areas, both in producing legislation[31] and in the establishment in 2013 of the European Cybercrime Centre in The Hague, but there are only three Commonwealth member countries (Cyprus, Malta and the UK) within the Union.

Recent developments: the Caribbean, the Pacific and Africa

2.28 Of much greater relevance to Commonwealth member countries are developments in the Caribbean, the Pacific and Africa.

2.29 In the Caribbean, with support from the ITU and the European Commission, the HIPCAR project developed a Model Policy Guidelines and a Model Legislative Text[32] on

[28] In view of the continuing work of the open-ended expert group on cybercrime established by the General Assembly, UNODC cannot endorse this recommendation.

[29] Section 4.4.4.

[30] FATF Recommendation 36 encourages States to ratify and implement other relevant international conventions, such as the Council of Europe Convention on Cybercrime, 2001.

[31] Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market; Council Framework Decision 2001/413/JHA combating fraud and counterfeiting of non-cash means of payment; Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector; Council Framework Decision 2005/222/JHA on attacks against information systems (with a proposal for a replacement Directive in 2010); and Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

[32] See http://www.itu.int/en/ITU-D/Cybersecurity/Documents/HIPCAR%20Assessment%20Cybercrimes.pdf and http://www.itu.int/en/ITU-D/Cybersecurity/Documents/HIPCAR%20Model%20Law%20Cybercrimes.pdf

Cybercrime/e-Crimes and Electronic Evidence intended for adoption within the region; six Commonwealth member states were involved[33].

2.30 In the Pacific similar work has been done under the ICB4PAC project sponsored by the ITU and the European Union, which involves eight Commonwealth jurisdictions[34] in developing model legislation[35].

2.31 There have been a number of developments in Africa. The African Union (which has 53 member states of which 19 are members of the Commonwealth[36] has a Draft Convention on the Establishment of a Legal Framework Conducive to Cybersecurity in Africa but this has not yet secured the approval of the meeting of Heads of State or Government of the Union. Within the various regional groupings of African states, the Southern African Development Community (with 11 Commonwealth members[37]) has a draft Model Law on Computer Crime and Cybercrime[38] produced with the assistance of the ITU/European Union sponsored HIPSSA project; the Common Market for Eastern and Southern Africa (with 8 Commonwealth members) has a draft Model Bill on Cybersecurity; and the Economic Community of West African States (with 4 Commonwealth members[39]) has a draft Directive on Fighting Cybercrime within ECOWAS.

Recommendation concerning these other instruments

2.32 Some at least of these instruments were designed to be compatible with the Budapest Convention; all could be of value in securing more effective action against cybercrime. It is important that instruments designed to enhance co-operation within a given region should not be so framed as to have the unintended consequence of making co-operation beyond the region more difficult: criminals do not respect boundaries (and indeed exploit any opportunities divergent legislation may present). Subject to that, the Group believes that Commonwealth countries should be encouraged to consider becoming Party to any regional and/or international cybercrime conventions and participating in other initiatives to ensure co-ordinated action against cybercrime or, where possible, utilise them as models to guide the development or enhancement of their existing domestic frameworks.

On-going UN Work

2.33 The Group was kept informed about the work of the UN open-ended intergovernmental expert group on cybercrime convened pursuant to General Assembly resolution 65/230. The Group noted that there had been broad support for capacity-building and technical assistance, and for the role of UNODC in that regard. At its twenty-second session in April 2013, the UN Commission on Crime Prevention and Criminal Justice requested the expert group to continue its work towards fulfilling its mandate. The Commission also emphasised the need to reinforce technical assistance and capacity-building activities, based on national needs, for the prevention, prosecution and punishment of the use of information

[33] Barbados, Grenada, Jamaica, St Kitts and Nevis, St Lucia and Trinidad and Tobago (together with Haiti).

[34] Cook Islands, Fiji, Kiribati, Niue, Papua New Guinea, Samoa, Tuvalu, and Vanuatu.

[35] See http://www.itu.int/en/ITU-D/Cybersecurity/Documents/ICB4PAC%20Assessment%20Eletronic%20Crime.pdf and http://www.itu.int/en/ITU-D/Cybersecurity/Documents/ICB4PAC%20Skeleton%20Electronic%20Crime.pdf

[36] Botswana, Cameroon, The Gambia, Ghana, Kenya, Lesotho, Malawi, Mauritius, Mozambique, Namibia, Nigeria, Rwanda, Seychelles, Sierra Leone, South Africa, Swaziland, Tanzania, Uganda and Zambia.

[37] Botswana, Lesotho, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Swaziland, Tanzania and Zambia.

[38] See http://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf

[39] The Gambia, Ghana, Nigeria and Sierra Leone.

technologies for criminal purposes.[40]

Other components of a response to cybercrime

2.34 National legislation and international instruments are essential but are not enough. Commonwealth countries must develop and implement all other components of an effective response both to cybercrime, and to the challenges related to the recognition, collection, preservation and admissibility of electronic evidence in relation to any type of criminal activity. These may include: (a) national strategies that co-ordinate government departments and other agencies; (b) appropriately resourced and trained prosecutors, law enforcement personnel and judiciary; (c) efficient response systems such as 24/7 networks; and (d) mechanisms and protocols for co-operating with Communication Service Providers (CSPs) and the private sector as a whole. Cyber security is a distinct but very important issue and much can be done in preventive and defensive work, including a range of regulatory frameworks and systems.

Resources and capacity-building

2.35 All this requires adequate resources and capacity. Part 3 of the Report examines issues relating to training, but here we identify some of the sources of assistance in capacity-building. The following paragraphs mention some of the organisations whose mandate includes cybercrime issues, and give rather more detail about those with a specifically Commonwealth location or focus and the work of the Commonwealth Secretariat and its programmes[41].

Commonwealth bodies

The Commonwealth Secretariat

2.36 The Commonwealth Secretariat and its Divisions carry out mandates given by CHOGM and the relevant meetings of Ministers. In delivering on its mandates, the Secretariat has co-operated closely with international, regional and national organisations to deliver efficient technical assistance to develop the practical skills of investigators, prosecutors and judges. The comparative advantage of the Secretariat lies in the close connections it has with criminal justice officials in member countries, particularly in the small jurisdictions. The Secretariat has supported and assisted the formation and continued activities of the Caribbean Prosecutors Association, and the Pacific Prosecutors Association, has held or supported several regional judicial fora, and engages closely with similar regional networks relevant to other member countries. The Secretariat has also supported the foundation of the Africa Anti-Corruption Centre in Botswana. The contacts created through these regional networks allow the Secretariat to engage closely with practitioners to discover the difficulties faced by a jurisdiction on the ground, and develop technical assistance accordingly. In delivering technical assistance, the Secretariat has observed the importance to member countries of providing criminal justice officials with the practical skills to tackle cybercrime. As such, cybercrime has formed a key part of many of the Secretariat's programmes.

Commonwealth programmes and initiatives

[40] U.N. Commission on Crime Prevention and Criminal Justice, Resolutions 22/7 (on-going work of expert group) and 22/8 (promotion of technical assistance and capacity building). See Report of the Commission at its 22nd Session, E/2013/30, E/CN.15/2013/27, Chapter 1 Part D.

[41] Information about the work of 2Centre and GSPEN is given in Part 3 of this Report.

2.37 The *Commonwealth Connects* programme is a vehicle for technology and knowledge transfer in areas such as eGovernment Services, Telecommunication Regulation and related activities having a bearing on national, social and economic development. In 2002 a Commonwealth Expert Group on Information Technology produced a report: *A Commonwealth Action Programme for the Digital Divide* whose recommendations were endorsed by the CHOGM in that year. A further report in 2004 set out a structure for a programme, with the Commonwealth Secretariat as co-ordinator and relevant Commonwealth agencies as key delivery organisations. A steering committee under the chairmanship of the Foreign Minister of Malta developed the proposals and the programme was formally launched in August 2006. Its work includes promoting the development of national ICT strategies; sharing ICT resources for capacity building; and supporting pan-Commonwealth ICT-based initiatives.

2.38 The *Commonwealth Internet Governance Forum (CIGF)* was established by the Commonwealth Secretariat in 2010 to encourage greater participation from Commonwealth member states on policy issues and discussions related to Internet Governance, including those under the aegis of the UN Internet Governance Forum. It has compiled lists of resources on child protection and cyber security.

2.39 In 2011, the CIGF promoted the idea of a *Commonwealth Cybercrime Initiative* (CCI). The aim was to assist Commonwealth member states to implement a programme of measures including an appropriate legal framework for responding to cybercrime and acquiring cyber evidence. It was recognised that while the Commonwealth benefited from a common institutional backdrop, traditions, language and values, as an institution it had little by way of specialist capacity or funds for such a venture. Fundamental to the idea of the CCI was that it could act as a catalyst and broker working with the broad alliance of partners, each partner having a unique contribution to make. The CCI is thus an innovative umbrella type construct, comprising a consortium of partners including states, organisations, networks, NGOs and individuals who are able to offer their expertise and capacity to develop projects to assist jurisdictions within the Commonwealth. The list of current partners indicates its potential[42].

2.40 The purpose of the CCI is to:

(i) to conduct independent, holistic needs assessments for developing Commonwealth states in terms of their capacity to address the threat from cybercrime (covering all components from national strategy and legal framework to CIRT and public awareness);

(ii) further a needs assessment, and where the necessary level of state commitment is identified, to co-ordinate comprehensive, long-term programmes of assistance, harnessing the motivations of governments, international organisations and the private sector; and

[42] TheAnti-Phishing Working Group (APWG), Caribbean Telecommunications Union (CTU), Centre for Internet Safety at the University of Canberra (CIS), Children's Charities' Coalition on Internet Safety (CHIS), Commonwealth Business Council (CBC), Commonwealth Secretariat, CTO, COMNET, Council of Europe, CyberEthics Cyprus, DiploFoundation, European NGO Alliance for Child Safety Online (eNACSO), Global Prosecutors' e-Crime Network (GPEN), Institute for Security Studies, South Africa (ISS), International Center for Missing and Exploited Children (ICMEC), ICSPA, ITU, ICANN, Internet Watch Foundation (IWF), Interpol, Kenya Communications Commission, Secretariat of the Pacific Community, Serious Organised Crime Agency (SOCA) and UNODC.

(iii) to serve as a forum for states and international organisations and others to co-ordinate their capacity building work across Commonwealth states; and to discuss, debate and refine capacity-building methodology.

2.41 The CCI was endorsed by CHOGM in 2011. Because of the sequence of meetings, the proposal was not considered by Law Ministers at their Meeting earlier that year. Funding was provided by the Commonwealth Secretariat and the Governments of Malta and the United Kingdom to provide the necessary resources to give practical reality to the Initiative, by engaging with potential partners and securing their collaboration, and by establishing its structures and working methods. For the initial period, until 30 June 2013, this task was undertaken by COMNET, an independent Foundation established in the mid-90s, as a joint initiative of the Commonwealth Secretariat and the Government of Malta, where it is based. COMNET has a record of work amongst Commonwealth and other developing countries; its mission is to help realise the transformational potential of ICT for development, amongst such countries.

2.42 In 2012, its first year of operation, the CCI responded to a major request from Ghana and had formal requests for assistance from The Gambia, Kenya, Maldives, Trinidad & Tobago, and Uganda, together with expressions of interest from a number of other Commonwealth countries. It also established its working methods, described below.

2.43 This is a strong record for a very new Initiative, However, as it became clear that the CCI's governance structure was preventing the participation of some prospective partners and that funding for administration as opposed to project work would not be forthcoming once the initial phase was over, the decision was taken in May 2013 that the management of the CCI should pass from COMNET to the Commonwealth Secretariat itself. This was in no way a reflection on the quality of COMNET's work during the initial phase, which showed both energy and creativity.

2.44 The Commonwealth Secretariat, which already deals with cybercrime issues as part of its work on such topics as money-laundering and terrorism, seems a natural home for the CCI, which will benefit from the Secretariat's established financial management and procurement procedures. The United Kingdom Government is committed to the Initiative and has agreed to assist the Commonwealth Secretariat with administrative support for the work of the CCI, initially through SOCA and its successor the National Crime Agency (NCA).

2.45 It is not intended that the CCI's working method, developed during the first year of its operation, will change under the new administrative arrangements. Requests for assistance will be made to the Commonwealth Secretariat and considered by the CCI's Cybercrime Executive Management Committee (CEMC), formerly the Management Group, composed principally of representatives of governments, the two relevant Divisions of the Commonwealth Secretariat (GIDD and LCAD), and a representative of SOCA/NCA. The Committee is responsible for the overall policy of the CCI and will have to prioritise requests for assistance. If following a preliminary study it decides to act on a request, it sends a team of experts to the state concerned to conduct a Gap Analysis and Needs Assessment using a checklist developed by the Initiative, and to make a Needs Assessment Report. In a few cases, such assessments have been conducted by a CCI partner agency (or a group of such agencies), but the Group notes that most teams have been made up of individual experts with their expenses covered by a Projects Fund established within the CCI.

2.46 The Needs Assessment Report once agreed with the requesting state is shared with the CCI's Operations Consortium of agencies, organisations and individual experts willing to contribute to its work; it meets physically about twice a year but information is also exchanged through its virtual network. It may identify a range of different types of assistance needed by the state visited. There is of course close consultation with that state's government, a process which necessarily takes some time. Many aspects of the assistance identified, and agreed with the government, will fall within the mandate and expertise of a CCI partner, and will be undertaken by the partners concerned under their usual procedures in terms of funding and responsibility. Otherwise the CCI and its partners may be able to assist in identifying funding and/or expertise from elsewhere. The CCI will also assist the requesting state in co-ordinating the various pieces of work to ensure an effective outcome.

2.47 This methodology can be seen at work in the first project undertaken by the CCI, in Ghana. In January 2012 the Ghana Ministry of Communications requested assistance from the CCI in developing a cyber security strategy and the establishment of a national CIRT. In the following month the CCI sent out a team from SOCA, ITU and ICSPA to conduct a Needs Assessment. In April 2012, the CCI submitted a Needs Assessment Report to the Minister and in August 2012 the Minister submitted a further and more developed request for assistance in line with the Report’s recommendations. This was shared with the partners with the result that offers of assistance and/or funding were identified against all elements of the request. In January 2013 the CCI sent the proposal to the Minister and in April 2013 a meeting took place in which the proposals were discussed and agreed. These included a University Partnership to promote joint research and training programmes; assistance in establishing a CIRT with ITU; assistance from SOCA and the CPS in conducting a resource and training needs analysis for the criminal justice system; and a scheme in which the IWF will provide a reporting line for child abuse images. More recently Needs Assessment teams have been established to examine requests from Kenya, Trinidad and Tobago, The Gambia and Uganda.

2.48 The Group finds the innovative methodology adopted by the CCI to be one likely to secure co-ordinated and comprehensive assistance to a Commonwealth member state. It should help avoid the duplication of effort sometimes found, with different agencies responding to requests by different departments of the same government. It should ensure the establishment and implementation of a national strategy that addresses all issues in a sustainable fashion. It does of course depend on the continued goodwill of the partner agencies as well as clear and focused management, but the Group has no reason to doubt that both will continue to be found.

2.49 Law Ministers have not previously had an opportunity to consider the work of the CCI. The Group recommends that Law Ministers should follow the lead of CHOGM in endorsing the Initiative and should ensure that their colleagues in government are aware of it and should, as appropriate, facilitate its work.

Commonwealth Telecommunications Organisation

2.50 Within the Commonwealth, the *Commonwealth Telecommunications Organisation (CTO)* is an international organisation, established in its present form in 1967, co-operating with but independent of the Commonwealth Secretariat. Its membership includes all member states of the Commonwealth and ICT sector members including government departments or regulators, private sector companies, civil society organisations, and other entities that share the CTO’s objectives. According to its Constitution, the CTO has four main purposes: (a) to support the development and use of ICTs within the Commonwealth and beyond; (b) to promote the provision and use of ICTs to meet the needs of members, to support development in member countries, and to ensure the inclusion of marginalised people; (c) to promote effective co-operation and partnership amongst its members and other organisations; and (d) to develop and implement activities to promote the above three objectives. The CTO delivers training and capacity building, carries out research and consultancies and organises international events and conferences.

Non-Commonwealth bodies

2.51 Amongst the non-Commonwealth organisations, the *United Nations Office on Drugs and Crime (UNODC)* is the lead entity within the United Nations structure for drug control, crime prevention and criminal justice matters at the global level. It acts as the Secretariat to the United Nations Crime Congress on Crime Prevention and Criminal Justice, held at five-year intervals, and the Commission on Crime Prevention and Criminal Justice, and is the guardian of a number of significant UN Conventions, including the Organized Crime Convention and the Convention against Corruption. The UNODC Global Programme on Cybercrime provides technical assistance to developing countries to prevent and combat cybercrime. This includes assistance in respect of international co-operation, capacity building, legislative reform, training programmes on investigative techniques and electronic evidence, cybercrime prevention activities and awareness raising, and enhanced national research and analysis on cybercrime. UNODC is based in Vienna and operates in more than 150 countries around the world through its network of field presences.

2.52 The *International Telecommunications Union (ITU)* is also within the United Nations structures as the specialised agency for information and communication technologies. It is based on public-private partnership, and has a membership of 193 countries and over 700 private-sector entities and academic institutions. Its headquarters are in Geneva and it has 12 regional and area offices around the world. It has published *Understanding Cybercrime: A Guide for Developing Countries* and mention has already been made of the ITU-European Commission projects to assist Caribbean, sub-Saharan Africa and Pacific states in developing cybercrime legislation.

2.53 Mention should also be made of the *Internet Governance Forum (IGF)*, unusual in being an open forum which has no formal membership. It was established by the World Summit on the Information Society in 2006. It has a UN mandate[43] to serve as a neutral space for dialogue, a means of identifying issues to be addressed by the international community and of shaping decisions that will be taken in other forums. It has a small Secretariat in Geneva.

2.54 The *Internet Corporation for Assigned Names and Numbers (ICANN)* is a private sector, non-profit global organisation that co-ordinates the Internet's identifier systems. It provides training to Domain Name System (DNS) operators in all geographic regions.

2.55 The *International Cyber Security Protection Alliance (ICSPA)* is a non-profit business-led coalition of national and multinational companies which recognises the need to provide additional resources and support to law enforcement officers around the world in the fight against cybercrime. Its *Project 2020: Research Project on the Practical Implications of Cybercrime* is an international consultation into the future of cybercrime seeking to anticipate developments in the field.

2.56 The *International Criminal Police Organization (ICPO-INTERPOL)* has a cybercrime programme which includes a global list of contact officers available 24/7 for cybercrime investigations (the list contained 134 contacts at the end of 2012); the identification of emerging threats; and the provision of a secure web portal for accessing operational information and documents.

[43] General Assembly Resolutions 60/252 of 27 March 2006 and 65/141 of 20 December 2010.

2.57 The *Council of Europe* is the senior European regional organisation with 47 member countries. It has long taken an active role in crime matters, notably through its European Committee on Crime Problems. Apart from the Budapest Convention, and its Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, it has conventions on Corruption; on the Prevention of Terrorism; on Money Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, on the Sexual Exploitation and Sexual Abuse of Children, and a wide range of treaties on international co-operation in criminal matters.

2.58 Other regional bodies have recognised the importance of cybercrime, for example in the Regional Crime and Security Strategy adopted by the Conference of Heads of Government of *CARICOM (the Caribbean Community)* in February 2013, and in the deliberations of the Committee of Representatives of Governments and Administrations of the *Pacific Community* in 2011.

2.59 There are close links between many of these bodies and a number have formal bilateral memoranda of understanding to avoid duplication.

The future role of the Commonwealth Secretariat

2.60 The Group recommends that the Commonwealth Secretariat should in managing the CCI and in its more general work on such matters as money-laundering and terrorism, without necessarily duplicating effort, continue its role in the development of capacity within the Commonwealth to combat cybercrime, and continue to collaborate with other international and regional organisations to provide and/or facilitate technical assistance in this field to member states.

2.61 There is a growing body of expertise in combating cybercrime, but for the reasons set out in Part 1 it must be kept up to date, and duplication must be avoided. The Group believes that there would be value in a virtual community within the Commonwealth to share information and exchange views and act as a repository of best practices and lessons learned. The Commonwealth Connects programme, already used in the context of the CCI, could play a role in this virtual community and the possibility of working in collaboration with other organisations should always be kept in mind. Close co-operation within the Commonwealth should never imply barriers to co-operation with countries and organisations with regional or global mandates.

RECOMMENDATIONS

5. The Group recommends that Commonwealth countries should be encouraged to bring their laws into line with the Commonwealth Model Law and the Harare Scheme (as revised).

6. The Group recommends that Commonwealth countries should be encouraged

(i) to accede, where practicable to the Budapest Convention[44]; and/or

(ii) where they can do so without prejudicing other forms of co-operation, to consider becoming Party to any regional and/or international cybercrime conventions and participating in other initiatives to ensure co-ordinated

[44] In view of the continuing work of the open-ended expert group on cybercrime established by the General Assembly, UNODC cannot endorse this part of the Recommendation.

action against cybercrime;

7. The Group considers that there is no immediate need to revise the Commonwealth Model Law, but given the rapid evolution of cybercrime, some supplementation may in future be judged necessary.

8. The Group recommends that Commonwealth countries should also be encouraged to develop and implement all other components of an effective and adequately resourced response to cybercrime, and the challenges related to the recognition, collection, preservation and admissibility of electronic evidence in relation to any type of criminal activity.

9. The Group recommends that the Commonwealth Secretariat should in managing the Commonwealth Cybercrime Initiative and in its more general work on such matters as money-laundering and terrorism, without necessarily duplicating effort, continue its role in the development of capacity within the Commonwealth to combat cybercrime, and continue to collaborate with other international and regional organisations to provide and/or facilitate technical assistance in this field to member states.

10. The Group recommends that Law Ministers should follow the lead of CHOGM in endorsing the Commonwealth Cybercrime Initiative and should ensure that their colleagues in Government are aware of it and should, as appropriate, facilitate its work.

11. The Group recommends that the Commonwealth Secretariat, in collaboration with other organisations and without duplication, should establish a virtual community to share information and exchange views, and a repository of best practices and lessons learned

PART 3: THE WORKING GROUP COLLABORATE WITH OTHER INTERNATIONAL AND REGIONAL BODIES WITH A VIEW TO IDENTIFYING BEST PRACTICE, EDUCATIONAL MATERIAL AND TRAINING PROGRAMMES FOR INVESTIGATORS, PROSECUTORS AND JUDICIAL OFFICERS

3.1 Training is an essential element in the building of capacity against cybercrime, but it is important to bear in mind that there are no ‘one size fits all’ solutions. What is appropriate depends on a number of considerations:

(a) as with other elements of anti-cybercrime strategies, training elements need to be proportionate and responsive to the needs of each individual country. This will depend on factors such as the degree of national reliance on technology and the amount of institutional and investigative capacity required and so the extent of training needed to bring existing personnel up to an appropriate level;

(b) training elements are also closely linked to other strategic elements, especially the development of appropriate legislation;

(c) cybercrime occurs primarily within infrastructures and digital environments created and operated by the private sector, which requires the mobilisation of private sector resources in developing and delivering training;

(d) most cybercrime occurs primarily within infrastructures owned by the private sector, which require the mobilisation of private sector resources in developing and delivering training;

(e) as has been emphasised in Part 1, cybercrime is increasingly transnational in nature. International co-operation is a highly desirable feature of training and is likely to make co-operation easier and more effective in actual practice;

(f) while many areas of training focus on cybercrime *per se*, training in evidence needs to take into account the fact that evidence of almost any type of crime may be found in electronic form. Adequate resources need to be put in place to enable governments to ensure that the standards and procedures adopted will enable the transfer of information, intelligence and most importantly, evidence, in acceptable forms to both sending and recipient jurisdictions.

3.2 Co-ordination of training activities is essential to avoid a continuation of the situation where donors deliver training that they consider to be important, without reference to the needs of the audience or the work of other donors. This wastes scarce resources as well as providing, in many cases, training that is not relevant to the audience. This Part may provide some assistance in identifying an approach to the considered assessment of training needs and in identifying a platform through which future training activities may be co-ordinated in an effective manner.

Requirements for skills and knowledge

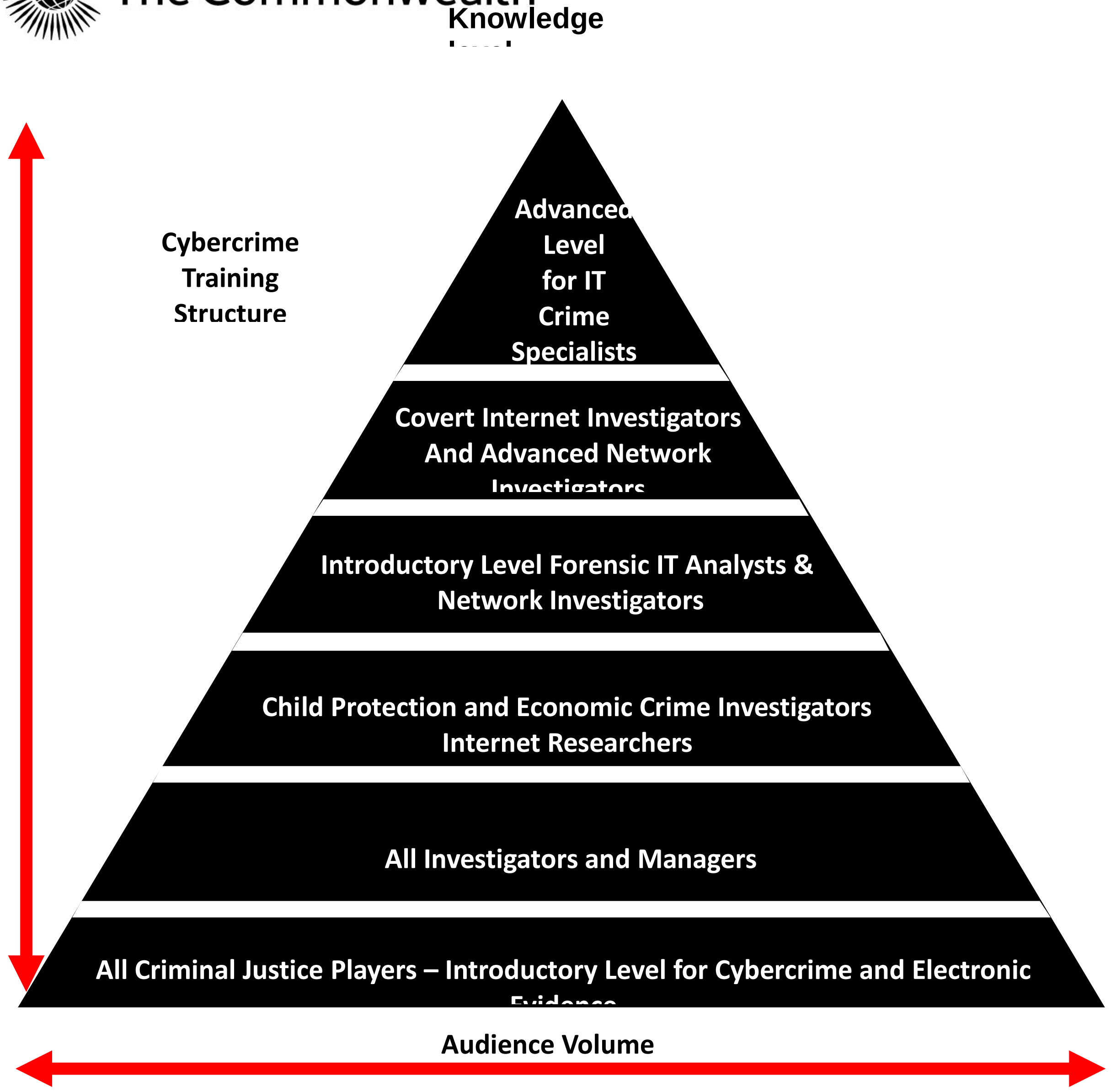
3.3 As noted in Part 1, the speed of change in technology and its impact on crime are increasing rapidly. The knowledge and skills needed to deal effectively with cybercrime and electronic evidence are manifold and constantly challenged by offender innovations. There is some need for highly trained, skilled and specialised experts, but the extent to which information and communications technologies have become pervasive is such that all criminal justice actors should have at least a basic understanding of such technologies and related problems. At this basic level, the widest audience needs to be able to recognise and deal with the evidence that computers and other digital media may provide in any type of investigation and prosecution. At this level, it should be a fairly simple exercise to introduce elements of relevant training into existing programmes for all within the criminal justice system.

3.4 Beyond a basic general awareness and understanding, there are many different needs. These depend on factors which include the role of each individual, the nature of the institution in which he or she works, and his or her functions within the organisation, the size of the organisation, the volume of cybercrime cases it handles and the degree of specialisation of its personnel (some states choosing to establish dedicated cybercrime units). Depending on these factors, training needs may be focused more on investigative law or evidence law, or on elements such as forensics or the technical skills needed to locate, preserve and seize digital evidence.

3.5 In addition to broad-based general skills training and the training of specialised personnel, specific cybercrime elements may also need to be developed and incorporated into training programmes for specialists in other areas such as organised crime, money laundering or financial and economic crime. In some cases training may be multidisciplinary and be offered to the whole range of criminal justice actors but in other scenarios it may need to be designed and delivered to each professional or institutional group separately. A further consideration, especially for smaller agencies, will be whether training and skills development is intended to be “top-down” and self-sustaining or not. In a very large agency, a cybercrime group, once established, may be largely self-sustaining, able to keep abreast of new developments in technologies and criminal methods, and train newcomers as needed. In small agencies and where case volumes are lower, ongoing training support – sending newcomers abroad for training for example – may be more effective.

3.6 At the highest level, the knowledge and skills that are needed by those tasked with investigating electronic attacks on critical national infrastructure and other targets, as well as those dealing with the analysis and interpretation of electronic evidence, irrespective of the crime type, are far greater than those engaged in more traditional law enforcement related work. Here a clear plan will need to be developed to meet the varying needs of each individual. The numbers of people requiring this high level training will vary from country to country, and in some smaller countries may even be in single figures. Where the number of trainees does not support a national approach, it may be necessary to look at options, such as regional training, since there is no less a requirement for staff to be adequately trained just because they are few in number. A structured approach has to be developed in order to identify these issues in each country.

3.7 An example of the levels within such a structure is given in the following chart which principally relates to the law enforcement community; however the principle that the higher the knowledge level required, the lower the number of staff that need to be trained can equally be applied to all actors in the criminal justice system.


Knowledge
Level
Cybercrime
Training
Structure
Advanced
Level
for IT
Crime
Specialists
Covert Internet Investigators
And Advanced Network
Investigators
Introductory Level Forensic IT Analysts &
Network Investigators
Child Protection and Economic Crime Investigators
Internet Researchers
All Investigators and Managers
All Criminal Justice Players – Introductory Level for Cybercrime and Electronic
Evidence
Audience Volume

Existing Commonwealth resources

3.8 It would not be feasible to include in this Report a comprehensive catalogue of training providers and of their products and good practice material. Such a listing would inevitably be incomplete and would almost immediately be out of date. Accordingly, this report mentions some of the main providers but concentrates more on setting out a model for training, which takes advantage of the relatively homogeneous nature of the Commonwealth and the commonalities between its judicial systems.

Commonwealth Secretariat

3.9 The Secretariat has a history and experience of delivering tailor-made technical assistance to member countries. It has close connections with criminal justice officials at all levels, particularly in small Commonwealth jurisdictions, and has worked closely with national, international and regional organisations to encourage the development of regional networks between investigators, prosecutors and judges. The Secretariat has adopted a holistic approach in carrying out its criminal justice mandates. A core strategy has been the holding of regional programmes in order to address the common difficulties faced in the areas covered by the Secretariat's mandates (including economic and financial crime, international co-operation, anti-money laundering and countering the financing of terrorism), followed up by national programmes tailored to the particular challenges of one jurisdiction. This approach has enabled the Secretariat and member countries to build relationships with partners across national borders and encourage networking; the Secretariat has supported the formation and continued activities of bodies such as the Pacific Prosecutors Association and the Caribbean Prosecutors Association.

3.10 The challenges presented by electronic evidence and cybercrime have been the subject of papers and discussion at those bodies' conferences and at other workshops organised in collaboration with national governments. For instance, the Pacific Prosecution Conference held in Samoa in May/June 2010 had 'The Impact of Technology on the Commission, Detection and Prosecution of Crime' as its main focus. In collaboration with the Governments of Bermuda and Maldives respectively, the Secretariat organised Hi Tec Crime training workshops for Commonwealth Caribbean member countries[45] in August 2009 and in the Maldives in June 2010. In each case, the delivery of training was undertaken by the Global Prosecutors E-Crime Network (GPEN) of the International Association of Prosecutors (IAP).

3.11 A number of the international organisations already mentioned in Part 2 of this report have considerable experience in the provision of training courses and some courses have been developed at a national level in countries which have been dealing with cybercrime and electronic evidence for many years. It would be possible to create a programme that will take advantage of such courses and also address gaps in provision.

Other resources

Council of Europe

3.12 Among the resources provided by the Council of Europe are *Cybercrime training for judges and prosecutors: a concept* (2009) (the purpose of the concept is to help judicial training institutions develop training programmes on cybercrime and electronic evidence for judges and prosecutors and to integrate such training in regular initial and in-service training, i.e., to institutionalise it); *Training manual on cybercrime for judges* (2010) (this provisional training manual is designed to provide the material for an introductory training course, which should last for a minimum of two days); and *Electronic Evidence Guide* (2013) (this guide provides advice and guidance for all criminal justice actors on dealing with electronic evidence).

3.13 Within the joint European Union and the Council of Europe regional project CyberCrime@IPA, more specific training materials have been developed aimed at implementing the Concept Paper, *Training on Cybercrime and Electronic Evidence*. There are also Council of Europe training programmes for criminal justice actors, for example a First Responder course, an Introductory cybercrime and electronic evidence course, and an Advanced cybercrime and electronic evidence course; a 3-day introductory training course for judges and prosecutors – consisting of a full training pack that may be adapted for use in country (2012); a 2-day scenario based interactive training course for judges and prosecutors – consisting of a full training pack that may be adapted for use in country (2012);

[45] Anguilla, Antigua, Bahamas, Barbados, Belize, British Virgin Islands, Dominica, Guyana, Jamaica, Montserrat, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Trinidad and Tobago, Turks and Caicos Islands and Cayman Islands.

and a 2-day training skills development module that is designed to enhance the skills of trainers who will deliver the previously listed 2 courses in country (2012).

2Centre

3.14 The Study, *Co-operation between law enforcement, Industry and Academia to deliver long term sustainable training to key cybercrime personnel,* undertaken in 2008 deals with many of the issues that are covered by this Group. The study made recommendations to improve the development and delivery of sustainable; standards based, scalable training to the law enforcement community. This report led to the development of the EC funded project to create national centres of excellence in cybercrime training, research and education (2CENTRE). A number of national centres have been created in Belgium, Estonia, France, Germany, Greece, Ireland, Romania, Spain, and the United Kingdom. Others are in the process of being formed. It is not suggested that this is a perfect fit for Commonwealth countries; however it may be of interest to examine work that has been carried out[46].

GPEN

3.15 GPEN operates under the auspices of the International Association of Prosecutors (IAP). It provides password access on the IAP website for all IAP members (individual members and authorised officers of organisational members) to a secure system through which it can enhance international co-operation in the e-crime arena of member countries (by identifying contacts and exchanging information); reduce duplication of training and realise significant cost savings as countries will no longer need to devise their own training material from scratch; develop appropriate training courses to train prosecutors who will be able to train their colleagues; encourage the sharing of best practice and dissemination of lessons learnt; improve the exchange of crucial information and data quickly and efficiently, especially in relation to crimes with an inter-jurisdictional dimension; and encourage all jurisdictions to develop a co-ordinated approach for dealing with e-crime that supports effective prosecutions and promotes the principles of the Budapest Convention.

3.16 The GPEN initiative is developing a database of e-crime prosecutors from around the world; a forum/message board for the exchange of queries and advice; a virtual Global E-crime Prosecutors College, a database of e-crime training courses and presentations; a library of e-crime material, i.e. legal guidance; and an industry page for partners of the International Association of Prosecutors (IAP).

An approach for training in the Commonwealth

3.17 Training cannot be dealt with in isolation but it is an essential part of an overall solution. Many organisations have committed resources to the development of strategies for addressing cybercrime and the development of legislation. It is hoped that they will appreciate the need for the financing of training initiatives.

3.18 A model which draws on the experience already gained and that would suit Commonwealth countries in planning their approach to training would have a number of stages:

(i) an examination of the legislation in place to assess whether there are adequate substantive and procedural provisions to enable effective action against cybercrime and to allow the admission of electronic evidence in judicial proceedings;

[46] See www.2centre.eu/sites/default/files/LEA-ISP%20Training%20Strategy%20v1.0.pdf

(ii) enquiry as to the existing technical capacity and the training strategies and programmes already in place to support criminal justice actors, taking into account whether specialised cybercrime units exist;

(iii) enquiry as to capacity and practice in international co-operation, industry relations and tackling illegal financial transactions on the Internet.

(iv) The answers to these questions would then inform the supportive response that could be provided to countries in conjunction with local or regional project teams. The key component of these training projects would be to ensure that sustainable solutions were provided and that each country took responsibility for providing continuing support and education that would outlive the projects.

3.19 It is important to note that some work will often have been done on these issues though not necessarily from a training perspective. For example, an account has already been given of some of the regional initiatives taken forward by the ITU which have produced relevant material on existing legislation; wasteful duplication of work already done must be avoided. A draft template for conducting a training needs analysis and syllabus was developed by the Group and is available from the Commonwealth Secretariat.

3.20 The implementation of the approach outlined here will require, depending on what has already been put in place, the conduct of training needs analyses, the development of training strategies, the development and delivery of training programmes for criminal justice actors, including ‘train the trainer’ programmes. Where training materials are developed on an international or regional basis, it is important that they should be given to the countries concerned as a resource to include in their own national programmes.

3.21 The sustainability of training programmes is fundamental to success and this could be supported by the development, wherever possible, of regional training centres for criminal justice actors. Such a centre might be based within a university or professional training institution but should have multiple stakeholders, with support from the private sector as well as government and international or regional organisations.

Practical recommendations

3.22 Experience of working in various jurisdictions suggests that a training needs analysis would find that current initial and in-service training programmes varied significantly in their ability to provide criminal justice actors with the level of knowledge required to deal with cybercrime and electronic evidence. The Group believes that the training of officials tasked with responding and reacting to its effect should be considered a priority.

Initial training

3.23 In countries where initial training is practical training ‘on the job’, it is recommended that part of such training is related to cybercrime and electronic evidence. In some countries, certain groups within the category of ‘criminal justice actors’ may at present receive no initial ‘on the job’ training; judicial officers are an example. In such cases, an opportunity should be created, through mentoring by fellow judges, or by the organisation of one-off training courses on the issue.

3.24 In countries where initial training is provided by criminal justice training institutions their curriculum should contain as a minimum one basic level module on cybercrime and electronic evidence. These should, in addition, be covered in modules covering substantive and procedural law. Optional modules for advanced knowledge on cybercrime and electronic evidence should be offered.

In-service training

3.25 In-service training institutions should offer at least one basic level module on cybercrime and electronic evidence in order to impart basic knowledge to criminal justice actors who had no such training in their initial training.

Training materials

3.26 The Group has had very much in mind the need to avoid wasteful duplication of effort. There would be such duplication were every country or every training institution to develop its own materials. Training materials need to be developed which reflect common international standards and good practice. While criminal justice actors need to be trained in the application of local national legislation, it is nevertheless possible to develop standardised training materials in a way that leaves sufficient room to take into account local national systems and legislation. Funding to develop training materials, including where appropriate on-line courses, would be a good use of resources. This work need not be done ‘from scratch’: materials already in use could be evaluated and built upon.

3.27 The aim should be to develop standardised courses or modules that could be replicated on a broad scale and designed to allow criminal justice actors to progress from basic to advanced levels as their professional duties so required. Trainers would need to be trained in the delivery of such courses to the point that training can be delivered by local trainers with only limited need for international trainers. Adequate systems for the monitoring and evaluation of training should be in place, as part of a strategy for continuing education and professional development, to ensure that the training delivered is effective, relevant and of benefit and value to the recipients.

3.28 The Group believes that there would be value in enabling some criminal justice actors to be trained by institutions offering such courses in other Commonwealth countries both at the basic and advanced level.

3.29 The possibility should be explored of establishing within the Commonwealth one or more centres of excellence addressing cybercrime issues. In addition to carrying out basic and advanced training on cybercrime and electronic evidence such a centre could test and further develop standardised courses and materials, disseminate good practices, carry out research on training, maintain a register of trainers, offer training of trainers and provide training to other countries with similar needs.

Enhancing knowledge through networking

3.30 In addition to training, peer-to-peer interaction and networking among the target audience, as well as with a range of other stakeholders, will be of crucial importance. Criminal justice actors should make use of existing networks and details of such networks should be made available and accessible. Consideration should be given, perhaps by the CMJA, to the creation of an international network of cybercrime or e-crime judges, as this particular group does not benefit from existing networks.

3.31 The Commonwealth Connects programme might be used to provide information and contact details about different networks and should promote access to existing training materials, initiatives and good practice.

Public-private co-operation

3.32 The expertise of the private sector/industry in respect of new technologies is an essential element for criminal justice training and the promotion of awareness. Private sector experts usually have the best and most up to date knowledge of hardware and networks needed to train investigators, and service providers and commercial users of the technologies often become aware of new crime trends or criminal activities first as they or their customers are targeted. Training institutes should consider involving academic and private sector experts in the design of their programmes and the development of training material. The participatory nature of this process can facilitate the co-operation and involvement of different stakeholders and the bringing together of knowledge and expertise. The advantages may also be reciprocal to some degree, as engagement in cybercrime training with law enforcement and prosecution experts may also help raise the awareness of cybercrime and the challenges of investigation and prosecution in the private sector.

3.33 Public-private co-operation has to be utilised sensitively in order to maintain the independence and impartiality of those responsible for criminal justice, particularly prosecutors and judges. Private sector involvement in general training is not as potentially problematic as it would be in the conduct of investigations or prosecutions, but may still have to be managed so as not to influence law enforcement, prosecutorial or judicial decisions. It is also important that any publicity or public attention to private sector involvement not create any appearance that the independence of criminal justice agencies or actors is compromised. Industry should not engage with training institutions for criminal justice actors in the expectation that they may thereby gain some advantage in terms of any criminal justice outcomes, but should do so on the basis that they will be enabling well informed decision making.

The role of the Commonwealth Secretariat

3.34 This part of the Group’s Report has identified a number of tasks in respect of training which need to be undertaken with a degree of urgency. The Group believes that the Commonwealth Secretariat should take a lead by

(a) maintaining up-to-date information (in conjunction with other international organisations) about existing training products that may be available to Commonwealth countries from third party, national and international organisations;

(b) making use of the Commonwealth Connects platform to maintain a database of existing regional and international training courses and centres and available materials that can be accessed or distributed in response to requests from national governments, judicial or law enforcement bodies;

(c) maintaining similarly a database of trainers that are qualified and able to support training activities for criminal justice actors in Commonwealth countries; and

(d) working with training course providers, including those experienced in training the judiciary in the Commonwealth, such as the CMJA, in order to create and develop course materials and training of trainers courses in fields not covered by existing national, regional or international training courses, especially where gaps have been identified and where further capacity building is required.

RECOMMENDATIONS

12. The Group recommends that all Commonwealth countries be encouraged to incorporate cybercrime and electronic evidence training within their national training programmes for criminal justice actors.

13. The Group recommends that Commonwealth countries should be encouraged to follow the model recommended within the report and follow the steps and adopt the measures listed in order to achieve an effective training strategy supported by relevant educational material and good practice.

14. The Commonwealth Secretariat should take a lead on cybercrime and electronic evidence training of criminal justice actors by

(a) maintaining up-to-date information (in conjunction with other international organisations) about existing training products that may be available to Commonwealth countries from third party, national and international organisations;
(b) making use of the Commonwealth Connects platform to maintain a database of existing regional and international training courses and centres and available materials that can be accessed or distributed in response to requests from national governments, judicial or law enforcement bodies;
(c) maintaining similarly a database of trainers and training providers that are qualified and able to support training activities for criminal justice actors in Commonwealth countries; and
(d) working with training course providers, including those experienced in training the judiciary in the Commonwealth, such as the Commonwealth Magistrates and Judges Association, in order to create and develop course materials and training of trainers courses in fields not covered by existing national, regional or international training courses especially where gaps have been identified and where further capacity building is required.

15. Training institutes should consider involving academic and private sector experts in the design of their programmes and the development of training material.

Implementation

Throughout its work the Group has been conscious of the need for urgent action on a number of fronts and of the resource implications of its Recommendations. Some of the Recommendations are addressed to member states of the Commonwealth, and if the Recommendations are to be implemented financial and human resources will have to be found from the national budget and/or with the help of funding bodies. Other Recommendations are addressed to the Commonwealth Secretariat. The Secretariat has many mandates and limited resources and the Group strongly recommends that the member states contribute the extra-budgetary resources needed for the implementation of the relevant Recommendations.

RECOMMENDATION

16. Bearing in mind the seriousness of the practical implications of cybercrime and the urgent need for the commitment of adequate resources, the Group strongly recommends that member states contribute the resources needed for the implementation of the foregoing recommendations.

The Commonwealth

APPENDIX

Members of the Working Group of Experts on Cybercrime

	Members	
1	**Colin Nicholls QC** *Chair of the Working Group*	Life President of the Commonwealth Lawyers Association
2	**Australia** a. Sarah Chidgey b. Tom Sharp c. Lucinda Atkinson d. Anthony Coles e. Leanne Loan	Australia Attorney-General’s Department
3	**Canada** a. Lucie Angers b. Christopher Ram	Canada Department of Justice
4	**Singapore** a. Christopher Ong Siu Jin **b.** G. Kannan	Singapore Attorney-General’s Chambers
5	**South Africa** a. Adv. Pieter du Rand	South Africa Department of Justice and Constitutional Development
6	**Tonga** a. ‘Aminiasi Kefu	Tonga Crown Law Department
7	**Trinidad and Tobago** a. Sunita Harrikissoon	Trinidad & Tobago Ministry of the Attorney General
8	**United Kingdom** a. Justin Millar b. Rob Kempsell c. Tim Crosland	UK Home Office UK Foreign and Commonwealth Office UK Serious Organised Crime Agency
9	**Intl. Telecom Union** a. Malcolm Johnson b. Marco Obiso c. Sandro Bazzanella	International Telecommunications Union
10	**UNODC** a. Gillian Murray	United Nations Office on Drugs and Crime

	b. Steven Malby	
11	**Council of Europe** a. Alexander Seger b. Cristina Schulmann	Council of Europe
12	**CTO** a. Lasantha de Alwis	Commonwealth Telecommunications Organisation
13	**CLA** a. Claire Martin b. Richard Graham c. Mark Deem	Commonwealth Lawyers Association
14	**CMJA** a. Dr Karen Brewer	Commonwealth Magistrates' and Judges' Association
15	**IAP** a. Elizabeth Howe	International Association of Prosecutors
16	**COMNET** a. Joseph V Tabone b. Lara Pace	COMNET
17	**ICANN** a. Dave Piscitello	Internet Corporation for Assigned Names and Numbers
18	Professor Jonathan Clough	Monash University, Australia
19	Zahid Jamil	Jamil & Jamil, Pakistan
Co-opted Experts		
20	Professor David McClean	University of Sheffield
21	Esther George	UK Crown Prosecution Service
22	Nigel Jones	Technology Risk Limited
SECRETARIAT Jarvis Matiya Shadrach Haruna Luke Bowyer Anthony Ming		Commonwealth Secretariat, Marlborough House London Head Justice Section – Justice Section Legal Adviser – Criminal Law Section Legal Intern – Criminal Law Section Adviser (Informatics) – Governance and Institutional Development Division

The Commonwealth

ANNEX B

COMMONWEALTH CYBERCRIME INITIATIVE (CCI)

OPERATING FRAMEWORK

I. INTRODUCTION

The overriding principle of CCI is to harness and bring coherence to the Commonwealth's existing commitments and resources in the fight against cybercrime. The commitment to ensure the processes described below are performed efficiently and effectively is a joint one, shared by the Commonwealth Secretariat and those states, organisations, and persons who have expressed a willingness and ability to assist in the work of the Initiative (its partners).

The object of this Framework is to clarify the responsibilities of the Commonwealth Secretariat and its partners in carrying out that task. The Framework is a statement of intention describing how parties shall operate together. The Framework is flexible and shall adapt to meet changing conditions, whilst retaining the core CCI methodology.

All participants in the Initiative share a common goal to combat cybercrime and to prevent the emergence of cybercrime safe havens. The Commonwealth is seen as a trusted partner able to link members of the consortium together under the Commonwealth umbrella.

II. THE FRAMEWORK

2. General

2.1 The CCI is a programme of the Commonwealth Secretariat designed to provide member states with coherent and sustainable assistance in building the necessary capacity to combat cybercrime.

2.2 Co-operating with a range of committed international partners, it extends support to member states by assisting them to develop all elements of an effective response to cybercrime, including prevention measures, establishing appropriate legal frameworks, and attendant investigative, technical, enforcement and prosecutorial capabilities.

2.3 It is administered by the Commonwealth Secretariat through the Commonwealth Secretariat's Legal and Constitutional Affairs and Government and Institutional Development Divisions (LCAD and GIDD), assisted by the UK's National Crime Agency (NCA), an Executive Management Committee (CEMC), and an Operating Consortium (COC).

2.4 The Commonwealth Secretariat is the focal point of the CCI. It is represented on the CEMC and provides secretarial and administrative functions to the CEMC with the assistance of NCA.

2.5 The CEMC consists of representatives of member states who wish to contribute to the resourcing and strategic planning of capacity building work across the Commonwealth, the Commonwealth Secretariat, SOCA, and COC. It provides overall direction and management of CCI, co-ordinates its activities, and liaises with its partners in the COC in determining the needs assessments of requesting states and the implementation of action plans

2.6 The COC includes Commonwealth states, organisations, and persons with the necessary expertise in combating cybercrime and providing capacity building who have expressed a willingness to carry out or assist in the implementation of requests. Members bring specific cybercrime skills and resources to the consortium and collectively create synergies to assist member countries. Although scoping missions will generally be conducted by independent experts who are free from the limitations of corporate mandates, the COC is the CCI's primary resource for the implementation of plans of action.

III PHASE 1

3. Requests for Assistance

3.1 All requests for assistance will be addressed to the Commonwealth Secretariat.

3.2 The Commonwealth Secretariat (CS) will assist member states in formalising requests including:

- ensuring they are submitted by an appropriately senior individual within the Government Department of the Requesting State or other competent authority responsible for the development and implementation of a national cybercrime or cybersecurity strategy (national strategy);
- encouraging member states to frame requests in terms of the development and implementation of a national strategy.
- advising on time frames.

3.3 The Commonwealth Secretariat will develop a request template for this purpose.

3.4 Once a formal request for assistance has been received and reviewed by the Commonwealth Secretariat, the Commonwealth Secretariat will submit it to the CEMC.

4. The Decision whether to conduct a Needs Assessment

4.1 Upon receiving a formal request the EMC will decide whether to conduct a Needs Assessment.

4.2 In making its decision the EMC will take into account

- the approximate number of requests it can respond to effectively in any given period;
- whether there are strategic reasons to offer assistance to particular countries (for example, there might be an opportunity to integrate cybercrime preventative measures into a current ICT development programme).

4.3 The CEMC with the assistance of the Commonwealth Secretariat and the COC will develop and keep under review a list of experts willing and able to conduct needs assessments. Experts must meet at least the following criteria:

- recognised expertise either in relation to the criminal justice response to cybercrime and the acquisition of digital evidence; or in preventative measures (and specifically information security);
- political awareness and sensitivity;
- independence from any conflicting interest;
- a willingness to follow the CCI model for needs assessments;

- following completion of a needs assessment, CCI EMC will review the status of the experts on the list.

4.4 The Commonwealth Secretariat will maintain the list.

4.5 Expert expenses (travel, accommodation, subsistence, visa, inoculations and insurance) will be met from the CCI project fund (see para. 12 below). Additionally, where an individual's time is not being recompensed by an employer, an honorarium of £1000 may, if necessary, be paid for the visit and, where appropriate, up to a further £1000 for time spent in the preparation of the Needs Assessment report.

5. Preliminary Steps and the In-Country Needs Assessment

5.1 Preliminary desk-top research will initially help inform a decision on whether a Needs Assessment is required, and then, where a decision is taken to proceed, provide background to assist effective preparation. The CEMC will identify an individual from the CCI community (not necessarily an expert from the panel) to conduct such research, covering matters such as point in electoral cycle; capacity building work previously undertaken or already planned; current state of any existing national strategy. If no appropriate individual can be identified SOCA will conduct basic inquiries as to needs through its international network.

5.2 The Commonwealth Secretariat will agree a timescale for the Needs Assessment with the requesting state, which will indicate the requirements in terms of stakeholders to be interviewed, sending an advance copy of the CCI Barometer Report template to advance notice of some of the themes that will be explored, and requesting a flow-chart illustrating the different roles and responsibilities of relevant stakeholders.

6. Appointment of the Needs Assessment Team

6.1 The CEMC will appoint a Needs Assessment Team consisting of two experts from the list/panel of experts to conduct the Needs Assessment, one of whom shall be nominated as Project Leader.

6.2 The CEMC will appoint an Assessment Mentor to the Assessment Team who shall be a member or selected nominee of the CEMC.

6.3 The Assessment Mentor will advise the two experts of CCI methodology and the expected outcomes from the Assessment

6.4 At least 2 weeks prior to the Assessment, the Commonwealth Secretariat will arrange a virtual conference (including the Needs Assessment Team and mentor, and facilitators from the Requesting State) to help refine the scope and structure of the assessment process.

6.5 The Commonwealth Secretariat will ensure the experts have appropriate advice on visa and inoculation requirements.

7. Conduct of the Needs Assessment

7.1 The Lead Expert will be responsible for the conduct of the Assessment and for completion of the Assessment Report.

7.2 The overriding principle of the assessment is ‘assistance not interference’. The assessment process should aim to facilitate active, engaged discussion about the state’s requirements; as well as to co-ordinate stakeholders in country.

7.3 The assessment shall be conducted with reference to the CCI checklist and barometer report. It will not be permitted to become a ‘tick box’ exercise.

7.4 The Assessment shall be conducted over a minimum of four full working days. To ensure time is used most effectively it is recommended that meetings are conducted from a fixed location in the lead Ministry of the Requesting State, with a representative from the Ministry in attendance throughout. Not only does this save travel time, it communicates to stakeholders that the project is locally owned and driven.

7.5 In addition to meeting local stakeholders the Assessment Team shall also arrange to meet with relevant international actors in country to ensure donor co-ordination.

8. The Needs Assessment Report

8.1 The Lead expert is responsible for ensuring the Assessment Report is completed within 4-6 weeks of the country visit. The Needs Assessment mentor will offer appropriate guidance to the lead expert in this task.

8.2 The completed report should be shared initially only with the EMC for editing and review. This review will be completed within 2 weeks.

8.3 The Assessment Report will then be shared with representatives of the Requesting State inviting them to edit and review it.

8.4 The Assessment Team and representatives of the Requesting State will then agree a List of Requirements, which will provide a clear basis for further assistance.

IV PHASE 2

9. Implementation of the List of Requirements

9.1 The decision whether to proceed to CCI Phase 2 and implement the List of Requirements will be made by the EMG and the Requesting State.

9.2 It will not always be necessary or appropriate to progress to CCI Phase 2. In some cases, for example, CCI Phase 1 will have been sufficient to mobilise the appropriate strategy development and implementation in-country or the political commitment may be lacking.

9.3 Where EMC and the Requesting State agree that a List of Requirements will be implemented CEMC will identify a Project Co-ordinator, who may be one of the two experts who conducted the assessment, the Assessment Mentor, or some other appropriate individual or individuals.

9.4 The Project Co-ordinator will liaise with members of the COC and potential funders to identify organisations and/or individuals who are willing to draft a Programme of Work and implement the List of Requirements agreed in Phase 1.

9.5 Once a Programme of Work has been agreed it will be submitted to the EMC for review.

9.6 If the EMC approves of the Programme of Work the Commonwealth Secretariat will present it to the Requesting State for agreement.

9.7 Depending on the scale of the Programme of Work it may be appropriate to: (i) seek funding for a dedicated project co-ordinator; (ii) draft an MOU setting out the expectations of the Requesting State, the Commonwealth Secretariat and the partner(s) who have expressed a willingness to implement the List of Requirements; and/or (iii) to convene a Project Launch

9.8 It will be the role of the Project Co-ordinator to assist with co-ordination between the parties involved in Phase 2 and to provide quarterly updates to the EMC on progress and outcomes.

9.9 Phase 2 will normally be conducted over a period of between 1 and 2 years.

10. Implementation of the Programme of Work

10.1. Implementation of the Programme of Work will be a matter for the project co-ordinator, the Secretariat and the volunteering members of the COC, according to any agreements made between those parties, and between those parties and the requesting state.

11. Partner Co-ordination

11.1 Collaboration is at the heart of CCI and the consortium will be maintained through a combination of virtual and physical interactions.

11.2 SOCA will convene meetings of the CEMC and COC as required and provide a minute taker. Meetings of the CEMC will be held every two months and meetings of the COC twice annually. The meetings may be virtual meetings.

11.3 The Commonwealth Secretariat will host the meetings and provide facilities for remote connection and refreshment.

11.4 The Commonwealth Secretariat will establish CEMC and COC mailing lists, enabling partners to communicate to the network at any time.

12. The Project Fund

12.1 The Commonwealth Secretariat will maintain a Project Fund to support the Needs Assessment process, specific project co-ordination, and contributions to Phase 2 as it considers appropriate.

12.2 The Commonwealth Secretariat will provide for the administration of CCI and contribute to Needs Assessment through its General Funds. States may voluntarily provide extra funds, either for specific CCI projects (usually at Phase 2) or for CCI projects generally.