

How Interconnectivity can work for Journalists.

- Thank Commonwealth Journalists Association to invite me to participate in this event and I wish you as participants good deliberations in the coming three days.
- However I would like to plead ignorance on the subject matter “how connectivity can work for journalists”. I feel it would be utterly presumptuous of me to be telling an august body of seasoned journalists how to capitalise on the capabilities afforded us by this wonderful development which is the Internet. I look to you for educating me on this. You are infinitely more *au courant* with the transformation of Journalism since the expansion of the Internet and Social Media including developments such as:
 - Citizen Journalism – the instant imaging and reporting that can take place with citizens being equipped with image making devices on their phones and having an optimum global publishing platform like Twitter. The change means that reporting happens instantaneously and not necessarily by people trained in conveying such important information. However, it provides for a widespread and intimate source of information. Eg. Arab Spring.
 - Government threat of Internet Shutdown – We saw this during the Arab Spring last year and in Iran in 2009.
- Rather I would like to speak about the Internet and the benefits it has brought us together with its attendant challenges. And then I would like to touch a little on the Commonwealth’s contribution to Internet Governance. And perhaps key to this issue in this audience, I would like to provoke some debate on whether journalists should be saying more about the workings of the Internet and public policy issues associated with this.
- But first a little about the Internet and facts which many of you may be familiar with. The Internet is a commodity which we now take for granted. Not since the invention of the Gutenberg printing press in the 15th century has there been a development of such global impact in terms of social and economic development. We have come to

be entirely dependent on it in our place or work, in the classroom, in hospitals and in the home. Its overarching benefits cannot be over stated. And yet few of us are mindful either of the perils associated with this or of responsible measures we can take at home or in our places of work to mitigate these in some measure. If we can compare sitting at our computer keyboards with sitting at the wheel of a car, another commodity whose purpose we are all familiar with, using this analogy, it would render our travel much safer if we knew the rules of the road, had a vague idea on its workings, and most importantly knew how to drive. The same can be said for the Internet. The purpose of this overview of developments of the Internet is therefore as much about understanding a little about the nature of the Internet, how it evolved and how it operates, in order to help make our Internet experience more secure and rewarding. It is also intended to generate some debate at this conference and beyond when you go back to your respective countries on some important public policy issues including that of Internet security.

- While the Internet has now been around for decades, it was never intended to proliferate in the manner that it has. Its origins go back to the 60s and its intended purpose then was as a US academic network. It was not until the 90s that its evolution took a radical turn as the result of a landmark US Government decision to open it up for access to all comers translating it into a network of networks. Until then all organisations, public and private, had their own discrete networks with very limited external controlled access provision. To this end in 1998 the US Government set up the Internet Corporation of Assigned Names and Numbers (ICANN,) a not for profit organisation registered in California. ICANN's responsibility was for the maintenance of the Internet's architecture with particular emphasis on its universal access, reliability and security. What is different about ICANN from more traditional organisational models is that it is a bottom up multi-stakeholder set-up rather than a hierarchical top down organisation. And this is significant. The purpose of the model of choice was to give vent to the creativity of the broadest spectrum of user communities in shaping the Internet, and the outcome is precisely what we have today.
- But in order to get a sense of the success of this modality one has to look at the astonishing growth of the Internet. Soon after ICANN was formed in 1998, there

were 20,000,000 users connected to the Internet. These were mostly based in North American and Western countries. This number had grown to one and a half billion by June 2010. Following prolonged deliberations with a view to broadening universal access, ICANN introduced a new measure that enabled the recognition of non Roman script such as Arabic, Mandarin, Japanese etc. in websites and e-mails with effect from July 2010. Another recent additional policy change having a bearing on accessibility is the expansion of what are called generic top level domains (there are 22 of these) such as .com, org, .bus etc. and about 220 country top level domains - .mt, uk, .au etc. In the short space of a year these developments have yielded an additional billion users. Added to this if we factor in the increased use of smart phones, tablets and other intelligent devices, Internet connectivity is tracking towards four billion users by 2013.

- Despite this phenomenal success the Internet is a mass of conflicting tensions which give it its dynamics, and as such not without its detractors. On the one hand it is premised on the fundamental value of openness and freedom of expression that drives it, and countering this, there is the threat to privacy and intellectual property as well as a clamouring for censorship in other quarters. Voices for regulation have so far been drowned by those against, (Internet users would have experienced the blackouts on some Internet sites last week, but more of that later) citing the Internet's success as a manifestation of this. It is a cause for unquestionable good as evidenced by the role it plays in developments we have been witnessing in the Middle East in recent months. On the negative side, the Internet played a central role in fuelling last year's riots in Britain as well as in tracking protestors in some countries.
- This centrality and universality of the Internet with its inherent democracy does not sit comfortably with many governments who are at odds with a medium which is at the heart of our global economy, over which they have little say, and which is perceived as an American instrument of influence and control.
- This latter is the major threat of the Internet as we know it to-day. The movement is for the most part driven by China, Russia and Saudi Arabia who hold sway over what are termed the 77 non aligned countries most of which are lesser developed and many forming part of the Commonwealth. These countries would like to have in

place a supra national governmental body, possibly the UN, that will provide the oversight over the Internet's operations and be the arbiters on issues of public policy. In the opposite corner we have the consensus of most Western countries including the EU that this is a dynamic which is best left to the private sector driven by the wise dictum that "if it's working, don't fix it".

- Governments are a vital Internet constituency represented by a government Advisory Committee to the ICANN Board whose mandate is to advise the ICANN Board on public policy issues. In an effort to allay concerns about the latter the mandate of this Committee has been reinforced in recent years. And much of the concern of governments centres on the reliability, robustness and security of the Internet. To this end governments have advocated caution in the face of major policy changes having a bearing on any rapid expansion, pending the resolution of a number of associated issues, with security featuring prominently among these. The ICANN Board made some concessions but in the end it over-ruled government advice to hold back on the expansion of generic address space until all outstanding issues were resolved. The outcome of this action will be exponential growth of even greater proportions than previously experienced and a corresponding escalation of criminal behaviour on the Internet.
- But how serious is the issue of criminality on the Internet? Recently just as a snapshot, trawling international media in the course of a week, you have the American defence secretary talking of a digital "Pearl Harbour". In the same week the Prime Minister of the United Kingdom announced a budgetary appropriation of £650M to fight e-crime and its assistance in setting up the International Cybercrime Security Protection Alliance, and this in the face of the country's most stringent austerity programme since World War 2. Then moving to Australia where the Attorney General while announcing controversial new measures to combat cyber crime stated, "Cybercrime is a growing threat to individual, businesses and governments around the world and has already overtaken the drug trade as the most profitable form of all crimes. With more Australian families, business and government conducting all manner of activities every year on line, there are more opportunities for cyber criminals to steal money, identities and information from unsuspecting victims". A Canadian editorial the same week reads "Put that website

down, you don't know where it's been". A feature article in the Economist around the same time provides an insight into the hacking underworld. "Online scammers, thieves and industrial spies are draining billions from the global economy. 60,000 new malicious software variants are detected every day", and stating that much of this activity can be stemmed as it is traceable to 50 ISPs out of a total of 5000 world-wide.

- Why this is not done or at least not done fast enough is down to a very complex set of factors, not the last of these being the borderless nature of the Internet.
- Quite apart from the challenge of tracking back and identifying the source of a criminal activity on the Internet, the investigation, prosecution and enforcement capabilities vary from country to country. Often these capabilities are worryingly scant in a large part of the globe.
- The Australian Government is the first to have come out with a public consultation document on cyber security with other countries closely following. The reason for this is that this is an issue that touches all of us. It is vitally important for us to be informed about the issue and alert us to the threats because security and protection are a shared responsibility. The purpose of my zeroing in on this topic with a group of Commonwealth journalists is as much about drawing awareness to this issue. As you no doubt are aware, there are myriad players in the Internet chain – ICANN, Telecom service providers, ISPs, registrars and registries, Internet exchanges, web domain owners, government, business, schools, banks, and regulators, with the user at the end of the chain. Each and every level of this hierarchy has a corresponding share of responsibility for Internet security. Each and every one of these links in the chain has been the target of cyber attacks at some point in time with remarkable frequency. American defence data bases have been penetrated, the communications of a whole country have been blocked, and the last few months have seen the largest heists of personal data from major corporations, governments and including banks. I can added that my own VISA account was hacked recently and the web site of my organisation suffered three attacks in one week.
- In Malta's case the last decade of relative prosperity and economic stability may have lulled us into a state of relative ambivalence about happenings beyond our

shores. It is interesting to note that while the subject of cyber crime has been the focus of so much media attention, the Malta media have not had much to say on the matter. But things are changing. In an article titled “Fears over government silence on Internet Treaty” in yesterday’s Malta Sunday Times, Bertrand Borg sets out his concerns about Malta signing up with 22 other EU member states to sign up to a controversial intellectual property rights treaty amid fears it paves the way for wide-scale Internet censorship. In doing so Malta and Europe are joining the US, Japan and 10 other countries as signatory to the treaty. ACTA seeks to create a new international regime for the protection of IP rights. Proponents claim it will encourage innovation by protecting copyright, trademark and patent holders and combat piracy. Aspects of Internet regulation are current hot topics in many countries.

- Critics of the ACTA treaty claim that it was negotiated in complete secrecy until drafts by Wikileaks were leaked to the media in 2009 – it violates human rights and could lead to a policed Internet, censorship and would strangle small-scale creativity
- But the reality behind Internet security is that we all have a part to play in this. Governments have to have in place the appropriate legal infrastructure, national critical infrastructure contingency plans, and suitable forensic capability to investigate criminal activities, to prosecute and take appropriate measures. Telecom service providers need to have suitable redundancy architected in their networks together with contingency plans. The judiciary has to be suitably enlightened about this form of criminal activity to render appropriate judgements swiftly. Businesses have a responsibility to ensure secure environments to protect their data and ensure the security of financial transactions. Schools have a responsibility to protect children from certain harmful content and to teach them about the perils of the Internet. Our universities and technical colleges have the responsibility to turn out Internet savvy graduates and others with the skills to ensure we have secure networks and systems. And parents have a responsibility to have a better understanding of the Internet’s benefits and potential hazards in order to afford their families the appropriate protection.
- The Maltese government ticks a lot of the boxes in terms of policies, legislation and good practice while no doubt more needs to be done. It is also active in European

and global Internet and security circles. Our Ministers and diplomats have punched above their weight in the political contest relating to operating Internet modalities that allow for multi-stakeholder inputs but with a premium on reliability and security.

- Malta now has in place a national Internet governance Group led by the Malta Communications Authority and drawing on representation from the Attorney General's Department, Ministry of Education, University, Chamber of Commerce, Telecom, ISPs and IT industry, civil society, law enforcement, consumer agency, banks etc. The group which is in its early stages will be taking stock of relevant issues which need to be addressed with a view to formulating a plan of action on a variety of fronts including initiatives aimed at improving cyber security. This is a promising development affording the many constituencies opportunities to provide inputs into the manner of addressing these very important public policy issues. There is also the benefit at every level, from citizen to government in sharing best practice.
- In recognition of the important role of the Internet in our lives and on development in general, the United Nations launched an annual Internet Governance Forum in 2005 with the objective of giving stakeholders a platform to facilitate policy inputs on the Internet's development having to do with access, content, security, openness etc. This has in turn spawned regional and national Internet governance groups or fora with similar objectives and which in turn feed into the global Internet Governance Forum. These national bodies perform an important role in disseminating information and raising awareness which in turn serve to inform national policies relating to the internet.
- By way of recognition of the Internet's contribution to socio-economic development, the Commonwealth set up the Internet Governance Forum about three years ago within the frame of its ICT for development programme. As in the case of other IG fora, its aim is to disseminate relevant information to its member governments and stakeholders which will serve to inform national positions on public policy issues associated with Internet Governance. Apart from participating in the UN's annual IGF, the Commonwealth IGF has set up a repository on its website on the subject of

Internet Security and Child Protection as well as organised related awareness and capacity building activities.

- However given the priority of the need to better address the issue of cybercrime, Commonwealth Heads of Government in Perth endorsed a landmark initiative to address this.
- The Commonwealth Cybercrime Initiative is intended to provide assistance to member states to build the necessary capacity to combat cyber crime. It is a holistic approach aimed at:
 - Providing a harmonised Commonwealth legal framework on cybercrime which could form the basis for countries accession to the Budapest convention which is presently the global treaty on cybercrime;
 - Providing training to prosecutors and judiciary;
 - Providing law enforcement agencies with the technology and capacity to monitor, investigate, intercept or shut down illegal activities as the case may be.

In a way this initiative in itself is a model of how the Commonwealth can contribute to tackling pressing global issues. While the Commonwealth is leading this initiative, it is doing so in partnership with the Council of Europe, the International Telecommunications Union, the UN, ICANN, the UK's Serious Organise Crime Agency, Interpol, CTO, COMNET and several institutions or organisations with substantive resources to dedicate to this effort – there are about 20 such institutions that have been drawn into this initiative.

With scant resources of its own the Commonwealth Secretariat has mustered this partnership to exploit synergies that can be realised, while providing the lead role of catalyst and facilitator. A formal governance structure is now in place to enable this initiative to make the transition from concept to implementation. Requests for assistance are being reviewed from as far afield as the Pacific to the Caribbean and with projects covering the broadest spectrum ranging from the development of national cybercrime strategies at one end to the building of Computer Emergency Response Teams at the other. I can provide more information on this important initiative should participants be interested.

- As I have attempted to convey in the foregoing, the issue of cyber security is a complex one which is beyond the scope of a single country, entity or individual to address. This notwithstanding, there is a relative contribution that all can make towards rendering the cyber environment more secure and this is an area where the media has a role in raising awareness, generating debate and hopefully catalyse action where this is required.
- So in concluding this rambling discourse, I have tried to synthesise developments of the Internet of the last two decades the benefits of which you are all aware of but I have also tried to draw out the down side of this which is the threat to security resulting from criminal activity afforded by the Internet. I have also briefly touched on an important Commonwealth initiative which is intended to help countries in building the necessary capacity to combat cybercrime. Perhaps topics for debate I could leave with you are:
 - Should the Internet be regulated?
 - Should governments have more of a say in deciding on public policy issues relating to Internet governance? Is the present multi-stakeholder model serving us well?
 - What is the role of the media in raising awareness about appropriate good practice in our reliance on the Internet?
 - Should Internet activity be monitored to mitigate criminal activity or threats to security?

Thank and open for debate or questions.