

Rt. Hon Alun Michael MP

A contribution to the Digital Britain consultation

I warmly welcome the initiative now being taken by Government to produce a joined up approach in accelerating the UK's engagement with the digital revolution. Responses so far demonstrate that this is an incredibly multifaceted and complex challenge, as a result of the extent to which the internet in particular and electronic media generally are all pervasive and reach into every aspect of public and private life.

The following is a personal submission responding to Lord Carter's request for reactions to the interim Digital Britain report and his explanation of the Governments aspirations in this area. It is based on experience as a Minister, on work with colleagues across Party in the House of Commons on Internet-related issues and on experience of International debate of these issues.

I wish to contribute on three specific issues:

- How best to coordinate government thinking, action and engagement – right across the departments and agencies of government and across the boundaries of Ministerial responsibility.
- How to make Digital Britain a vehicle for British leadership in the area of Internet Governance and international relations.
- How to make Britain the Safest place to do business online.

How the Government should rise to the challenge of the Digital Britain agenda set out by Lord Carter

Inevitably the complexity and pervasiveness described above means that almost every Government department has an interest in "Digital Britain" in one way or another, and usually in a variety of different contexts.

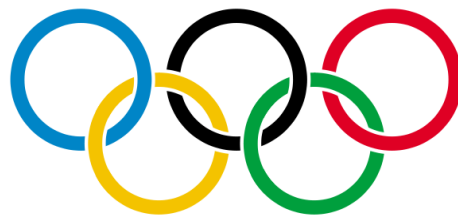
That makes it enormously difficult for Government to have a single joined up approach, but it is also what makes such an approach essential.

For that reason I find the Digital Britain project exciting, but the interim report is disappointing in that it only joins up the thinking from the Department for Business and the Department Culture Media & Sport (DCMS). As I see it, the Department for Business leads on a number of issues including the IT industries and also leads for the whole of Government on Internet Governance, whereas DCMS leads on a number of issues including broadcasting and intellectual property. There is an inevitable overlap on these issues but it is still only one small part of the picture.

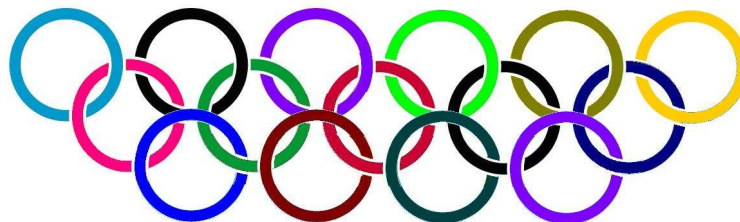
The challenge requires neither pessimism nor undue optimism ! During my time as Industry Minister I worked very closely with my DCMS colleague (then James

Purnell) on the promotion of the creative industries in the digital age and on digital switchover. For that reason I can see that even linking up the overall policy approaches of these two departments is quite ambitious in terms of normal working within government, but frankly it is not enough. The challenge for Digital Britain is to be truly joined up right across Government.

In my experience each department sees this as a cross-government issue, but each starts from its own perspective, which is why we have a plethora of initiatives, agencies, working groups, task forces and articles of legislation. In each case the lead department may have a sensible focus on an important area of policy and may acknowledge the interest of others, but this ends up with a series of overlapping circles of influence which makes the Olympic symbol look simple :



When you start to map the relationships that spin out from an even larger number of Government Departments and Agencies, the picture that is closer to reality is this :



Industry leaders frequently complain that they are asked to sit on, contribute time to, and give money towards fulfilling the roles of a series of overlapping areas of activity led by different departments.

My worry is that there several dangers and we may end up with an organisational muddle – something that looks very simple but doesn't succeed in practice, or something complex that doesn't work. If leadership on digital issues is located within one department that could risk denying the policy interests of several other departments and those they exist to serve, support or regulate. A bilateral "deal" between two departments risks sidelining important considerations elsewhere.

On the other hand, leadership is needed and there is a poor history of delivery when that location is within a generalist department like the Treasury or Cabinet Office if there is a tension with the "delivery" departments.

Nor does the history of Cabinet committee coordination look very convincing at all as a solution. I was a member of PSX(e), which was the Ministerial-level Cabinet sub-committee for Electronic Service Delivery, on and off for almost a decade and I found it the most frustrating and ineffective way of coordinating action, even though there was a great deal of good will on the part of Ministers and officials alike.

Perhaps a new different and innovative approach is needed?

The most successful example I can point to is that of social exclusion where action was coordinated from 1997 onwards by a new and dynamic social inclusion unit which included high-flying and effective civil servants together with individuals seconded from industry and the voluntary sector. That senior level of policy leadership and multi-stakeholder engagement made an enormous difference in the early years of the Labour Government.

The other things that were different about that model is that key tasks were identified within a wide ranging plan, ownership was shared across departments and leadership was given jointly to a senior official and a second-tier minister in the lead department. I was at the Home Office and at the time and (as Deputy Home Secretary) I was the designated minister. The challenge was taken so seriously that the then permanent secretary, Sir Richard Wilson, took a personal interest and brought back a highly talented civil servant from his secondment at the Cabinet Office to be the lead official.

This was “different” in many other ways. Meetings of the working groups were very different from normal Cabinet Committees where Ministers speak and officials by and large listen, in that both Ministers and officials were expected to be dynamic participants and share ownership of their responsibilities. It was very liberating and empowering.

While the Government’s approach to social exclusion continues to be high on the agenda this innovative leadership approach was time-limited, although I am not sure whether that was planned or a case of “business as usual” eventually repopulating the territory once held for a time by “innovation”.

My point is that the Digital Britain agenda is at least as all-pervasive and complex an area of policy (or should that be “policies”?) as social exclusion and neither is a purely technical challenge, although that is the way that both have been perceived at times in the past.

I therefore propose that the Minister – with the personal endorsement of the Prime Minister - draws together a small group of people from inside and outside government to brainstorm approaches to managing a radical agenda for Digital Britain. I suggest that this should include a Parliamentary element, and I would personally value an opportunity to make a contribution.

1. How the Government should lead:

The fact is that many experts and industry insiders are now saying that the scale and scope of online crime is quickly spiralling out of our control. They argue that, for the criminals, unit costs are dwindling as the arrival of ever more efficient technologies erode the “price of doing business” on the internet whilst simultaneously fostering the formation of wide ranging online networks of criminals who share “best practice” and aggregate their respective knowledge bases of the latest criminal techniques.

It is my personal view that this is being overstated: criminal activity and fraud using the internet are big because the volume of internet activity is massive, but my understanding is that losses are not greater than losses experienced at the cutting edge of the high street retail trade, so it needs to be handled with a sense of proportion and care. People who are not familiar with the internet become nervous as a result of spam, pop-ups and other activity, which are nuisances rather than real threats, so that confidence is a real issue too.

In essence, some criminals are definitely adopting increasingly coordinated and organized approaches. If we fail to do the same, we run the risk that the divisions and differences in the priorities of different groupings of Government, Industry and consumers (as well as overlapping of duplicate initiatives) will increase everyone's collective vulnerability. That will lead to a sort of moral panic on the part of the general public, followed by an increasing reluctance on the part of the fearful public to go online. That will be bad for business and will increase the digital divide.

We need to draw on all the expertise and talent available throughout Industry, Government, Parliament, and Civil Society in order to create a multi-stakeholder partnership capable of developing a rapid and coordinated response to emerging online threats. It needs to be strategic and it needs to be comprehensive. Industry is supportive in principle and many people have said to me "of course this makes sense to me, it's a no-brainer," but they need to be convinced that the Government is fully committed to this approach before they will sign up. They also expect reassurance that the establishment of a joined-up partnership framework in this area will release them from some of the plethora of task forces and working groups with which they are already engaged (at least nine Government Departments and a much larger group of Government Agencies).

2. How to build on the UK's leadership on Internet Governance

Britain has played a leading role in preventing the "Governance" of the Internet becoming a source of active international conflict. Our ideas at the World Summit on the Information Society in Tunis (2005) helped to bridge the gap between those who wanted to establish a UN agency for the Internet and those who wanted no governmental engagement at all especially at an international level.

Since 2005 we have developed a significant UK presence at the Internet Governance Forum (IGF) which last met in Hyderabad in December 2008. Our delegation, which I led in 2008, included what we see as the four key partners : Government, Industry, Parliament and "Civil Society". It is developing faster than is normal for such loose-knit alliances – but needs to have much greater engagement at the top end of Industry and commitment needs to be strengthened on the part of all four sectoral partners if we are to avoid a return to the polarised stand-off with which we started in Tunis.

In turn, we have led by example in promoting good practice and in engaging the four partner groupings in setting the UK agenda. But we need to accelerate this activity within the UK and show the benefits of a co-operative approach over the obvious alternative of a purely legislative and bureaucratic approach.

The approach to this issue – which most people see as an issue for “techies” when in reality it is about people about governance and communication – should build on the work that has been done so far : That can be summarised as follows.

(a) **Strategic considerations** – The UK has two overarching aims in respect of international debate over the future governance of the Internet.

- **To combat initiatives to create an international agency to regulate the Internet.** A rigid UN treaty or a bureaucratic international agency would be slow, ineffective and frustrate the beneficial qualities of the Internet.
- **To demonstrate that a cooperative approach – based on UK proposals at the 2005 World Summit on the Information Society in Tunis – delivers to the benefit of everyone.** “Dynamic Coalitions” and “Enhanced Cooperation” can help to build responsive multilateral arrangements which are fast enough and flexible enough to keep pace with the rapid development of the Internet.

(b) **Leading by showing** – having made the intellectual case before and after 2005, the UK became convinced that the only way to persuade the international community to accept our approach was to prove that it works in practice. At Rio in 2007 we promised to establish the UK IGF. It would focus on sharing best practice models and on the creation of an Internet Crime Reduction Partnership.

- **We have established the UK IGF.** It involves an annual programme designed to create an environment in which common ideas are developed, leading to joint action.
- **The nominees for the Nominet Best Practice Awards have surprised us all in the quality and variety of their innovative approaches.** They range from major public companies to small firms, charities and community groups. We put these in the showcase at Hyderabad and this is likely to become a mainstream activity in the future.
- **PITCOM’s work with schools, APCOMM’s Parliament & Internet Conference, EURIM’s work on crime reduction, and the UK’s initiatives on Child Protection have significantly influenced developments.** In each case we have been able to showcase activities which give the UK team real authority in plenary and workshop sessions of the IGF.
- **We have shown that Parliamentarians can make a significant contribution.** Our strength is the UK team includes all four partners (Government, Industry, Parliament and “Civil Society”).

(c) **The value of the IGF has increased over time.** The most important developments in 2008 are:

- **The UK's initiative in creating the UK IGF broke new ground when we made the commitment in 2007.** However, by the time we got to Hyderabad in 2008 there were several exciting reports about evolving national and regional IGF groups. New regional structures include the EU IGF, East African, West African and Asian IGFs. National IGFs are being developed in several other countries including Australia, Germany and France.
- **There is now much more activity outside the main IGF event.** Substantial work is being done by coalitions throughout the year. There is a developing interest in citizen engagement as a response to points made by the UK delegation. Child protection and children's issues are now mainstream issues.

(d) **Will the mandate be renewed?** In one sense the progress so far is impressive as this is a totally new way of working on difficult issues of governance. But time is now short.

- The initial IGF mandate was five years and it runs out in 2010. At the end of the mandate there is a danger that we will revert to the clash between USA's view (leave it all alone) and the view taken by the Chinese and others who argue that the USA has too much direct "control" of the Internet. Some have maintained their view that a treaty and or agency should replace the IGF. However, even the Chinese have engaged constructively with the IGF process.
- During the coming year we need to demonstrate convincingly that the partnership approach is making a real difference and has the capacity to take on the difficult issues. We have shown that online child abuse is better tackled by our type of partnership than through a legislative approach, but we need to go much further and the creation of the Internet Crime & Disorder Reduction Partnership is the key issue.

(e) **The year ahead for the UK IGF:**

- We are planning a full 2009 programme, with a 2009 Best Practice Challenge, meetings for UK stakeholders to report back from Hyderabad, develop messages for Egypt. We have launched a UK IGF website with a blog, and are encouraging wide participation.
- New for 2009: we are exploring the possibility of creating a Commonwealth IGF process, in collaboration with the Commonwealth Secretariat and Commonwealth Countries. We look forward to working with European colleagues in the development of European regional IGF process.

- There is continued engagement on the part of several all-Party Groups within Parliament (PITCOM, Eurim and ApComms) all of which work closely with Industry partners amongst which the support of Nominet and Intellect is particularly important.

Conclusion While we already have clear Ministerial endorsement for this approach and the continued involvement of officials in the detailed work, it needs to be seen as a significant approach of “Digital Britain” to its place in the world.

3. How to make Britain the safest place to do business online.

Being safe online is a priority for business and it is a priority for individuals. It is therefore a priority for the UK economy and for Society at large. The fact that we have reached a plateau in terms of people going online and this partly reflects an unease about how safe the Internet is for those without a reasonable level of technical competence.

But just as there is a tendency to think that these are issues of “technology” best left to those with a technical background there is also a tendency to think that crime and other “nuisance” activities online are best left to the police and security services, or simply that it is up to individuals and businesses to learn how to protect themselves. It isn’t that simple. Just as the local Crime & Disorder Reduction Partnerships have delivered well on crime reduction locally across the UK there is the potential for a partnership approach to help make the UK “the safest place to do business online”.

All countries will want to lay claim to such an aspiration but we have the potential in the UK to make it happen. Approaches like that of the Wales e-Crime Forum and the Yorkshire e-Business Crime Reduction Centre have shown the way and others are following at a local and regional level. But the approach is piecemeal. A UK-wide approach is essential for our effectiveness as “Team UK”, for our standing in the world and for our effectiveness within the UK.

This is not an alternative to the work of the Central e-Crime Unit nor to the steps being taken by the police across the UK, nor to the work of the National Fraud Strategic Authority. None of the three can succeed without the others and without the full-hearted support of both Government and Industry at the highest level.

The aim of making Britain “the safest place to do business online” not only fits well with the “Digital Britain” strategy, but is essential to it. Britain has a strong profile within the Internet Governance community and that needs to be exploited inside the UK and to potential investors.

Delivering on this aim has three main legs which are complimentary to each other. Indeed each is essential to the success of the others.

They are:

- The Fraud Strategic Authority established under the aegis of the Attorney General

- The Police Central e-Crime Unity led by ACPO and the Met under the aegis of the Home Secretary.
- The UK Internet Crime & Disorder Reduction Partnership on which work has been done through the UK IGF and also with the support of the EURIM e-Crime Group which I chair.

General support has been provided at every conference or discussion when the proposition to establish the partnership has been outlined and discussed. Ministers and officials in the relevant Government Departments have supported such an approach. But for it to be supported in practice through a cross-Whitehall approach to which Industry will sign up does require a very high level of long-term commitment by Government as a whole.

The strengths of this approach arise from.....

- Business engagement – developments in use of the Internet move so fast that the protection of the public (business, consumer, citizens, government agencies, and voluntary organisations) must be “designed in” and therefore security has to be linked directly to new developments and exploitation of the Internet.
- Government engagement – there are a multiplicity of initiatives developed quite properly by at least nine government departments and an even greater number of agencies. Some of these are well focused, but there is continual complaint from industry of receiving multiple requests for engagement and support. The partnership approach allows for a joined up approach across government led coherently by ministers.
- Parliamentary engagement – the engagement of MPs across party has given the UK a particular authority at the international level. It ensures that the partnership is not a creature of bureaucracy, but it also demonstrates through cross-party engagement that it is not an instrument of control by government.
- Civil Society engagement – in the field of child protection NGOs have led the way and again have given the UK international authority. The engagement of NGOs demonstrates that our approach is not about “control” but about shared values and mutual benefit.

Problems and challenges:

- Everyone I have spoken to acknowledges that this is a sensible and coherent approach. The effectiveness of a clinical analysis of the problem and a shared approach to developing targeted solutions has been proved in relation to local crime. The starting point is a strategic audit of the problems, followed by agreement on priorities and targeted, comprehensive action. The methodology that was shown to work in the Cardiff Violence Reduction Strategy is appropriate to the Internet.
- However, despite the support of all relevant government ministers, industry waits for government to show authoritatively that it supports this approach and wants the partnership to happen. As one chief executive

said to me “if government signs up to this...of course we will get involved, and put resource into doing so – but we’re not going to do so unless the government’s will is clear, and we will also expect a reduction in the innumerable working groups and task forces in which we asked to participate.” He puts succinctly a view that is shared by others who are less direct.

- It is now urgent to make progress because the other two legs of the stool – the Central e-Crime Unit and the National Fraud Strategic Authority – are moving apace. If the Crime Reduction Partnership is to be effective it has to keep up with their developments and be genuinely complementary to them.
- There are other approaches which are helpful to Internet safety and are complementary to this agenda. They include the Knowledge Transfer Network which works on behalf of the Department for Innovation, Universities and Science, the Information Security Strategic Authority within the Cabinet Office, as well as GetSafeOnline which is a partnership initiative which was established by Industry and Government, and a number of industry bodies which have been drawn together in the Information Security Awareness Forum. All of these have demonstrated a will to work coherently with the partnership and to help with the exemplars on which some work is being done at present but none of themselves can create the necessary comprehensive cross-government cohesion of approach. The essential requirement is a very strong and clear message from Government that this the way forward.

Conclusions

The Digital Britain approach gives a once-and-forever opportunity to forge a comprehensive alliance which harnesses the strength of Government, the dynamism of Industry, the democratic and cross-party support of Parliament and the power of popular engagement through “Civil Society”. That is not an idealistic dream and it is essential if Digital Britain is to become a reality – but it requires unity of purpose and real leadership and commitment from Government to make that partnership approach possible.

Rt Hon Alun Michael MP

11th March 2009