



A voice for the
COMMONWEALTH INTERNET GOVERNANCE FORUM

Commonwealth Cybercrime Initiative

Proposal

Commonwealth Internet Governance Forum

10/19/2011

Contents

1. Executive Summary	5
2. Purpose	7
3. Background	9
3.1 Global Impact and Dependence	9
3.2 The global threat	11
4 The Proposed Commonwealth Initiative:.....	14
4.1 What is needed? Summary of Objectives.....	14
4.2 Underlying Advantages	17
4.3 Why the Commonwealth – A Comparative Advantage	18
5 The Initiative.....	21
5.1 Commonwealth C2P Platform :.....	21
5.1.1 Outline	21
5.1.2 Knowledge Resources	22
5.1.3 Online Capacity Building	22
5.1.4 Interactive – Networking	22
5.1.5 Connecting to experts	23
5.1.6 Point of Contact for Projects.....	23
5.2 On the Ground Assistance Delivered Regionally and Nationally	23
5.2.1 Supportive Policy, Regulation, and Enforcement.	23
5.2.2 Preliminary High Level Cybercrime Health-Checks (Legal Framework Status)	24
5.2.3 Gap Analysis & Need Assessment (More Detailed Legal Framework Analysis outlining specific recommendations for Improvement)	25
5.2.4 Drafting of Legislative/Regulatory instruments (stand-alone/amendments)	25
5.2.5 Technical Assistance for Implementation of Post-Legislative Improvements and Reforms	26
5.2.6 Technical Assistance in terms of Training.....	27
6 Implementation Methodology and Modules.....	28

6.1	C2P – A Platform for Resources and Tools	29
6.2	Preparatory Phase (Regional Outreach & Energizing)	29
6.3	In-country Assistance	30
7	Expertise Required for Implementation	35
8	Potential Partners and Roles (in alphabetical order)	38
8.1	Centre for Internet Safety, Cyprus	38
8.2	Centre for Internet Safety, University of Canberra	38
8.3	Children’s Charities’ Coalition on Internet Safety	39
8.4	COMNET Foundation for ICT Development	39
8.5	Commonwealth Business Council (CBC)	40
8.6	Commonwealth Lawyers Association (CLA)	40
8.7	Commonwealth Parliamentary Association (CPA)	41
8.8	Commonwealth Secretariat	41
8.9	Commonwealth Telecommunications Organisation (CTO)	42
8.10	Council of Europe	42
8.11	Diplo Foundation	43
8.12	International Centre for Missing and Exploited Children (ICMEC)	44
8.13	International Corporation for Assigned Names & Numbers (ICANN)	44
8.14	International Cyber Security Protection Alliance (ICSPA)	45
8.15	International Telecommunication Union (ITU)	46
9	Funding Support:	48
9.1	Primary Funding Partners	48
9.2	Other Supporting Partners	48
10	Governance Structure	49
10.1	Commonwealth Cybercrime Initiative Steering Group	49
10.2	Advisory Committee: Accountable to the Executive Management	50
10.3	The Secretariat	51
11	Forward Plan	53
12	Conclusion	54

1. Executive Summary

The Internet is one of the truly revolutionary phenomena of our times. It has changed the way we live and work and we have come to rely on it in every sphere of our endeavours. From a population of 20 million connected to the Internet in 1998, we now have more than two billion and rising. It is estimated that this connectivity will now double in the coming years as a result of a number of factors including the introduction of non-Latin script top level domains for Internet addresses, expansion of the Internet's generic domain name space and the increasing prevalence of smart phones and tablets with Internet access.

While the benefits of this borderless ecosystem have grown exponentially, the Internet has also become an irresistible magnet for criminal behaviour. Cyber criminals have become increasingly inventive and gravitate to jurisdictions which offer them most protection because of outdated and non-harmonised legal regimes and law enforcement agencies which do not have the skills and resources to monitor Internet traffic, to investigate complaints, to prosecute or invoke any intervention that may be warranted. The global and borderless nature of the Internet enables criminals to co-operate and co-ordinate their activities and distribute their assets over several jurisdictions with impunity.

The Initiative which is the subject of this paper aims to address these issues by providing assistance to Commonwealth member states to implement a comprehensive legal framework for responding to cybercrime and acquiring cyber evidence. In so doing it will utilise the Commonwealth Model Law which is consistent with the Budapest Convention on Cybercrime. It will also develop the other components of an effective capability, including 24/7 networks and working protocols with service providers, and gateways for the exchange of intelligence and evidence. It will also assist law enforcement and national security agencies in acquiring the necessary technology and skills to enable them to conduct their work. It will help states wishing to accede to the Budapest Convention to achieve this objective and ensure that states unwilling or unable to do so will develop consistent and effective laws and procedures. The Commonwealth's ability to instigate such changes benefits from the common institutional backdrop, traditions, language and value system of member states; this is the Commonwealth's comparative advantage.

The Commonwealth as an institution has little by way of specialist capacity or funds for such a venture. Rather it is a catalyst and broker working with the broad alliance of partners with each partner having a unique contribution to make. Development and donor agencies are also expected to play a vital role in the Initiative. It is anticipated that much of the assistance in capacity building will be sought in less developed countries, including small states who do not have the resources and means to pay for this.

This Initiative was developed by the Commonwealth Internet Governance Forum, a multi-stakeholder entity established within the UN Internet Governance Forum (IGF) in recognition of the desperate and urgent need for action to tackle the growth of Cybercrime. The support for it has been overwhelming because a safer Internet is vital to our economic recovery and one of the principal motors contributing to global social and economic growth and development.

2. Purpose

In July the Commonwealth Law Ministers Meeting recognized the urgent need for updating of laws with respect to Cybercrime for member countries and the assistance that the Commonwealth could provide by contributing to work in this area. The Commonwealth Internet Governance Forum had also separately been working with a diverse group of experts towards a Cybercrime Initiative. The purpose of this paper is to provide an approach, in follow up to the Law Minister's call for such an Initiative combined with the work of the CIGF experts for consideration at the Commonwealth Heads of Government for a Cybercrime initiative which is designed to provide support to member states in realising the necessary policy, legal, human and technical infrastructures/capacities that will enable them to exploit the capabilities of the Internet for socio-economic development purposes while at the same time providing them with the tools to contribute to national and global efforts aimed at combating the attendant threat of cyber crime.

The Initiative aims to assist developing countries across the Commonwealth and beyond, to build their institutional capacity in the areas of policy, legislation and technical and operation abilities in fighting cybercrime through the sharing of expertise and best practice from existent resources with particular focus on the Commonwealth Model Law on Computer and Computer Related Crime¹, The Initiative will also take into account other consistent resources such as the ITU Toolkit for Cybercrime Legislation², and the Business Software Alliance's Model Law³ all of which are based and modelled upon the Budapest Convention on Cybercrime⁴ and thus, share a common core. Drawing upon such international instruments, the Initiative will promote and contribute to the development and application of norms of law and behaviour within cyberspace⁵. This in

¹ 'a model law on the basis of the work of the Council of Europe on the Draft Convention on Cyber Crime (COE Draft Convention).' - http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BD4109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf

² The definitions offered in the Sample Language are consistent with the definitions used and the intent behind similar terms in the cybercrime laws of developed nations and the Council of Europe Convention on Cybercrime (CoE Convention). - <http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html>

³ http://www.bsa.org/~media/Files/Policy/Security/CyberSecure/Cybersecurity_Framework.ashx
<http://www.comnet.org.mt/wp.../The-Cybercrime-Convention-Zahid-Jamil.ppt>

⁴ www.coe.int/cybercrime
http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_Guide_A5_12072011.pdf

⁵ P. 12 'International and Multi-stakeholder Organizations. Regional organizations have been particularly effective at tackling cybersecurity problems specific to their members. They will play an increasingly important

turn this will enhance international cooperation⁶ with respect to criminal and malicious activity in cyberspace⁷.

role in developing and applying norms of behavior. – White House International Strategy for Cyberspace, May 2011. –

http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

⁶ <http://www.smh.com.au/opinion/politics/cyber-law-casts-the-proper-net-20110829-1jib6.html>

⁷ *p. 20* – White House International Strategy for Cyberspace, May 2011. –

http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

3. Background

The Internet is a landmark development for civilisation equivalent to Gutenberg's first printing press in the 15th century and the industrial revolution which followed three centuries later.

3.1 Global Impact and Dependence

The borderless ecosystem of Cyberspace has flattened our world into a globally interconnected and interdependent network of systems. The benefits have grown exponentially in the areas of economic, social and democratic development and have been shared by both the developed, as well as developing countries.

The recent events in the Middle East highlight the vital importance of the internet in securing individual and democratic freedoms.

The recent global financial crisis underscores the importance of improving the security of transactions, trade and commerce in cyberspace.

Enhanced cyber security and improved user confidence for trade and commerce on the Internet will have a pivotal role in stimulating the global economic recovery.⁸

The advent of Internet banking, the growth of business process outsourcing, the expansion of electronic payment systems and the development generally of the global Internet economy have provided significant benefits for developing countries including small island states. The Tuvalu government's revenues largely derive from the use globally of .tv domain name. Small island states have benefitted by leveraging the power of the Internet for increasing the availability of Internet banking. Within the Commonwealth,

⁸ <http://www.gizmodo.com.au/2011/05/the-internet-creates-2-6-new-jobs-for-every-one-lost-offline/>
http://www.eg8forum.com/en/documents/McKinsey_report.pdf

India, Sri Lanka, Pakistan and Ghana have become destinations for outsourcing of call-centres and IT development.

The use of the Internet has grown from 16 million users in 1995 to 2.0 billion in 2011⁹ with the opportunity for the next billion to connect through the expansion of mobile access to the Internet, which is projected to surpass fixed access to the Internet by 2013¹⁰. The socio-economic landscape of the Internet will see dynamic changes in the light of developments such as social networking, cloud computing and the anticipated expansion of the new gTLDs space (including the introduction of internationalized non-Latin script)¹¹ and the development of Web 3.0, the “semantic web”¹².

These goals are essential for the collective future progress of both developed and developing economies and are also the shared objectives of the Harare Declaration and the mission of the Commonwealth.

Unfettered, secure, stable and reliable access to critical Internet resources is thus, key to sustaining growth in global socio-economic activity and is of vital importance to the developing countries of the Commonwealth .

At the same time this dependence has made the openness, interoperability, security, reliability and resilience of these systems a critical infrastructure for good governance in everything from delivery of public services, to trade, commerce, social development, defence and democratic freedoms of the global community.

⁹ <http://www.internetworldstats.com/emarketing.htm>

¹⁰ http://www.morganstanley.com/institutional/techresearch/pdfs/Internet_Trends_041210.pdf

¹¹ <http://icann.org/en/tlds/select.htm>

¹² Tim Berners-Lee originally expressed the vision of the semantic web as follows:

I have a dream for the Web [in which computers] become capable of analyzing all the data on the Web – the content, links, and transactions between people and computers. A ‘Semantic Web’, which should make this possible, has yet to emerge, but when it does, the day-to-day mechanisms of trade, bureaucracy and our daily lives will be handled by machines talking to machines. The ‘intelligent agents’ people have touted for ages will finally materialize.– Tim Berners-Lee, 1999

3.2 The global threat

Unfortunately, the Internet has also become an irresistible magnet for another human endeavour - **Crime**.

The Internet brings with it the attendant threat of crimes against computer systems i.e. cybercrime as well as the use of computers for criminal activities i.e. cyber enabled crime. Cybercrime includes not only crimes against computer systems (such as hacking, denial of service attacks and the set up of botnets) but also traditional crime committed on electronic networks (e.g. fraud via phishing and spam; illegal Internet-based trade in drugs, protected species and arms) and illegal content published electronically, (such as child sexual abuse material). Moreover Cyberspace may be used as part of the planning of, or to provide evidence in relation to, any form of criminality from terrorism to corruption. Consequently measures against cybercrime will have widespread application to the prevention and detection of crime.

Foremost in this is the prevalence of fraudulent financial dealings, drug trafficking and facilitation in other criminal activities such as money laundering, terrorist use of the Internet, child abuse images and human trafficking.

We have seen how criminals are able to take control of thousands of computers and create networks of robots – botnets - across the world multiplying their computing power and distributing their malicious activities across jurisdictions. A single botnet can cause incalculable loss.¹³ It is possible to rent a botnet for \$67 for 24 hours, and \$9 for hourly access¹⁴.

With the exponential growth of identity (ID) theft, Internet fraud, phishing and spear-phishing (there were at least 67,677 phishing incidents in the 2nd half of 2010)¹⁵ the global economy continues to suffer enormous financial losses. In particular this stems from the disharmony and lack of international cooperation in combating cybercrime, which in turn allows the existence of safe haven jurisdictions from which cyber criminals continue to operate. The

¹³ <http://abcnews.go.com/Technology/feds-crush-coreflood-botnet-infected-million-computers-stole/story?id=13369529>

¹⁴ <http://www.zdnet.com/blog/security/study-finds-the-average-price-for-renting-a-botnet/6528>

¹⁵ http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2010.pdf

cost to the UK economy alone is estimated to be at £27billion per year¹⁶, According to one analysis, the cost to individual companies can be as much as US\$52 million per year¹⁷

In addition to financial losses incurred by businesses, the public sector, and the global economy, there is also the loss of productivity. One study estimated the loss to business associated with disruption caused by criminal cyber attacks as 22 percent of external costs.¹⁸ Also, the prevalent threat of cybercrime has an impact on the productivity of employees (both private and public), as a result of requiring cumbersome and complex security measures which translate into global economic productivity losses associated with cybercrime.

Cybercriminals have become highly adept at exploiting the global nature of the Internet. The lack of harmonized legislation and international cooperation allows them to target victims across borders as well as domestically with impunity. Criminals exploit the fact that online fraud that crosses national borders is often difficult for law enforcement to investigate, let alone prosecute, as a result of either a lack of any legislation (at worst) in some countries or the lack of effective and harmonious legislation (at best), coupled with the problem of insufficient international cooperation.

Even when cybercrimes take place domestically (where the perpetrator and victim are in the same jurisdiction), such domestic cybercrimes are complicated by the fact that the tools for procuring the crimes are distributed all over the world in multiple locations (e.g. servers, hacking applications etc.). This presents major difficulties for law enforcement agencies when conducting searches, seizures and collection of evidence, not to mention the challenges that the prosecution faces in presenting the necessary evidence at trial.

¹⁶ <http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime>
<http://www.bbc.co.uk/news/uk-politics-12492309>

¹⁷ “Cyber crimes can do serious harm to an organization’s bottom line. We found that the median cost is \$3.8 million per year, but can range from \$1 million to \$52 million per year per company.” - [http://www.riskandinsurancechalkboard.com/uploads/file/Ponemon%20Study\(1\).pdf](http://www.riskandinsurancechalkboard.com/uploads/file/Ponemon%20Study(1).pdf)

¹⁸ [http://www.riskandinsurancechalkboard.com/uploads/file/Ponemon%20Study\(1\).pdf](http://www.riskandinsurancechalkboard.com/uploads/file/Ponemon%20Study(1).pdf)

Cybercrime being global and borderless, makes it necessary that criminal conduct on the Internet is recognised by national jurisdictions in a consistent way based on mutual cooperation, by means of globally accepted policies, with definitions secured by international agreement. Otherwise, we run the risk of creating safe havens for the perpetrators.

There is often a lack of harmony and compatibility in the criminalisation of behaviour on the Internet as well as the definitions of cyber offences. It is also important to prevent legal frameworks becoming outdated and ineffective if they do not include procedural powers to handle for example cyber forensics and electronic evidence.

The global and borderless nature of the Internet enables criminals to cooperate and coordinate their activities and securely distribute their activities and assets across multiple jurisdictions. It is important for national law enforcement agencies to similarly coordinate and cooperate internationally in real-time against cybercriminals thus, denying them safe havens.

Due to lack of resources, many developing countries have been unable to implement policy, regulatory frameworks and operational capacity (both of the technical communities and law enforcement) especially with respect to the ability of the private sector, technical community and law enforcement to forge cooperative mechanisms.

Outdated and disharmonious legal regimes across the world contribute to inadequacies and ineffectiveness of law enforcement to globally cooperate thereby providing cybercriminals with safe havens and an ideal enabling environment from which to take advantage.

Cybercriminals are therefore able to seek out safe havens where the legal regimes and law enforcement capacities are weaker and from where they can base, coordinate and launch their operations with impunity.

The inadequacies with respect to legal, policy, regulatory frameworks and operational capacity in safe havens therefore are a continuing and growing threat to the economy and security of the developed as well as developing countries and the global market.

4 The Proposed Commonwealth Initiative:

4.1 What is needed? Summary of Objectives

This global problem can only be addressed by a global solution and through international engagement.

What is needed is a concerted effort amongst the countries of the world to deny safe havens to cybercriminals by updating and harmonising policy and especially legal regimes in line with international best practice to enable real-time and effective international cooperation for investigation and prosecution of cybercrime.

Effective strategies to counter cybercrime and other Internet-based threats rely on a concerted, multi-lateral effort which involves the development of relevant, up-to-date policies, corresponding legal frameworks, including regulatory measures, meaningful enforcement, and extensive private sector engagement. Those countries that lack a mature national cybercrime strategy typically require assistance in building an institutional capacity and related human resources and skills in each of these areas.

The Commonwealth Cybercrime Initiative thus, aims to address the urgent need to assist developing countries in the Commonwealth (although it has application around the world) to build their institutional capacities especially with respect to policy, legislation, regulation as well as technical and operational abilities. In this way, their jurisdictions can be made more secure by denying safe havens and enabling them to become effective partners in the globally coordinated effort to combat cybercrime.

The Commonwealth Model Law on Computer and Computer Related Crime (“Model Law”) provides a foundation and basis for legislation and an ‘off-the-shelf’ tool through which to leverage the unique advantage of the Commonwealth’s shared legal traditions for the adoption and implementation of harmonized legal regimes, putting member states on the

road to combating cybercrime. For instance the Commonwealth's Harare Scheme¹⁹ can provide a model for domestic legislation to enable Mutual Legal Assistance for international cooperation. This will contribute, to enabling international cooperation between our nations and the global community in effectively combating cybercrime. The Commonwealth Model Law helps bring domestic legislation in line with existing international standards and instruments, including the Budapest Convention²⁰.

The **Commonwealth Cybercrime Initiative ("the Initiative")** thus, aims to assist developing countries across the Commonwealth and beyond to build their institutional and legislative capacity in fighting cybercrime through the sharing of expertise and best practice and upon the existing international standards and instruments and consistent resources and tools through:

- a minimum foundation and threshold with respect to common definitions and offences
- increasing harmonization of domestic criminal laws as they relate to cybercrime;
- the establishment of necessary procedural powers for investigation and prosecution
- the establishment of legal frameworks, protocols and codes of practice and protocols that will inter alia enable international cooperation beyond simply government to government, or LEAs to LEAs, to promote cooperation between private sector entities (e.g. banks, telcos, ISPs) and the technical community (e.g. ccTLD registries, APWG, RISG, CERTS²¹), both amongst themselves and with local and

¹⁹ Commonwealth Mutual Assistance In Criminal Matters - http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/2C167ECF-0FDE-481B-B552-E9BA23857CE3_HARARESCHEMERELATINGTOMUTUALASSISTANCE2005.pdf

²⁰ While Cyprus and the United Kingdom are parties to this treaty, Canada and South Africa are signatories and Australia is in the process of accession.

²¹ <http://www.networkworld.com/newsletters/2005/0110sec2.html> . Therefore, wherever in this document makes reference to the term Computer Emergency Response Team (CERT), it also means to include Computer Incident Response Teams (CIRT) as a possible sub-set of the broader term CERT.

national government agencies, regulators and/or LEA. Examples of such cooperative initiatives include CERTs, hotlines and, LEA-ISP cooperation guidelines;

- the building of operational and technical skills and capacities of the technical community and law enforcement to bolster investigative capabilities
- the establishment of a fast and effective regime of international cooperation for investigation and prosecution of cybercrime between law enforcement agencies
- the establishment of national policy strategies that create an enabling environment for the introduction of all the above across Commonwealth countries and beyond.

This will facilitate greater certainty with respect to prosecutions of cybercrime both at a domestic and international level, in particular speedy (real-time and 24x7) cross-border multilateral cooperation both at an operational and investigative level but also at the prosecutorial level.

The Initiative would in this way greatly benefit developing countries by reducing the immense costs to their economies caused by cybercrime, by raising their standards, skills and operational capabilities in addressing the challenges posed by cybercrime. And by thus, bridging this digital divide between developing countries and developed countries. The Initiative will also greatly contribute to making the global Internet, the developed economies and the global marketplace a more secure, reliable and safer environment thereby mitigating and reducing the immense costs to the global economy associated with cybercrime.²²

²² See 2.1 and 2.2 above

4.2 Underlying Advantages

The Commonwealth Model Law²³, like the ITU toolkit²⁴, follows closely the Budapest Convention. The Convention has been used by many countries as a basis for their domestic legislation. Consequently implementation of the Model Law not only provides a comprehensive framework for taking action against cybercrime, it will facilitate harmonisation of legislation, and assist states in conforming to the existing international standards, and in turn assist and encourage, those states which desire acceding to existing international treaties, including the Budapest Convention on Cybercrime²⁵. However, assistance under the Commonwealth Cybercrime Initiative is not intended to be dependent upon a commitment from recipient States to accede to any particular convention or instrument.

The Initiative will play a facilitating role with respect to assist in promoting and encouraging nations to consider the process of establishment and harmonization of cybercrime legislations and legal frameworks, making available existing international legal instruments adopted by several countries as well as capacity building tools and resources.

However the Initiative recognizes that a legal framework forms only the basis of a response to cybercrime. To be effective it needs to be combined with specialist law enforcement capability, a developed 24/7 network for international co-operation, and protocols and working arrangements with communication service providers. The Initiative (supported by a diverse range of partners including ITU and the Council of Europe) will promote development in all areas simultaneously, ensuring co-ordination and

²³ pg. 200 ‘...countries have used the Convention as a model and drafted parts of their legislation in accordance with the Convention on Cybercrime.....’ - Pg.225’ Due to the clear instruction as well as the recognition of the Council of Europe Convention on Cybercrime as an international standard by the expert group, the model law largely corresponds to the standards defined by that Convention. - ITU: UNDERSTANDING CYBERCRIME: A GUIDE FOR DEVELOPING COUNTRIES Draft March 2011 - http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_Guide_A5_12072011.pdf

²⁴ ‘The definitions offered in the Sample Language are consistent with the definitions used and the intent behind similar terms in the cybercrime laws of developed nations and the Council of Europe Convention on Cybercrime (CoE Convention).’ - <http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html>

momentum in the response to Cybercrime across the Commonwealth and beyond.

By virtue of its role the Commonwealth Initiative will contribute to the development of a harmonised policy, regulatory and especially the legal framework for combating cybercrime and facilitating international cooperation. The impact of such harmonisation and bolstering of operational cooperation extends beyond simply cybercrime cases. With the permeating effect of the Internet and electronic devices in all aspects of daily life, cybercrime is more often than not intertwined in all forms of criminal activities ranging from organized crime²⁶, drug trade, human trafficking, money laundering and child pornography. Ergo the greatly enhanced cooperation brought about on the back of expedited, real-time and 24x7 cooperation against cybercrime at operational, investigative, enforcement, and prosecutorial levels also brings great benefit to combating other crimes.

4.3 Why the Commonwealth – A Comparative Advantage

The shared legal traditions of the common law between the Member States provide the Commonwealth with a unique advantage for harmonising policies and legal frameworks and providing, with support from the Harare Scheme that has been updated to include terms from the Budapest Convention, a cooperative platform for collaboration, thereby contributing towards international cooperation in the global fight against cybercrime.

Member States of the Commonwealth share, at least at the basic level a legal system of common law and institutional structures. The historic, traditional and close relationship of Commonwealth countries with the UK and its legal system as well as amongst themselves creates an enabling environment

²⁶ 'organised crime, cyber crime and terrorism are transnational issues requiring a coordinated international response' - Quintet of Attorneys General - 9/10 November 2009 Communiqué [http://www.ag.gov.au/www/ministers/RWPAttach.nsf/VAP/\(3A6790B96C927794AF1031D9395C5C20\)~091111+McClelland+Quintet+Meeting+Communique.pdf/\\$file/091111+McClelland+Quintet+Meeting+Communique.pdf](http://www.ag.gov.au/www/ministers/RWPAttach.nsf/VAP/(3A6790B96C927794AF1031D9395C5C20)~091111+McClelland+Quintet+Meeting+Communique.pdf/$file/091111+McClelland+Quintet+Meeting+Communique.pdf) -

within the Commonwealth group for easier acceptance of model legislations in general by Commonwealth countries. This places the Commonwealth in a unique and advantageous position to take a lead with member countries to achieve the goal of harmonising and improving policy and legal frameworks, legal definitions, procedures, safeguards and mechanisms for mutual legal assistance, operational capabilities, international cooperation and collection of evidence which are not just limited to purely cybercrime cases but also extend to crimes that take on a greater gravity.

The Commonwealth Model Law on Computer Related Crime²⁷ and the Scheme on Mutual Assistance in Criminal Matters (the Harare Scheme²⁸) are examples of the products of Commonwealth mechanisms, such as the Law Ministers meetings which provide a unique and effective platform for establishing cooperative mechanisms between Commonwealth countries. Such mechanisms allow for easier acceptance of agreed language in policy and legal frameworks. Recognition at the Commonwealth Law Ministers' meetings enables easier acceptance of such agreed Model Laws, Schemes and frameworks at National levels by Commonwealth countries. The Commonwealth thus, presents an ideally effective opportunity for the implementation and adoption of cybercrime law/regulation and cyber security policy within its member states.

Hence, instead of expending resource, effort and time in lengthy negotiations for agreed language (in the areas of cyber security policy and legislative templates), existing cyber security policies/standards and particularly the Model Law and Harare Scheme provide an 'off-the-shelf' and accepted framework recognised by the Commonwealth nations that can help bridge the policy and more importantly the legislative gaps between the member states, requiring only for nations to participate in the process of adaptation, adoption and implementation.

²⁷ 'a model law on the basis of the work of the Council of Europe on the Draft Convention on Cyber Crime (COE Draft Convention).'

http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf

²⁸ Commonwealth Mutual Assistance In Criminal Matters
http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/2C167ECF-0FDE-481B-B552-E9BA23857CE3_HARARESCHEMERELATINGTOMUTUALASSISTANCE2005.pdf

The adoption at a national level by members of the Commonwealth Model Law, the Harare Scheme and associated policies lays the foundation for, and would be a first positive step towards, an expedited process for Member States of the Commonwealth to adopt policy and legal frameworks for international cooperation, thereby contributing towards a safer, more secure and reliable Internet.

Recognition also needs to be given to the interrelated spheres of cyber security and cybercrime. These are not necessarily mutually exclusive, nor are they components of each other but do share commonality in certain overlapping areas. Cyber security deals with protecting systems and can include threats that are malicious, as well as those that are a result of errors and gaps in systems. Cybercrime on the other hand deals exclusively with conduct that is malicious and hence, criminal in nature. Hence, one deals with protecting systems and the other with rule of law and maintenance of order in cyberspace. Both are a threat to the security of the Internet. The Commonwealth can contribute to both.

This Cybercrime Initiative, in an effort to lead from a position of its relative strength and comparative advantage available to the Commonwealth, will address the threat with a primary focus on Cybercrime whilst incorporating, as ancillary, several aspects that will also contribute to enhanced cyber security.

The Commonwealth can, in coordination with such actors provide a collaborative platform, thus bringing to the global effort a complimentary yet distinctive value-add, through its own unique advantages.

5 The Initiative

In order to achieve the above objectives, the Initiative will deploy a combination of resource platforms and facilities made available on a cross-Commonwealth basis as well as on-the-ground assistance at the country and regional levels.

5.1 Commonwealth C2P Platform :

5.1.1 Outline

The Commonwealth Connects Platform (C2P) is designed to provide access to information and knowledge resources across the Commonwealth as well as provide a set of practical tools to support policy and professional collaboration online. The C2P can thereby support essential capacity building work by creating and maintaining a knowledge repository relating to cybercrime, and by providing an online platform for networking, knowledge transfer and the exchange of best practice. Linked to the CIGF website and other partners, the C2P would supply explanatory notes and guides on best practice, case studies, and a directory of subject experts in policy, legal drafting, investigation, law enforcement and technology. In addition, the platform can be used to support the efforts of the Commonwealth Secretariat and other partners to render technical assistance and capacity building to member countries in the form of awareness seminars, training workshops, legal advice, and technical support.

5.1.2 Knowledge Resources

In concert with other partners, the C2P platform would facilitate the development of resource material and create an online repository of knowledge and tools for policy makers, regulatory bodies, judiciaries, chambers of advocates, law enforcement authorities, business (especially ISPs), civil society, and other stakeholders. Resource materials and tools, either developed by itself or by others, would include toolkits, guidelines, handbooks, manuals, country laws, model laws²⁹, treaties, conventions³⁰, reinforced by links to relevant platforms, institutions and other resources.

5.1.3 Online Capacity Building

From time to time the Commonwealth platform can host online events and online training through Podcasts, webinars, group chat sessions leveraging Facebook, Adobe Connect, Skype etc.

5.1.4 Interactive – Networking

The website could also provide space/links to resources that enable stakeholders to self-organise, network, share

²⁹ Commonwealth Model Law on Computer Related Crime – BSA Model on Cybercrime

³⁰ <http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm>

best practice using blogs, Facebook pages, P2P exchanges etc.

5.1.5 Connecting to experts

In response to requests, the Commonwealth Secretariat will connect stakeholders to experts. This will contribute to greater ownership and earlier adoption of measures to realise requisite capacities. It could serve to energise the activity in this area in and between developing countries thereby becoming important contributing partners in the global fight against cybercrime.

5.1.6 Point of Contact for Projects

The Commonwealth Secretariat as part of its Connects programme has a network of country contacts which can be used to advantage to advance the broader Commonwealth Cybercrime Initiative as well as in dealing with specific related issues which may arise from time to time.

5.2 On the Ground Assistance Delivered Regionally and Nationally

5.2.1 Supportive Policy, Regulation, and Enforcement.

The sharing and enhancement of policy skills and know-how can make an important contribution to kick starting countries' cybercrime strategies and advancing their agendas. These can enable governments to put in place the necessary complementary elements to support the preparation, adoption and implementation of cybercrime legislation, including:

- establishing strategic direction and a high level of policy coordination across government ministries
- ensuring adequate enforcement resources
- introducing measures for industry self-governance, such as technical standards and codes of practice
- concluding enforcement partnerships with industry and user groups
- establishing cross-national arrangements for policy coordination and enforcement cooperation.

5.2.2 Preliminary High Level Cybercrime Health-Checks (Legal Framework Status)

Preliminary legislative health-checks would study selected countries' statute books and procedures and prepare brief high level reports on the status of the legal framework with respect to cybercrime against the Model Law, existing international instruments and standards.³¹ These studies

³¹ *Ascertain whether your country has developed necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, General Assembly resolutions 55/63 and 56/121 on*

would be restricted to an analysis of the statutory and regulatory instruments.

5.2.3 Gap Analysis & Need Assessment (More Detailed Legal Framework Analysis outlining specific recommendations for Improvement)

This would require in-country research that would, assess the state of both the existent legal framework as well as its implementation and identify areas for improvement throughout the entire chain/lifecycle of a cybercrime from investigation to prosecution and enforcement, and make recommendations for improvement. This will involve meeting with stakeholders such as Government departments/authorities (Customs/Income Tax, e-government entities , regulators etc.), LEA, prosecutors, the judiciary, policy makers, businesses [including software development, BPOs, telecoms and financial sectors], stock market and others). This could then subsequently be followed by specific technical assistance on legislative drafting for implementation of the recommendations.

5.2.4 Drafting of Legislative/Regulatory instruments (stand-alone/amendments)

Based upon the Gap Analysis & Need Assessment Recommendations, a project for technical assistance with respect to drafting legislation to be introduced (including any amendments to existing laws) may be initiated at the

combating the criminal misuse of information technologies, and regional initiatives, including the Council of Europe Convention on Cybercrime. - **United National General Assembly Resolution**, 17 March 2010, - <http://ods-dds-ny.un.org/doc/UNDOC/GEN/N09/474/49/PDF/N0947449.pdf?OpenElement>

request of the country. This would focus on substantive, procedural and international cooperation gaps.

5.2.5 Technical Assistance for Implementation of Post-Legislative Improvements and Reforms

It would not be sufficient simply to improve the legislative/legal framework if proper implementation is not carried out. Hence, a legislative Improvements' process which results in passing of necessary legislation would need to be followed by implementing secondary legislation, regulations, rules and procedures, strengthening of regulatory frameworks as well as establishment of the necessary institutions (including CERTs). The experience of potential partners in supporting and establishing CERTS would constitute best practice to be adopted.

At the same time legal frameworks would need implementation that would enable, inter alia, cooperation - inter and intra private sector and the technical community, both between one another and also with the government, regulators and/or LEA. These could be through both mandatory, such as regulations, as well as voluntary mechanisms, such as the development of codes of practice, guidelines, MoUs etc. Efforts that have been successful in developed countries could also be considered for implementation including Internet Service Providers and Law Enforcement Cooperation Guidelines and other best practice. Such measures would enable operational and other cooperation between LEA and the private sector both domestically and internationally. Additionally adequate training to enable and familiarise stakeholders in

order to practically carry out the implementation would also be carried out.

5.2.6 Technical Assistance in terms of Training

At every stage (running in parallel) on regional as well as country level, the Initiative will engage in projects that will render technical assistance for capacity building. This will help develop regional and in-country capacity and energise interest, networking, development and exchange of best practices. At each level, training schemes in the form of workshops would also provide an opportunity to do research on the ground and undertake consultations with stakeholders

6 Implementation Methodology and Modules

While the Commonwealth is providing the leadership for this Initiative, it does not have, nor can it aspire to have other than minimal resources to launch the initiative and provide the operational support. It is for these reasons that the Commonwealth Secretariat recognises the need for securing partners and the endorsement of key Member States for the initiative in the lead up to CHOGM. The partners and national development agencies are vital to the successful launch and implementation since they hold the requisite resources both financial and technical. Indeed without these partnerships, it will simply not be viable for the Commonwealth to proceed with implementation.

Thus, in preparation for the presentation of this initiative to Heads of government, there is much advance activity envisaged in engaging partners and getting member countries signed up to it. The following events have provided an opportunity to introduce the planned Commonwealth Cybercrime Initiative and elicit feedback:

- The Commonwealth Law Minister's meeting on July 11th 2011
- High Level Meeting on Cybercrime (Quintet) – July 2011
- West African IGF 2011
- Caribbean IGF – August 2011
- East African IGF – August 2011
- Southern African IGF – September 2011
- IGF September 2011
- Commonwealth Committee of Whole – September 2011
- Commonwealth Business Forum - October 2011

The feedback from these events has been taken into account in the presentation of the Initiative to the Heads of Government in October 2011 for their approval.

In all these interactions it was of the utmost advantage for the Initiative to be framed in the context of issues of Internet security, anti-money laundering

cooperation by identifying the Model Law, where relevant legislation is not in place, as a means of enabling necessary cooperation on security and anti-terrorism efforts.

6.1 C2P – A Platform for Resources and Tools

The Commonwealth Secretariat's C2P in concert with the CIGF website will provide a very useful platform for knowledge transfer by virtue of subject repositories and social networking functionality.

6.2 Preparatory Phase (Regional Outreach & Energizing)

As referenced previously there has been considerable activity leading up to CHOGM in order to line up support and coincident with this, the Commonwealth Secretariat has to be suitably positioned to follow through with launching the Initiative expeditiously following CHOGM, subject to its endorsement. In this latter regard, in order to prepare the ground work for initiating various in-country assistance projects, it would serve the strategic interest to outreach and build on regional support for in-country efforts.

Certain regions can be selected where:

- there is a need which takes on a strategic priority
- certain levels of legislative reform already exists or is underway
- a willingness to participate and take advantage of this Initiative exists or is likely
- there exists a demonstrated commitment to international norms including human rights principles, in particular freedom of expression and safeguards, such as judicial or other independent supervision etc.
- willingness to adopt international best practice and cooperate internationally
- there exists a demonstrable need for assistance based on the potential impact of Cybercrime linked to a region .

With the support of partners (mentioned in section 8), initially seminars and workshops in such regions could play an important role in preparing the countries to capitalize on the assistance the Initiative makes possible. These interactions will also provide an invaluable source of experience and insight into the various levels of needs, requirements, challenges and opportunities in a particular jurisdiction.

6.3 In-country Assistance

While assistance under this Initiative can cover a pretty broad spectrum, the specifics of what assistance may be required is something that will have to be analysed in each and every case and following significant interactions in order to establish the current state of play in any jurisdiction. Assuming all this, following is a hypothetical sequencing of phased initiatives:

Phase 1 – Supportive Policy Frameworks and Harmonisation of Legislation

- Awareness
- Putting in place through discussion with policy makers and regulators the necessary complementary elements to support the assessment, preparation, adoption and implementation of cyber-crime legislation
- Need Assessment & Gap Analysis of the status of Legislation and Law Enforcement capacities (this will allow for better scoping of the Assistance Project)
- Technical Assistance & Mentoring for Legislative Drafting & Legislative Implementation- (includes Capacity Building)
- Stakeholders:
 - Parliamentarians and Legislators
 - Police and Prosecutors
 - Judiciary
 - Policy Makers and Regulators

- Private Sector (ranging from IT companies, Financial Institutions, ISPs etc.)
- Civil Society, Educators & General Public

Outcomes:

- Establishing a plan for strategic direction and a high level of coordination across government ministries
- Policy measures and legal frameworks for industry self-governance, such as technical standards and codes of practice
- Establishing enforcement partnerships with industry and user groups
- Establishing cross-national arrangements for policy coordination and enforcement cooperation.
- Submission of Draft Legislation which is consistent with the Commonwealth Model Law and existing international standards and instruments thus, contributes towards a safer, more secure and reliable internet
- To be followed by Technical Assistance to Legislature and Advocacy with Parliamentarians and other Policy Makers for passage through Legislature

Phase 2 – Implementation Post- Legislation

Technical Assistance, Mentoring & Capacity Building

Drafting Detailed Implementing Regulations/Rules for and Training of:

- Specialised Investigative Powers (LEA)
- Specialised Prosecutorial Services (Prosecutors)
- Specialised Procedural Codes (Ministry of Law/Justice)
- Specialised Evidence Collection (Forensics – Ministry of Law/Justice)
- Specialised Judicial Policies / Designated Benches (Judiciary)

- 24x7 Points of Contact (Ministry of Interior/CERT)
- Specialised Ministerial/Competent Authority Cadres (Ministry of IT/Interior)
- Secondary legislation (rules, regulations, procedures) for Implementation
- Legal Frameworks that enable both intra and inter private sector and technical community cooperation as well as cooperation with government, Regulators and LEAs.

Outcomes:

- Submission of Draft Regulations/Rules and Enabling Legal Frameworks
- Training workshops of all of the above and technical assistance for facilitating the establishment of the various institutions with the requisite specialised expertise throughout the investigative and prosecution chain/lifecycle.

Phase 3 - International Cooperation

Technical Assistance, Mentoring & Capacity Building:

- through training, readiness preparations and liaison for those recipient member states requesting assistance on accession or ratification of existing international conventions
- Establishment of an International Best Practice CERT
- Detailed Internal Processes for International Cooperation (Forms, Communications etc.)
- Liaison with International Conventions and Organisations
- Assisting regulators and law enforcement obtain, install and utilise appropriate tools for the operational enablement of investigations including, computer forensics labs, and infrastructure for monitoring, surveillance, interception and preservation of

computer data, traffic data and intelligence with respect to cybercrime and cyber security.

Possible Outcomes:

- Promotion of norms for acting in cyberspace across the international community
- Assistance rendered, when requested by a state, with respect to international institutions to liaise, cooperate and possibly accede to international instruments.
- Establishment of an in-country CERT (CERT important, but in addition jurisdictions need to have appropriate environment, technology and skills to launch or collaborate in investigations.
- Assisting the country in procuring implementing and installing operational tools and infrastructure such as:
 - Computer Forensics labs
 - Tools for monitoring, surveillance, interception and preservation of various forms of data (computer data, traffic data, subscriber data etc.)
- Establishing sustainable programs for training and building human capacity to utilise the above and enable effective cooperation and information sharing both domestically and internationally.

Phase 4 - Continuing Training, Mentoring & Capacity Building & Exchange Programs [Assistance with ongoing International Cooperation (handholding)]

- Train the Trainers:
 - Law Enforcement Agency – Investigators and Forensic Experts
 - Prosecutors
 - Judiciary

- Private Sector awareness, training and facilitation of cooperation (development of LEA-Private Sector/Technical Community Guidelines – e.g. LEA-ISP Guidelines)
- Civil society awareness raising and the engagement of civil society organisations for empowerment of individuals in Cyber security
- Exchange Programs – Sharing of Best Practices
- Setting up domestic capacity for ownership and sustainability

Outcomes:

Development of sustainable local institutions to enable:

- continuing development,
- improvement and growth

of specialised international best practice expertise and skills for the successful investigations and prosecutions of domestic and cross-border cybercrimes through effective international cooperation.

7 Expertise Required for Implementation

The nature of the skilled expertise required to assist in the development of capacity is highly specialized. This has to do with the dynamic nature of the Internet and its associated technologies. The following aims to identify some of the key resources which may be required to provide virtual or on the ground assistance:

- Policy

Expertise with respect to cybercrime related policies and experience of implementation in developing countries targeted towards:

- establishing strategic direction and a high level of coordination across government ministries;
- ensuring adequate enforcement resources;
- measures for industry self-governance, such as technical standards and codes of practice;
- concluding enforcement partnerships with industry and user groups;
- establishing cross-national arrangements for policy coordination and enforcement cooperation.

- Legal

- Expertise with international legal frameworks such as bilateral cooperation and exchange treaties, guidelines, legislations and procedures for detection, investigation, prosecution and international cooperation with respect to cybercrime, especially the challenges faced by developing countries.
- Expertise in the area of comparative legislative analysis, legislative drafting (consistent with international best practice) with a particular focus on developing country legislative requirements and experiences in general but in particular in the following areas:

- Cybercrime
- Cyber security
- Electronic Transactions
- Electronic Evidence
- Electronic Payment Systems
- Data Protection/Privacy
- experience in training and sensitization of prosecutors, law enforcement agents, forensic experts;
- experience in working with international multi-stakeholder technical bodies dealing with cyber security and global internet policy
- experience in working with developing country technical bodies dealing with cyber security and global internet policy
- experience with developing country and international business associations focused on electronic transactions, Internet policy, data protection and cyber security;
- expertise in dealing with developing country regulators, government/authorities on policy, legislation and advocacy especially in cyber security, cybercrime and the Internet.
- Technical (Private Sector, Technical Standard Setting Bodies, Experts/Consultants)
 - experience in setting up technical environments to enable Internet/telecom monitoring, investigation and intervention and provide associated training;
 - experience in setting up CERTs and provide associated training;
 - experience in private sector or technical body dealing with Internet standards, & policies, cyber security, telecom
 - experience with challenges faced by developing countries in implementation of technical standards for the Internet and cyber security

- experience with challenges faced by developing countries in handling incident response and cross-border cooperation in investigating cybercrime
- experience in working in global fora with respect to global Internet policy and cyber security.

8 Potential Partners and Roles (in alphabetical order)

8.1 Centre for Internet Safety, Cyprus

Cyprus Safer Internet Centre has been active in Cyprus since 2006. The Centre has been created as part of the Cyber ethics project which is co-funded by the Safer Internet Plus Programme of the European Commission. Cyprus Safer Internet Centre is a consortium made of five partners which are Cyprus Neuroscience and Technology Institute, Ministry of Education and Culture – Cyprus Pedagogical Institute, CYTA – Cyprus Telecommunication Authority, The Olive Branch Foundation and the Pan Cyprian Coordinating Committee for the Protection and Welfare of Children. The Centre serves as an Awareness Node along with its Hotline and the Helpline. The Helpline has been active since 2009 while the Hotline has been active since 2006. The centre undertakes various awareness raising activities along with the Hotline and Helpline services it provides. Throughout aforementioned Cyber ethics project Cyprus Safer Internet Centre, its partners, associated partners and advisory board have generated a widespread network across Europe on Internet Safety issues. Therefore, the Centre can serve as a link between the Commonwealth Initiative and the European Union for the good information flow amongst each other mainly on best practices in individual countries. Cyprus Safer Internet Centre can also willingly share the resources and experiences obtained during the course of the six years of implementing the Cyber ethics project.

8.2 Centre for Internet Safety, University of Canberra

The Centre for Internet Safety (CIS) at the University of Canberra was created to foster a safer, more trusted Internet by providing thought leadership and policy advice on the social, legal, political and economic impacts of cybercrime and threats to cyber security. The CIS focuses on providing tools and techniques for government, business and individuals to embrace the benefits of the online environment whilst addressing the misuse of Internet and related technologies.

The CIS is pleased to contribute its expertise in research and education for this Initiative. The CIS shares its ideas via publications, roundtables, conferences, public speaking and media engagements as actionable insights for governments, businesses and individuals.

8.3 Children's Charities' Coalition on Internet Safety

The Children's Charities' Coalition on Internet Safety brings together all of the UK's large professional child welfare and child protection organizations. Each agency shares a huge enthusiasm for the new technologies and is anxious to ensure that all children and young people have access to it. But equally the charities are determined that such access is both safe and appropriate. CHIS is a campaigning organization. It works with and lobbies Government, Parliament, the media and the internet industry in pursuit of its goals.

CHIS member organizations have a comprehensive range of expertise in child protection, child welfare and child development. They work extensively with individual children, young people and their families. A number run residential schools or similar facilities, some provide therapeutic or other forms of intervention and support or are engaged in arranging adoption and fostering placements. Several member organizations have wide ranging knowledge of how sex offenders prey on children, how children are trafficked, how sex tourism operates, how bullying can manifest itself, the harm it can do and what can be done to counter or recover from it. Every member organization of CHIS has professional standing within the world of child safety.

8.4 COMNET Foundation for ICT Development

COMNET is an international Foundation whose mission is to help realise the transformational potential of Information and Communication Technologies (ICT) for development, among Commonwealth and other developing countries.

The Foundation is the Commonwealth Secretariat's lead partner agency responsible for the Commonwealth Connects Programme and the

Commonwealth Internet Governance Forum which has been driving the development of the Commonwealth Cybercrime Initiative in collaboration with representatives of member governments and partner agencies.

Through the CIGF, COMNET will continue to raise awareness of the Initiative and provide the co-ordination in its launch and implementation working in conjunction with partners to identify candidate projects and in sourcing the relevant technical expertise and funding.

8.5 Commonwealth Business Council (CBC)

The Commonwealth Business Council (CBC) provides leadership in increasing international trade and investment flows, creating new business opportunities, promoting good governance and corporate social responsibility, reducing the digital divide and integrating developing countries into the global market. In fulfilling its mission, CBC strives to provide a bridge between private sector and governments, between emerging markets and between small businesses and international private sector.

The Initiative creates a more secure global environment and therefore enables secure and reliable delivery of services, thereby contributing to more favourable conditions for economic growth and global trade. Hence, the Initiative would be beneficial to Commonwealth businesses. For their part, the Commonwealth businesses and their international linkages, expertise and experience in tackling incidents of cybercrime and especially their ability to bring resources to the Initiative makes the CBC an important multistakeholder partner. The CBC could also play an important role in coordinating non-Commonwealth business' partnerships, resources and funding for the Initiative.

8.6 Commonwealth Lawyers Association (CLA)

The CLA Commonwealth countries share a substantial common ground in their legal systems and the lawyers of these countries have much to learn from the comparative experience of their colleagues in other

jurisdictions. This extends to many aspects of legal education and legal practice and here too there is much to be shared. The profession around the Commonwealth is committed to the preservation of the highest standards of ethics and integrity and to the furtherance of the rule of law for the benefit of society. As a pan-Commonwealth body, the CLA provides support in the pursuit of these objectives. As such the CLA could provide much support in terms of networking, awareness and advocacy for the harmonisation and updating of cybercrime related legal frameworks, especially in developing countries through the Commonwealth.

8.7 Commonwealth Parliamentary Association (CPA)

The CPA provides a unique platform for cooperation between Parliaments in Commonwealth nations and can be expected to contribute to the adoption and implementation of harmonised cybercrime legislation by the Legislatures of the Commonwealth

8.8 Commonwealth Secretariat

The Commonwealth Secretariat through COMNET and the Commonwealth IGF will provide the leadership and coordination role for the initiative whilst encouraging knowledge transfer. The Commonwealth C2P platform provides a focal point for the sharing of resources.

The Commonwealth Secretariat will provide seed financing to enable the launch and operational support of the initiative. It will also assist in brokering with partners for specific in-country projects and providing global leadership by:

- placing cybercrime on the agenda for CHOGM and seeking endorsement of this initiative;
- incorporate the combating of cybercrime as an area for technical assistance and capacity building under GIDD and LCAD's programming;

- use the COMMONWEALTH CONNECTS network to promote best practice and influence adoption of appropriate initiatives to combat cybercrime.

8.9 Commonwealth Telecommunications Organisation (CTO)

With its long standing presence in the Commonwealth and most particularly its network of sector specific specialists, it is envisaged that the CTO would be a major player in this Initiative. The organisation could play a role in planning and convening relevant outreach events, and in identifying technical experts to provide for specific in-country projects.

8.10 Council of Europe

As the principal player in the drafting and implementation of the Budapest Convention, the Council of Europe has been supporting countries on all continents in:

- the strengthening of cybercrime legislation (substantive and procedural law, including conditions and safeguards to protect human rights and rule of law principles) using the Budapest Convention as a guideline and framework of reference
- the creation of high-tech crime and other specialised units on cybercrime
- law enforcement and judicial training
- public-private cooperation, in particular law enforcement/service provider cooperation
- efficient international cooperation, including 24/7 points of contact
- financial investigations into criminal money on the Internet
- the protection of children against sexual exploitation and abuse
- the development of cybercrime strategies.

In addition to the Budapest Convention, specific tools on training, law enforcement/service provider cooperation and others have been developed. Standards and instruments related to cybercrime – such as on money laundering, terrorism, protection of children, and protection of personal data – are made use of when assisting countries.

As an organisation aimed at human rights, democracy and the rule of law, the Council of Europe is pursuing a criminal justice approach against cybercrime. The organisation is therefore cooperating with criminal justice authorities worldwide and can draw on significant public and private sector subject-matter expertise.

The Council of Europe is following a multi-stakeholder approach and is thus an interested partner in the Initiative.

The Council of Europe being committed to assisting countries in the implementation of the principles of the Budapest Convention, will supporting those countries with appropriate legislation who may wish to accede to this treaty and make use of it as a framework for international cooperation and work with the Commonwealth Cybercrime Initiative in this respect.³²

8.11 Diplo Foundation

Diplo Foundation is a leading provider of capacity building in the field of Internet governance. Over the last 10 years, its IG capacity building programme involved more than 1100 participants from 186 countries, including 53 Commonwealth countries. Diplo also successfully carried out an EU-ACP supported capacity building programme for the ACP (Africa - Caribbean - Pacific) countries customised to regional challenges. In

³² P.20 ‘...allies regularly depend upon cooperation and assistance from other countries when investigating and prosecuting cybercrime cases. This cooperation is most effective and meaningful when the countries have common cybercrime laws, which facilitates evidence-sharing, extradition, and other types of coordination. The Budapest Convention on Cybercrime provides countries with a model for drafting and updating their current laws, and it has proven to be an effective mechanism for enhancing international cooperation in cybercrime cases’ – White House International Strategy for Cyberspace, May 2011.

– http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

addition to providing online and in situ training in the foundations of Internet governance, specialised programmes were developed as advanced courses in cyber security, privacy and data protection, infrastructure and intellectual property rights, as well as in policy research methodologies and in ICT policy and strategic planning.

In this new cyber security Initiative, Diplo can contribute through its highly effective capacity building methodology, consisting of policy training, policy research and policy immersion. By developing customised programmes for specific national contexts, this approach facilitates the building of national, institutional and individual capacities in the field of cyber security policy. It also aims at creating multi-stakeholder communities of practice for sustainable impact.

8.12 International Centre for Missing and Exploited Children (ICMEC)

The International Centre for Missing and Exploited Children is an international non-governmental organization working globally to protect children from abduction and sexual exploitation. ICMEC is pleased to contribute its Child Pornography: Model Legislation and Global Review as a resource for the initiative. Coupled with technical assistance, this report serves as a tool for assessing current and proposed anti-child pornography legislation, as well as drafting new legislation. In addition, ICMEC will offer several other resources relevant to financial and industry players working to disrupt the economics of commercial child pornography globally. ICMEC may also provide technical assistance for training law enforcement to investigate computer-facilitated crimes against children.

Through research, technical assistance, advocacy, and training, ICMEC strives to inform policymakers, law enforcement, and others in an effort to enhance and enrich frontline practices.

8.13 International Corporation for Assigned Names & Numbers (ICANN)

ICANN is a global organization that coordinates the Internet unique identifier systems for worldwide public benefit, enabling a single, global interoperable Internet. ICANN's inclusive multi-stakeholder model and community-developed policies facilitate the use of the Internet's systems unique identifiers by the billions of computers, phones, devices and people connected into one Internet and the people who use them.

ICANN could facilitate the delivery of training on the domain name system, its structure and multi-stakeholder ecosystem, and technical assistance with regard to protection of domain name security with capacity building in countries for development of knowledge and expertise for investigations related to the domain name system.

8.14 International Cyber Security Protection Alliance (ICSPA)

The ICSPA was established in 2010 and recently launched in London with the UK Prime Minister and government's support and endorsement. Its mission is to:

- Enhance the online safety and security of business communities, by helping to deliver resources and expertise from the private sector to support both domestic and international law enforcement agencies in their task of reducing harm from cybercrime. This will include raising public sector funding from governments and institutions that wish to help increase the capacity and capability of cybercrime units in countries which face the greatest challenges.

The ICSPA's founding members include multi-national corporations (such as EADS Cassidian Cyber Security, McAfee, Visa Europe and Trend Micro) whose senior executives are committed to harnessing the technical expertise, experience and skills of their workforce to support project work in many countries around the world. By working closely with the ICSPA, Commonwealth countries could benefit directly by helping the ICSPA to identify work programmes that meet the aims and objectives of both the CIGF and the ICSPA.

With the practical field experience of alliance members, it makes ICSPA an eminently suitable partner to work in conjunction with the Commonwealth in this vital global Initiative.

8.15 International Telecommunication Union (ITU)

The ITU is a partner organisation of the Commonwealth IGF and is an important stakeholder in matters relating to the Internet. The ITU provides technical assistance to Member States on cybercrime and Cyber Security, making available technical expertise and cybercrime resources to facilitate the establishment of technical and legal measures and legislative frameworks at the national level. The ITU aims at building and/or strengthening national and regional capacities to counter cybercrime and it ensures extensive reach to almost all required stakeholders in countries and regions. ITU has extensive programmes on all continents in order to assist countries and regions to harmonize their cybercrime laws.

The ITU Toolkit for Cybercrime Legislation aims to provide countries with sample legislative language and reference material that can assist in the establishment of harmonized cybercrime laws and procedural rules. Another publication by the ITU Understanding Cybercrime Guide provides a resource of extensive information aimed at particularly developing countries.

ITU is the pre-eminent global standards body for telecommunications and information and communication technologies (ICTs). Building confidence and security in the use of ICTs is a major objective. Over seventy technical standards (ITU-T Recommendations) focus on security including cyber security. For example ITU has adopted a suite of global technical standards that provide a common framework for exchanging information on cyber security known as CYBEX; Recommendation ITU-T X.509 is the cornerstone for designing applications related to public key infrastructure (PKI); and Recommendation ITU-T X.805 provides for an end-to-end architecture description from a security perspective.

The experience of ITU in establishing Computer Incident Response Teams (CIRT) would represent a valuable resource.

The ITU's involvement in the Initiative would bring outreach to other multi-lateral agencies and non-Commonwealth countries, as well as providing a global perspective for the achievement of international cooperation.

9 Funding Support:

9.1 Primary Funding Partners

This is a landmark Initiative for the Commonwealth which is only possible with the commitment of its partners who bring to this access to specialist resources and financing. Thus the Commonwealth's contribution to this can be seen as largely value-added with much of the necessary resources coming from its partners and the business community for specific in-country projects. The Commonwealth however will need to establish an appropriate fund to cover the following:

- up-dating of Commonwealth Model law;
- assembling a repository of relevant policies;
- launching of the initiative;
- providing leadership and ongoing operational support;

9.2 Other Supporting Partners

Since the development of the Internet is generally coordinated and managed by private sector-led organisations (e.g. APWG) and businesses (e.g. Symantec, AT&T, Microsoft), their involvement, technical assistance and support for the Initiative is vital and is expected to constitute a complementary source of funding for in-country projects

10 Governance Structure

The impetus and preparatory work for the Commonwealth Cybercrime Initiative grew out of the Commonwealth Internet Governance Forum led by the COMNET Foundation for ICT Development. Initially, therefore, the governance arrangements for the Cybercrime Initiative would be formed around the COMNET Foundation, which has a well established mandate and role in the area of Internet policy.

Established as an international not for profit Foundation in 1995, COMNET has in recent years been assigned the lead by the Commonwealth Secretariat in the implementation of its ICT for development programme which is premised on technology and knowledge transfer between Commonwealth member states aimed at fast tracking such development. It is in this context that COMNET has been leading the Commonwealth Internet Governance Forum thus giving it the appropriate credentials and statutory requirements to co-ordinate the launch and provide the operational support for the Commonwealth Cybercrime Initiative. (See Appendix). Reporting to its Board of Directors, COMNET will be building on this statutory framework to implement a Governance Structure as follows:

10.1 Commonwealth Cybercrime Initiative Steering Group

This will be comprised as follows:

- Chairman IGF – Chairman
- Representative Commonwealth Secretariat
- Representative Council of Europe
- Representative ITU
- Representative UK government – Vice Chairman
- Representative Sri Lanka government
- Representative Law Enforcement Agencies (SOCA)
- Representative Canadian Government
- Representative CTO
- Representative Legal Adviser
- CIGF Coordinator COMNET – Secretary

Its Terms of Reference will be as follows:

- Driving the formulation of the Initiative;
- Providing appropriate liaison with Commonwealth Secretariat and Commonwealth Connects Steering Committee;
- Liaising with Constitutional and Legal Affairs Group of Commonwealth Secretariat in order to ensure convergence with Commonwealth Law Ministers initiative.
- Developing a strategy for its launch and implementation,
- Securing implementation partners;
- Raising awareness and securing buy in of member states,
- Endeavouring optimal technology/knowledge transfer in building capacity;
- Identifying financial and technical resources for implementation;
- Commissioning relevant research to avoid replication and to promote fast track implementation;
- Approving projects and overseeing their implementation;
- Ensuring appropriate governance structure is in place to oversee Initiative.

10.2 Advisory Committee: Accountable to the Executive Management

The Advisory Committee will be comprised of a representative from each of the organisations identified as follows:

- Chairman CIGF – Chairman
- International Corporation of Assigned Names and Numbers
- Diplo Foundation
- International Cyber Security Protection Alliance
- International Centre for Missing and Exploited Children
- Commonwealth Business Council
- Commonwealth Parliamentary Association
- Commonwealth Lawyers Association
- Commonwealth Judges Association

- Commonwealth Law Education Association
- East Africa IGF
- Caribbean Telecommunications Unit
- Secretariat for the Pacific Community
- Centre for Internet Safety, Canberra
- Cyprus Centre for Internet Safety
- CIGF Coordinator – Secretary

Any Partner organisation that will join the Initiative as negotiations continue will be invited to join the Advisory Committee.

The Terms of Reference of the Committee will be to advise the Executive Management including as follows:

- Providing input into the formulation of the Initiative and the strategy for its implementation,
- Identifying and recommending candidate countries' and projects for the Initiative;
- Helping secure champions and contributing expertise,
- Providing input into the formulation of projects,
- Proposing participating partners and resources for specific projects,
- Contributing to implementation of projects as a group or individual members,
- Provide general advice and direction in the interest of progressing the implementation of the Commonwealth initiative.

10.3 The Secretariat

This will be provided by the COMNET Foundation for ICT Development, as the agency tasked by the Commonwealth Secretariat to lead the Commonwealth

Connects Programme and in turn, the Commonwealth Internet Governance Forum.

A COMNET statutory requirement is for the conduct of an annual audit of its accounts by independent and accredited auditors.

11 Forward Plan

Given the positive statements of support for Commonwealth cyber security initiative that emerged from the Law Ministers meeting in July 2011, it is now incumbent on the Commonwealth Secretariat to muster the partnerships, and seek the endorsement of as many member governments in the period leading up to CHOGM. Regional IGFs in Africa and the Caribbean have provided the opportunity for this, as did the IGF 2011 in Nairobi. This Commonwealth initiative was presented at all these events.

This programme of presentations is to be followed by placing the Initiative on the agenda of the Commonwealth Heads of Government Meeting (CHOGM) in Perth in October 2011 for formal endorsement by Heads of Government. Side events at CHOGM will also serve as an opportunity to engage with and showcase support of stakeholders. Cyber security now features in the Commonwealth Business Forum programme and efforts will be made to broaden consultation on the Initiative with other important constituencies such as civil society, youth and the media.

This should be followed by a series of regional workshops. At each workshop one or two countries can be selected for the initial implementation of the various Phases outlined in Section 5.

It is highly recommended that:

- due to the urgency that exists in combating cybercrime, the Initiative be launched as soon as possible, especially keeping in mind the ancillary and additional benefits that such work will have in the international cooperation for combating terrorism, money laundering and other urgent threats.
- the formats of engagement (be it the website or regional/country-specific trainings and assessments) should ensure multi-stakeholder participation, support and input.

12 Conclusion

The formulation of this proposal has been driven by a team consisting of a number of Commonwealth member country representatives, multilateral agencies including the Council of Europe and the International Telecommunication Union and a number of Commonwealth partner agencies. As the proposal started taking shape and we broadened our consultations, several other entities expressed an interest in collaborating in this initiative and are now reflected in Section 8. This can be taken as testament to the merit of the initiative and its coherent and practical approach to contribute to an enhanced cyberspace. In leading this initiative the Commonwealth Secretariat is relying on the capabilities, developments and resources of these partner agencies in its launch and implementation.

In leading this initiative the Commonwealth Initiative will be playing a pivotal role in coalescing support in particular among developing countries, for collaborating in the global fight against cybercrime by:

- contributing to policy frameworks that would create an enabling environment for implementation of the following;
- encouraging and assisting in the implementation of a minimum harmonised standard for cybercrime (along the lines of the Commonwealth Model Law³³ the Harare Scheme³⁴ and existing international standards and instruments).
- greatly enhancing real-time cooperation at the operational, investigative and prosecutorial levels between these countries and developed countries;
- enable the implementation of industry standards, codes and best practices for greater operational cooperation;
- building capacity in these countries; and

³³ 'a model law on the basis of the work of the Council of Europe on the Draft Convention on Cyber Crime (COE Draft Convention).'

http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf

³⁴ Commonwealth Mutual Assistance In Criminal Matters
http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/2C167ECF-0FDE-481B-B552-E9BA23857CE3_HARARESCHEMERELATINGTOMUTUALASSISTANCE2005.pdf

- providing on the ground support to have in place the requisite legal, human and technical capacity which they desperately need..

The Initiative is intended to serve the broadest community interests in contributing to a safer, more secure and reliable Internet by providing a uniquely effective means of raising standards in developing countries with respect to their abilities for combating and cooperating in the global fight against cybercrime. It will develop capacity in the areas of policy, legislation, regulation, training, capacity building, operational support, infrastructure and international cooperation.

Furthermore, this Initiative is not merely a one way street that only aims to benefit developing countries. The tremendous financial and security threat that cybercrime poses towards the developed world means that this Initiative would also, contribute a strategic benefit for the global economy by denying cybercriminals safe havens from which to operate.

**COMNET Foundation for ICT Development
Consolidated Statute**

Article 1

Establishment and Name

An international, non-governmental, self-sustaining, non-profit-making Foundation, originally founded as the Commonwealth Network of Information Technology for Development (COMNET-IT), is being hereby renamed the COMNET Foundation for ICT Development, hereafter called 'the Foundation'.

Article 2

Duration

The duration of the Foundation is indeterminate.

Article 3

Original Founders

The following organisations or entities are the original sponsors of the Foundation:

- a) The Commonwealth Secretariat, Marlborough House, Pall Mall, London, SW1Y 5HX, United Kingdom, which provided initial funds for COMNET-IT.
- b) The Government of Malta as the host for Secretariat, with responsibility for Administrative functions of the Foundation.
- c) Management Systems Unit Limited, Villa Portelli, Kalkara CSP10, Malta, the executing agent on behalf of the Government of Malta providing the physical accommodation, administrative and technical support for the Foundation's Secretariat.
- d) The National Centre for Software Technology, Bombay, India, providing network development expertise and operational support.

Handwritten signatures:
A
M
A

Article 4

Aims

The aims of the Foundation are to

- a) promote communications between people engaged in the development process, whether as organised groups or individuals, through the use of computer networks, with the purpose of accelerating social and economic development
- b) promote a greater understanding of the role of information technology in accelerating social and economic development
- c) facilitate the provision and exchange of information about development related issues, existing skills and expertise, as well as available products and services using computer-based communication networks
- d) provide a means of communicating with Commonwealth partners about new developments in research, applications, products and services involving new information technologies and thus encourage technology transfer and interdisciplinary collaboration
- e) advance literacy, especially among people from technologically less advanced countries, in the use of IT-based communication networks as a means of improving and expanding communication between persons or institutions responsible for or engaged in development activities.

Article 5

Methods

In seeking to achieve its aims the Foundation may

- a) encourage and facilitate the use of existing computer-based communication networks for conducting dialogue and information exchange between people and groups specifically interested in fostering social and economic development.
- b) provide and facilitate the transfer of computer-based networking technology, by supplying network start-up technology and assistance, carrying out network maintenance and servicing; and providing training to install, maintain, service, administer and manage computer-based networks.
- c) engage in research and publication, including conducting case studies, on the use of computer networks and other information technologies in selected areas of socio-economic development.
- d) provide access to information on various topic areas related to ICT as a driver for socio-economic development.
- e) promote technical co-operation between people and institutions in Commonwealth countries with regards to the development and application of computer-based communications and information technologies.
- f) enter into contractual agreements, including agreements to implement projects on behalf of non-governmental and inter-governmental institutions.
- g) engage institutions having the appropriate technical capacity in directly undertaking operational activities involving computer-based communications and information technologies
- h) use any other means appropriate to the pursuance of its aims.

Handwritten initials: MK