****

**UK Contribution to the Seoul Conference on Cyberspace**

**UK Contribution to the Seoul Conference on Cyberspace**

**Next Steps: key activities to take forward the London Agenda**

As initiators of this London Agenda, working closely with the governments of Hungary and Korea, and building on the “Seoul Framework for and Commitment to an Open and Secure Cyberspace”, the UK offers the following summary of activities taking place over the coming months to take forward the six London Agenda themes.

**Economic Growth and Development**

1. The economic benefits of cyberspace are well understood but not yet evenly shared. Despite the progress made over recent years, there remains more to be done to close the digital divide and to bring down prices to affordable levels.  The UN Broadband Commission and the International Telecommunication Union (ITU) have played a central role in this, and a number of key players in industry have developed innovative approaches to bring down costs.  Prices nonetheless remain consistently high, especially in the countries and communities least able to afford it.  To unlock transformative approaches to this challenge, a new global coalition, the Alliance for Affordable Internet (A4AI), was launched in Abuja on 7th October 2013. A4AI is a collaboration between business, civil society and the development community. It will work to mobilise country stakeholders and support the development of policy and regulatory reform proposals underpinned by research and multi-stakeholder dialogue.

2. Investment in infrastructure is not enough on its own to drive growth in the digital economy. In particular, policies need to be adopted at both national and international levels that provide the conditions for growth.  A number of Internet Policy Principles have been developed over the past few years: by the OECD, Brazil and others. Work is underway by the Internet Governance Forum (IGF) to draw from these models and to provide guidance to states and regional organisations seeking to develop growth-friendly approaches. Progress will be reported at the IGF meeting in Bali, 21-25 October 2013. The aim is to develop this into a "Multi-stakeholder Framework of Commitments towards Principles for Internet Governance Policy Making". These principles will then need to be further developed into model policies, backed up by practical capacity building assistance.  The Commonwealth Cyberspace Policy Framework, adopted by the Commonwealth Telecommunications Organisation Council in Abuja on 10 October 2013, is a good example of how to provide practical assistance to countries seeking to modernise their policies for the digital age, and provides a template that could be adapted in other regional and international fora.

**Social and Cultural benefits**

3. As recognised by the World Summit on the Information Society (WSIS), information technology is not only a driver of economic growth, but also a driver for a wider range of social and cultural benefits.  Again, investment in infrastructure is vital, but the benefits of these investments can be greatly enhanced through the adoption of best practice in such areas as open government, online education, and delivery of eGovernment services.  More and more countries are starting to develop best practice in this area: the time has come to start to draw this together, to establish how countries might share their experiences, and to make the dividends accessible to a wider range of stakeholders.  The Open Government Partnership, meeting in London at the end of October 2013, provides an opportunity to address how this might be taken forward.  There would be merit in exploring whether a similar partnership for sharing best practice in the development and delivery of eGovernment services would also be of value, drawing on the ideas discussed this week in the Social and Economic Benefits panel: we are interested in views on this.

4. The Human Rights Council last year provided essential affirmation that rights in the offline world are equally applicable online.  As such, basic human rights principles need to be embedded into national-level laws and policies relating to the Internet (and indeed into the policies and practices of industry and other non-governmental entities).  In particular, practical guidance is needed on how to ensure that laws, policies and practices designed to address security needs do not inadvertently undermine these principles.  The work announced earlier this year at the Stockholm Internet Forum (SIF), and which was discussed in the panel this week, aims to take this work forward by formulating concrete best practices and policies for institutional capacity building. It will be developed further between IGF 2013 and the SIF in May 2014.  The inclusion of business and civil society in this process has been key to its legitimacy and its success.

**Cybersecurity**

5. Since the 2011 London Conference, many countries have invested significant efforts in improving their ICT resilience.  As discussed this week, capacity building efforts are vital to ensure that all counties are able to address the cybersecurity challenges.  But, as highlighted at the first conference in 2011, these are trans-national issues, and countries need to be able to work effectively together to tackle common threats.  CERTs play a central role in domestic cybersecurity and should form the backbone of our international approach.  CERT to CERT cooperation is indeed working well in some areas but the global picture is uneven.  Simple measures, such as improving mutual awareness, sharing contact points and developing protocols for exchanging information, can make a significant difference.

6. The work of regional organisations in support of establishing CERT communities continues to bear fruit. Work is ongoing in the OAS, in the EU, the AU and AP-CERT. This work will continue to deliver in the course of 2014.

7. Much can be achieved through regional CERT groups, but more is needed to ensure that CERTs can cooperate between the regions.  The MERIDIAN community of national critical information infrastructure protection (CIIP) experts, launched in 2005 and meeting in Argentina in November 2013, represents countries widely dispersed across the world and provides an ideal opportunity to explore how trans-regional cooperation might be improved.

8. At Davos in 2013, the World Economic Forum (WEF) launched the Partnering for Cyber Resilience Principles and Guidelines. They are currently running workshops to develop these further. The results will be announced at Davos in 2014.

**Cybercrime**

9. Tackling cybercrime requires cooperation among national law enforcement agencies and with the private sector, and a related focus on capacity building and technical assistance.  This was recognised by the April 2013 UN Crime Commission and at the Seoul preparatory workshop held in June.  There has been good progress in recent years in the fight against cybercrime, including a steady increase in new and prospective signatories to the Council of Europe Convention on Cybercrime (the Budapest Convention), strong growth in the G8 24/7 Network, the launch of EUROPOL’s Cybercrime Centre, and a strong commitment to capacity building at bilateral, regional and international levels.  The planned launch of INTERPOL’s new Global Complex for Innovation in Singapore in 2014 will be a significant milestone and will provide a unique platform for facilitating contact between law enforcement agencies worldwide.  A common feature of these successes is the extensive involvement of the private sector, which has a unique role in complementing law enforcement efforts, and it is important that we continue to support their involvement in combatting cybercrime.

10. The successful investigation and prosecution of cybercrime requires effective legislative and judicial mechanisms.  While each country will need to adopt legislation that suits its own broader legal environment, there are best practice models that can be adopted.  The Budapest Convention is one such model, as is the AU’s draft proposal for a Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa. Other model frameworks are under development.  Regional organisations are well placed to take this work forward, given their ability to adapt more easily to local legislative conditions, but we also need to ensure that cross-jurisdictional cooperation is facilitated at the global level, for instance through the creation of a UNODC repository of cybercrime legislation, as approved by the April 2013 UN Crime Commission.

**International Security**

11. Significant progress has been made on the international security aspects of cyber with the consensus agreement by the UN Group of Government Experts (UNGGE), reflected in their report of June 2013. The UNGGE made recommendations for further work and discussions are ongoing at the UN General Assembly on the establishment of a new one. The ASEAN Regional Forum (ARF) and the Organisation for Security and Cooperation in Europe (OSCE) have begun discussions on cyber confidence building measures and work is in progress to take this forward during 2014.

12. The UNGGE recognised that industry and civil society have a stake in the outcomes of these discussions, and encouraged us to find ways to involve them in the debate.  Likewise, there are a number of countries that sit outside the major fora that have been advancing the debate, but who are concerned about the potential impact of state behaviour in cyberspace on security within their regions.  Ways in which we might engage the broader audience in this debate were raised during the International Security panel: the ICT4Peace Foundation announced that they will provide an initial focal point for collating the views of civil society, business and academia on norms and confidence building measures (CBMs), and for establishing means to report these views to government.  We should support this initiative.  We should also not lose sight of the fact that information technology has the potential to be a powerful tool in support of conflict prevention and conflict resolution, and need to reflect this in our broader capacity building efforts.

**Capacity Building**

13. The central importance of capacity building in cyberspace has been given increasing prominence as the London/Budapest/Seoul series of conferences has progressed. We have all recognised that, while progress has been made on closing the digital divide, there is more to be done.  We have also recognised that a secure infrastructure, in which the end-user and businesses have trust, requires investment in security. To do otherwise would risk undermining the social and economic benefits we are seeking to achieve. The commitment to increase capacity building efforts globally has been a welcome outcome from Seoul.  We now need to ensure that these efforts are taken forward in a scalable and sustainable framework.

14. There are a number of events taking place over the coming months progressing this work:

- First, the Oxford Global Cyber Security Capacity Centre, the initial concept for which was announced at Budapest last year, is developing a partnership with UNDP and other key international bodies and will be running a conference in Oxford at the end of next month to develop further the underpinning models that will help to inform work in this area.

- The Oxford Centre is also working with leading providers of capacity building, in the public, private and international organisations sectors, to improve mutual visibility of the various initiatives underway.  This is key to enabling all stakeholders to understand what programmes are available, and what we need to do to close strategic gaps.

- The World Bank and the Government of Korea will launch in 2014 the Global Cyber Security Centre. Once open this will be able to help other states by sharing experience and training in ICT policy and cyber security.

- The Council of Europe is establishing a capacity building centre in Romania in 2014 to strengthen their existing work on the skills and capacity requirements to implement the Budapest Convention.

- Finally, a number of other leading actors will be holding stakeholder conferences over the coming months to establish ways to increase the supply of funding and expertise and to better synchronise their efforts. This includes:

* The EU will be convening stakeholders in early 2014 to launch its increased commitment to cyber capacity building;
* The ARF will be delivering its members’ proposal for increased capacity building across the region;
* And the Commonwealth Cyber Crime Initiative will conduct further needs assessments in key partner countries and coordinate agencies delivery of capacity building.

**Conclusion**

15. Much progress has been made since the London Conference on Cyberspace in November 2011. The process has helped to catalyse action across a wide range of different fora and in different parts of the world, by highlighting work already underway and inspiring new initiatives.   All these activities have their own momentum and their own ways of working, but the London process provides a unique opportunity to take stock and to satisfy ourselves that what we need to do is being done to promote a prosperous and secure cyberspace for us all.