

Commonwealth ICT Ministers Forum 2014

Marlborough House, London

3 - 4 March 2014

Commonwealth Cybergovernance Model

1. Introduction

1.1. Recognising the central importance of the internet to Commonwealth members and following the *Abuja Declaration of Proposed Commonwealth Cybergovernance Model of 9 October 2013 and subsequent consultations*, the Commonwealth Telecommunications Organisation offers this draft set of principles for consideration and adoption during the Commonwealth ICT Ministers Forum. The principles are intended to guide Commonwealth members to plan and implement practical actions in policy development, regulation and legislation, cross-border collaboration, capacity building, technical measures and other operational activities.

2. Cyberspace – the internet and more

2.1. We are in an era of changing economic circumstances creating both opportunity and uncertainty, giving rise to new trade and economic patterns together with unforeseen threats to peace and security, and a surge in popular demands for democracy, human rights and for broadened social and economic opportunities. Previously unimagined access to information and communication between individuals across our planet is driving economic and social development in the 21st century. Cyberspace¹ provides this access, helping us to bridge the digital divide while influencing every aspect of our economic and social activities. Cyberspace is becoming our global central nervous system. Cyberspace continues to develop at a pace unparalleled in our history - growth is anticipated from 2bn to 4bn users by 2020², many in developing countries. This pace of change necessitates urgent action in reaching consensus on Cybergovernance.

2.2. Its open, decentralised and distributed nature, that empowers the individual, has fostered innovation, collaboration and rapid development. Enjoyment of those benefits relies upon its safety, security and resilience. Cyberspace can also be a vehicle for crime, extremism and other social ills³. Governments, industry, civil society and users have a shared responsibility⁴ to tackle those threats to society. Necessary security measures may be in tension with the very features that have made Cyberspace a success and, in

¹ Cyberspace encompasses the internet, mobile and fixed-line access, plus all the networked machine-to-machine communications and other networked communications that are beyond the World Wide Web.

² Microsoft report "Linking Cybersecurity Policy and Performance", February 2013

³ ITU Regional Development Forum for the AFR Region, meeting in Accra, Ghana 1 October 2013

⁴ World Economic Forum report "Risk and Responsibility in a Hyperconnected World", January 2014

determining an equitable balance, our behaviour in Cyberspace will benefit from our shared Commonwealth values that govern many aspects of our lives.

3. Applying Commonwealth values in Cyberspace

3.1. The Commonwealth Charter of March 2013 reflects the values and aspirations which unite the Commonwealth - democracy, development, human rights and the rule of law. The Charter expresses the commitment of member states to the development of free and democratic societies and the promotion of peace and prosperity to improve the lives of all peoples of the Commonwealth. It also acknowledges the role of civil society in supporting the goals and values of the Commonwealth.

3.2. The principles concerning our use of Cyberspace today and the evolving nature of Cyberspace tomorrow should be derived from, should respect and reflect our shared Commonwealth values as set out in the Commonwealth Charter. Within the context of the Charter as a whole, we identify the key characteristics, which led to our principles, as exemplified in Appendix 1. This analysis is based on the principle that what is unacceptable off-line is unacceptable on-line. Priorities for practical action, in accordance with these principles, will depend on the prevailing circumstances in each country.

4. Commonwealth principles for the use of Cyberspace

4.1. As we operate in Cyberspace and work with others to shape its continuing development, we will use the following principles to guide our decisions, actions and demonstrate our progress towards meeting these principles. The principles are best considered collectively and not each in isolation without regard to the whole because frequently some are in tension with each other. We reiterate the urgency with which these issues need to be addressed.

Principle 1: We contribute to a safe and an effective global Cyberspace

- as a partnership between public and private sectors, civil society and users, a collective creation;
- with multi-stakeholder, transparent and collaborative governance promoting continuous development of Cyberspace;
- where investment in the Cyberspace is encouraged and rewarded;
- by providing sufficient neutrality of the network as a provider of information services;
- by offering stability in the provision of reliable and resilient information services;
- by having standardisation to achieve global interoperability;
- by enabling all to participate with equal opportunity of universal access;
- as an open, distributed, interconnected internet;
- by providing an environment that is safe for its users, particularly the young and vulnerable;
- made available to users at an affordable price.

Principle 2: Our actions in Cyberspace support broader economic and social development

- by enabling innovation and sustainable development, creating greater coherence and synergy, through collaboration and the widespread dissemination of knowledge;
- respecting cultural and linguistic diversity without the imposition of beliefs;
- promoting cross-border delivery of services and free flow of labour in a multi-lateral trading system;
- allowing free association and interaction between individuals across borders;
- supporting and enhancing digital literacy;
- providing everyone with information that promotes and protects their rights and is relevant to their interests, for example to support transparent and accountable government;
- enabling and promoting multi-stakeholder partnerships;
- facilitating pan-Commonwealth consultations and international linkages in a globally connected space that also serves local interests.

Principle 3: We act individually and collectively to tackle cybercrime⁵

- nations, organisations and society work together to foster respect for the law;
- to develop relevant and proportionate laws to tackle Cybercrime effectively;
- to protect our critical national and shared infrastructures;
- meeting internationally-recognised standards and good practice to deliver security;
- with effective government structures working collaboratively within and between states;
- with governments, relevant international organisations and the private sector working closely to prevent and respond to incidents.

Principle 4: We each exercise our rights and meet our responsibilities in Cyberspace

- we defend in Cyberspace the values of human rights, freedom of expression and privacy as stated in our Charter of the Commonwealth;
- individuals, organisations and nations are empowered through their access to knowledge;
- users benefit from the fruits of their labours; intellectual property is protected accordingly;
- users can benefit from the commercial value of their own information; accordingly, responsibility and liability for information lies with those who create it;
- responsible behaviour demands users all meet minimum Cyber hygiene requirements;

⁵ Cyber crime is an umbrella term frequently used to describe two distinct, but closely related criminal activities: cyber-dependent and cyber-enabled crimes. Use of the term Cybercrime reflects the particular difficulties arising in dealing with criminal acts that make use of the internet and other ICTs including those crimes that cross jurisdictions, encountering the juxtaposition of permissive laws and constraining laws, requiring cooperation between authorities in new ways. A helpful elaboration, amongst others, can be found in a 2013 UK Home office report "Cybercrime: a review of the evidence" https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf.

- we protect the vulnerable in society in their use of Cyberspace;
- we, individually and collectively, understand the consequences of our actions and our responsibility to cooperate to make the shared environment safe; our obligation is in direct proportion to culpability and capability.

5 Practical application of these principles

5.1. Each Commonwealth member may find it beneficial to develop individually, a whole of government strategy, reflecting the many facets in making Cyberspace safe, secure, resilient and rewarding, that will address unique local needs of countries with their different regions, sectors and industries and deliver their particular economic and social priorities.

5.2. Appendix 2 offers a guide to sample practical actions that can be taken by Commonwealth members, based on these principles. Appendix 3 provides a list of organisations offering practical guidance on Cybersecurity. Appendix 2 and 3, for guidance only, are illustrative and new initiatives in this fast-moving topic may not be reflected.

Appendix 1: Implications for cyberspace of each element of the Commonwealth Charter

a. Democracy

Our Charter says, *"We recognise the inalienable right of individuals to participate in democratic processes, in particular through free and fair elections in shaping the society in which they live..."* Used effectively, Cyberspace supports participative democracy⁶ by offering multiple channels for citizen's engagement with the democratic process, transparency and accountability of our governments, leading to good governance and a fairer society.

b. Human Rights

Our Charter says, *"We are committed to the Universal Declaration of Human Rights and other relevant human rights covenants and international instruments. We are committed to equality and respect for the protection and promotion of civil, political, economic, social and cultural rights, including the right to development, for all without discrimination on any grounds as the foundations of peaceful, just and stable societies..."* The operation of Cyberspace could and should respect, reflect and protect these rights as they are applied both online and offline. Widespread access to information through Cyberspace and the network of stakeholders it could help build, equips societies to protect Human Rights⁷ while supporting individuals in their quest for dignified livelihoods.

c. International peace, security and economic development

Our Charter says, *"We firmly believe that international peace and security, sustainable economic growth and development and the rule of law are essential to the progress and prosperity of all. We are committed to an effective multilateral system based on inclusiveness, equity, justice and international law..."* Whilst Cyberspace can give rise to some new threats to global peace, it has a significant role to play in engendering international peace by promoting understanding across cultures and communities, respect for international law and adherence to accepted norms of behaviour. The contribution Cyberspace could make to economic development is far more than the already significant contribution it is making⁸. The operation of an open and inclusive Cyberspace, while recognising legitimate economic, security, cultural and social concerns of members, will deliver these Charter outcomes.

d. Tolerance, respect and understanding

Our Charter says, *"We emphasise the need to promote tolerance, respect, understanding, moderation and religious freedom which are essential to the development of free and democratic societies, and recall that respect for the dignity of all human beings is critical to promoting peace and prosperity. We accept that diversity and understanding the richness of our multiple identities are fundamental to the Commonwealth's principles and*

⁶ Cell vs. internet: The Impact on democratisation in Africa, Dr Patience Akpan-Obong August 2010

⁷ The Internet Society, "Internet and Human rights: The Challenge of Empowered Communities", Nov 2012

⁸ OECD report "The internet economy on the rise – progress since the Seoul Declaration" published 2013

approach." Cyberspace provides direct person-to-person social interactions⁹ between social, ethnic, religious and racial groups and thereby promotes respect for cultural and linguistic diversity, encouraging social development. This can help¹⁰ break down barriers of ignorance, suspicion and prejudice, help protect the vulnerable poor, disabled and rural, supporting these Charter outcomes.

e. Freedom of Expression

Our Charter says, *"We are committed to peaceful, open dialogue and the free flow of information, including through a free and responsible media, and to enhancing democratic traditions and strengthening democratic processes."* Cyberspace provides the means for unparalleled channels for the free flow of information; its evolution and operation must continue to deliver the means for open and responsible dialogue.

f. Rule of Law

Our Charter says, *"We believe in the rule of law as an essential protection for the people of the Commonwealth and as an assurance of limited and accountable government..."* Our operation and use of Cyberspace must respect the law, the law must comply with international norms, and the law must be capable of protecting the people and property. As Cyberspace develops, Members must participate in the continued development of norms of behaviour and laws.

g. Good Governance

Our Charter says, *"We reiterate our commitment to promote good governance through the rule of law, to ensure transparency and accountability and to root out, both at national and international levels, systemic and systematic corruption."* Cyberspace can support good governance of our countries through transparency and accountability of government¹¹ and private sector activities. The governance of Cyberspace itself should in turn be inclusive, transparent and accountable with the active participation of governments, private sector and civil society.

h. Sustainable Development

Our Charter says, *"We recognise that sustainable development can help to eradicate poverty by pursuing inclusive growth whilst preserving and conserving natural ecosystems and promoting social equity. We stress the importance of sustainable economic and social transformation to eliminate poverty and meet the basic needs of the vast majority of the people of the world and reiterate that economic and social progress enhances the sustainability of democracy."*

⁹ "Universities and schools using internet forums in support of the UN International Year of the Youth 2010/11"

¹⁰ "UNESCO Programme of Action on a Culture of Peace, Action 6h"

¹¹ McKinsey report, "The Lions go Digital: The Internet's Transformative potential in Africa" Nov 2013

Cyberspace is a doorway to the global economy and an opportunity for less developed states to participate in world markets, to develop new markets, and to commoditise their resources, promoting economic development¹².

"We are committed to removing wide disparities and unequal living standards as guided by internationally agreed development goals. We are also committed to building economic resilience and promoting social equity, and we reiterate the value in technical assistance, capacity building and practical cooperation in promoting development. We are committed to an effective, equitable, rules-based multilateral trading system, the freest possible flow of multilateral trade on terms fair and equitable to all, while taking into account the special requirements of small states and developing countries."

Cyberspace can help find synergies with other development work and thereby bring greater coherence to development initiatives. Through more universal access to information and to markets, Cyberspace can help remove disparities of opportunity and the means to bring these aspirations to fruition.

i. Protecting the Environment

Our Charter says, *"We recognise the importance of the protection and conservation of our natural ecosystems and affirm that sustainable management of the natural environment is the key to sustained human development. We recognise the importance of multilateral cooperation, sustained commitment and collective action..."* The availability of previously unparalleled amounts of sensory information, through Cyberspace, helps us better manage¹³ our environment and can reveal to the public eye any emerging damage¹⁴.

j. Access to Health, Education, Food and Shelter

Our Charter says, *"We recognise the necessity of access to affordable health care, education, clean drinking water, sanitation and housing for all citizens and emphasise the importance of promoting health and well-being in combating communicable and non-communicable diseases."* Access to information¹⁵, reliable metrics¹⁶ and delivery channels offered by Cyberspace form a key part of delivering these outcomes, particularly for rural communities.

k. Gender Equality

Our Charter says, *"We recognise that gender equality and women's empowerment are essential components of human development and basic human rights. The advancement of women's rights and the education of girls are critical preconditions for effective and sustainable development."* Cyberspace can contribute significantly to promoting gender equality and equity, supporting Millennium 2015 Development Goal 3, though this depends upon access to ICT for women and girls, particularly in rural areas¹⁷. Its nature as an open

¹² McKinsey report, "The Lions go Digital: The Internet's Transformative potential in Africa" Nov 2013

¹³ "Open Data for Africa, an African Development Bank initiative, 2013. "

¹⁴ "Use of Big Data from near-real-time photography shows tropical mammals on the decline, 12 December 2013

¹⁵ Food and Agriculture Organisation of the UN: initiatives to support the delivery of MDG 1

¹⁶ UNICEF, "Committing to Child survival: a promise renewed, Progress Report 2013"

¹⁷ "Gender Equality Issues in ICT" – a World Bank project

source of information and its ability to empower individuals, make Cyberspace a platform to promote gender equality.

I. Importance of Young People in the Commonwealth

Our Charter says, *"We recognise the positive and active role and contributions of young people in promoting development, peace, democracy and in protecting and promoting other Commonwealth values, such as tolerance and understanding, including respect for other cultures..."* Young people, being digital natives, have embraced Cyberspace wholeheartedly and come up with numerous innovations that have enriched Cyberspace¹⁸. Through education and guidance on the safe and effective use of Cyberspace, young people will channel this dynamism and creativity into higher purposes, fostering wider social understanding and triggering valuable innovation.

m. Recognition of the Needs of Small States

Our Charter says, *"We are committed to assisting small and developing states in the Commonwealth, including the particular needs of small island developing states..."* Cyberspace could help small island states surmount numerous challenges including paucity of expertise, geographic isolation and economies of scale¹⁹. Cyberspace offers a gateway to global markets for small scale producers as much as for large scale producers, breaking down one of the key barriers to market entry faced by small island states.

n. Recognition of the Needs of Vulnerable States

Our Charter says, *"We are committed to collaborating to find ways to provide immediate help to the poorest and most vulnerable including least developed countries, and to develop responses to protect the people most at risk."* Cyberspace could help poorest, most marginalised and vulnerable by providing access to information and to markets for economic development.

o. The Role of Civil Society

Our Charter says, *"We recognise the important role that civil society plays in our communities and countries as partners in promoting and supporting Commonwealth values and principles..."* Cyberspace offers the means for easier and more effective engagement by individuals in society, particularly the rural, the vulnerable and marginalised. A more active civil society can help promote our values and principles in today's Cyberspace. A more active civil society can also stimulate further progress in support of our values and principles by engaging directly in the development and operation of tomorrow's Cyberspace.

¹⁸ Facebook was launched by a 20 year old student

¹⁹ UNESCO-supported "Small Islands Voice" initiative and its Global Internet Forum and Internet based Youth Forum. See also the reports of the "Small Islands Voice" meetings in Mauritius 2005

p. Cyberspace itself

Our Charter recognises the transformational role of Information and Communication Technology, which underpins Cyberspace, and the need to harness its power in a positive way: *"We also recognise the importance of information and communication technologies as powerful instruments of development; delivering savings, efficiencies and growth in our economies, as well as promoting education, learning and the sharing of culture. We are committed to strengthening its use while enhancing its security, for the purpose of advancing our societies."*

Appendix 2: A guide to practical actions for Commonwealth members

This guide offers a sample of the practical actions that can be implemented by nations to make the Cyberspace safe, secure, resilient and rewarding, based on the Commonwealth Principles. Against each of the 4 principles, this guide offers a corresponding set of practical actions, covering policy and technical measures including new technologies, legislation and regulations, organisational structures and international cooperation. For each of these, nations may seek capacity-building resources.

Commonwealth members may wish to prioritise their actions as short-term and long-term according to their circumstances, while recognising the impact of their actions the on global community.

Principle 1: we contribute to a safe and an effective global Cyberspace

- as a partnership between public and private sectors, civil society and users, a collective creation;
- with multi-stakeholder, transparent and collaborative governance promoting continuous development of Cyberspace;
- where investment in the Cyberspace is encouraged and rewarded;
- by providing sufficient neutrality of the network as a provider of information services;
- by offering stability in the provision of reliable and resilient information services;
- by having standardisation to achieve global interoperability;
- by enabling all to participate with equal opportunity of universal access;
- as an open, distributed, interconnected internet;
- by providing an environment that is safe for its users, particularly the young and vulnerable;
- made available to users at an affordable price.

Examples of practical actions to underpin this principle:

- Promoting a culture of Cybersecurity by raising awareness, setting standards and providing skills development
- Developing and tailoring national Cybersecurity strategies that reflect the particular needs of each Member nation while recognising its effect on global security
- Implementing working models for Public-Private collaboration in developing and operating Cyberspace
- Identifying the Cybersecurity aspects pertinent to the critical infrastructure and developing a collaborative solution with the private sector and other Commonwealth Members to exceed minimum Cybersecurity standards
- Developing understanding among policy makers of the key factors about network neutrality: the need for a standardised yet open Cyberspace infrastructure, etc
- Collaborative working across governments and the private sector to provide reliable and affordable access initiatives
- Developing an understanding by government and private sector decision-makers about protecting market mechanisms for an effective Cyberspace that is safe, secure resilient and rewarding.
- Preparing for and introducing IPV6 as part of delivering Sustainable Broadband to citizens
- Participating in and supporting the work of the Internet

Principle 2: our actions in Cyberspace support broader economic and social development

- by enabling innovation and sustainable development, creating greater coherence and synergy, through collaboration and the widespread dissemination of knowledge;
- respecting cultural and linguistic diversity without the imposition of beliefs;
- promoting cross-border delivery of services and free flow of labour in a multi-lateral trading system;
- allowing free association and interaction between individuals across borders;
- supporting and enhancing digital literacy;
- providing everyone with information that promotes and protects their rights and is relevant to their interests, for example to support transparent and accountable government;
- enabling and promoting multi-stakeholder partnerships;
- facilitating pan-Commonwealth consultations and international linkages in a globally connected space that also serves local interests.

Examples of practical actions to underpin this principle:

- Creating policy and regulatory frameworks that encourage innovation and entrepreneurship through the safe use of Cyberspace for collaboration and the widespread dissemination of knowledge
- Creating safe, secure on-line markets for small and medium scale enterprises and rural enterprises
- Setting policy for public sector, civil society academia on publishing accessible, comprehensible on-line data
- Advice on creating open, transparent and accountable government using Cyberspace
- Providing guidance and creating facilitating policy frameworks for the safe collection and use of electronic patient data to improve health outcomes
- Providing good-practice for on-line publishing to encourage mutual understanding between cultures
- Agreeing common, practical Cyberspace collaborative working tools to improve international working links

Principle 3: we act individually and collectively to tackle Cybercrime

- nations, organisations and society work together to foster respect for the law;
- to develop relevant and proportionate laws to tackle Cybercrime effectively;
- to protect our critical national and shared infrastructures;
- meeting internationally-recognised standards and good practice to deliver security;
- with effective government structures working collaboratively within and between states;
- with governments, relevant international organisations and the private sector working closely to prevent and respond to incidents.

Examples of practical actions to underpin this principle:

- Implementing laws to fight Cybercrime including computer and network misuse legislation, etc
- Establishing the necessary organisations, with appropriate authorities and resources to investigate and prosecute Cybercrimes.
- Strengthening mechanisms for international co-operation including exchange of information and provision of mutual assistance (adopting current Commonwealth frameworks such as Harare Mutual Legal Assistance Scheme for the Cyber age)
- Identifying national critical information infrastructure and their regional linkages, developing strategies for their protection
- Developing sufficient expertise in computer forensics and the collection and safe custody of evidence to support criminal prosecution of Cybercrimes
- Following best practice on setting up CERTs for national and local incident response
- Adopting measures to encourage sharing of incident information between CERTs
- Implementing international standards, like ISO-27000, in a proportionate and prioritised manner

Principle 4: we each exercise our rights and meet our responsibilities in Cyberspace

- we defend in Cyberspace the values of human rights, freedom of expression and privacy as stated in our Charter of the Commonwealth;
- individuals, organisations and nations are empowered through their access to knowledge;
- users benefit from the fruits of their labours; intellectual property is protected accordingly;
- users can benefit from the commercial value of their own information; accordingly, responsibility and liability for information lies with those who create it;
- responsible behaviour demands users all meet minimum Cyber hygiene requirements;
- we protect the vulnerable in society in their use of Cyberspace;
- we, individually and collectively, understand the consequences of our actions and our responsibility to cooperate to make the shared environment safe; our obligation is in direct proportion to culpability and capability.

Examples of practical actions to underpin this principle:

- Developing policy and providing guidance on achieving the balance between privacy and Freedom of Expression
- Developing policy and providing guidance on the balance between access to knowledge and protecting IP on-line
- With ISP's, developing rules for minimum on-line hygiene requirements and responsible on-line behaviour, based on internationally-recognised good practice guides
- Tracking the emerging ideas on how individuals can monetise their data and providing advance assistance to citizens
- Contributing to international dialogues on respect for human rights and actively seeking to develop consensus
- Providing materials to teach children and adults about their rights and obligations in Cyberspace.
- Providing materials to teach children and adults how to operate safely in Cyberspace
- Putting in place specific measures to protect children and other vulnerable users when on-line

Appendix 3: Sample of Multilateral Organisations offering practical Cybersecurity guidance

African Union: The AU has, within its Information Society Division, goals to help introduce the digital era and knowledge society to Africa, to help bridge the digital divide and to coordinate and harmonise ICT-related projects. It has recently drafted a convention on cyber crime. See <http://pages.au.int/infosoc>"

Commonwealth Telecommunications Organisation

The Commonwealth Telecommunications Organisation (CTO) is an international organisation based in London and established through a Headquarters Agreement with the Government of the United Kingdom of Great Britain and Northern Ireland. It is the oldest and largest Commonwealth organisation engaged in multilateral collaboration in the field of information and communication technologies (ICTs), and uses its experience and expertise to support its members in integrating ICTs to deliver effective development interventions that enrich, empower, and emancipate people within the Commonwealth and beyond.

Commonwealth Cybercrime Initiative: CCI is a multi-stakeholder partnership centred around the Commonwealth that seeks to leverage the strengths of its individual partners to address Cybercrime needs of individual countries in a cohesive manner.

European Union Agency for Network and Information Security: [ENISA](#)'s mission is to achieve a high and effective level of Network and Information Security within the European Union. ENISA 's work programme produces a range of [publications](#) about Cybersecurity. See <http://www.enisa.europa.eu/>

Forum of Incident Response and Security Teams: [FIRST](#) is an international forum that offers good-practice, tools and provides trusted communications between its members. FIRST exercises no authority over the organisation and operation of member teams. See <http://www.first.org/>

Global Cyber Security Capacity Centre: This new [centre](#) is developing a more detailed guide of practical Cybersecurity resources available from these sources listed in this appendix and others, identifying best-of-breed. This will be published during 2014. See <http://www.cybersecurity.ox.ac.uk/>

International Standards Organisation: [ISO](#) is the worlds' largest developer of voluntary international standards and publishes ISO-27000 series of standards that helps organisations keep information assets secure. See <http://www.iso.org/>

International Telecommunication Union: The [ITU](#) is the United Nations specialized agency for information and communication technologies – ICTs. It allocates global radio spectrum and satellite orbits, develops the technical standards that ensure networks and technologies seamlessly interconnect, and strives to improve access to ICTs to underserved communities worldwide. The ITU has a [Global Cybersecurity Agenda](#). See <http://www.itu.int/>

International Multilateral Partnership Against Cyber Threats: [IMPACT](#) is the executing body for Cybersecurity for the ITU and the operational home of the ITU's [Global Cybersecurity Agenda](#). See <http://www.impact-alliance.org>

Organisation of American States: The [OAS](#) is a regional organisation comprising member states from the north and south Americas, created in the words of its own charter "to achieve an order of peace and justice, to promote their solidarity, to strengthen their collaboration, and to defend their sovereignty, their territorial integrity, and their independence". The OAS has a [Cyber Security Program](#). See <http://www.oas.org/>

Organisation for Economic Co-operation and Development: The [OECD](#) promotes policies that will improve the economic and social well-being of people around the world by providing a forum in which governments can work together to share experiences and seek solutions to common problems. The OECD has a topic called [the internet](#). See <http://www.oecd.org/>

World Economic Forum: [WEF](#) is an independent international organisation committed to improving the state of the world by engaging business, political, academic and other leaders of society. The WEF has recently (January 2014) published [Risk and Responsibility in a Hyperconnected World](#) which addresses the issue of Cyber resilience. See <http://www.weforum.org>