

23 November 2011

**Speech by James Brokenshire, Parliamentary Under-Secretary for Crime and Security,
delivered at the 10th anniversary of the Budapest Convention, Council of Europe,
Strasbourg**

Checked against delivery

Good morning everyone, and I would firstly like to thank the Secretary General of the Council of Europe for arranging this event to mark the 10th anniversary of the Budapest Convention. I am delighted to be here, and to be able to show the support of the UK, as the current chair of the Council of Europe, for the Budapest Convention.

I am very pleased to see representatives from such a wide range of countries, from all areas of the world, who have come together to mark the anniversary of what I and the UK Government - and I believe many other countries - see as the most important international agreement on cyber crime.

As with everyone here at the Octopus Conference, the UK Government is clear that the internet is something that everyone can and should benefit from. We are keen to promote the benefits of this technology for both economic growth and social value. The opportunities that the major sectors of the economy - the public, business and government - have from using technology for work and for pleasure are significant, and we want to ensure that these opportunities are realised, harnessing the benefits, the opportunities of e-government and cloud-based, network-based solutions. But we also want to ensure that the legitimate use of cyberspace is not damaged by the activities of organised cyber criminals.

We believe that just as we all benefit from the internet, so we all have a responsibility to help prevent crime, and to take appropriate action to protect ourselves online and help take the opportunities available to us. There are many relationships that we need - with business and with the public - highlighting why this matters - underlining its relevance to business as usual and how safeguarding our systems isn't something for the IT specialists - it matters to all of us and we all need to get better at taking the simple steps to deliver significant safety improvements. But one of the key areas for cooperation is at international level.

And this is where the Budapest Convention is so important in helping us tackle cyber crime.

The Convention provides an integrated model of the three main elements of a legal framework to tackle cyber crime:

- it contains the offences that may be committed online;
- it outlines the procedural law required to allow law enforcement to gather evidence;
- and it sets out the way that countries can cooperate with each other to prevent, detect

and investigate crime.

This fits in with the approach the UK is taking to tackling cyber crime at both domestic and international level.

We believe that one of the key responsibilities that government has – and we believe that this is a responsibility for all governments - is to ensure that the right legislation and procedural law is in place to allow law enforcement agencies to carry out investigations and to seek convictions for those responsible for online crime in the courts.

We also believe that it is essential to use the law in practice. I am absolutely clear that this is about tackling crime committed using technology, and the people committing are criminals, not technologists. We cannot, and should not, avoid seeking to identify, investigate and prosecute such criminals, even where they use advanced technology to commit their crimes. That is why, in the UK, we will be setting up a new National Cyber Crime Unit as part of the National Crime Agency, to lead work at national level to deal with online criminals. This unit will be the international point of contact for the 24/7 network, allowing us to support and be supported by other countries when these crimes occur.

Tackling cyber crime is not just the job of government, but the responsibility of us all. At the London Conference it was recognised that businesses and the public have responsibility to help ensure the safety of the internet. Most of the internet infrastructure and the services provided across it belong to the private sector, and much of the evidence on the use of the internet by criminals is held by internet service providers. We welcome the framework that the Convention sets out for gathering evidence from those who hold it, recognising the need for robust procedural law that takes into account the need to act proportionately and in accordance with laws on data protection.

Cyber crime is a significant threat to the economic and social well-being of our countries and our citizens, and as online criminals operate across national borders, we want to support work to build strong international relationships to tackle it. In the same way that we have a responsibility to act domestically, I believe that we as government have the same responsibility to act in cooperation with our international partners, and this is where I believe that the Convention provides the most value.

As I have said, we strongly urge countries to develop their legislation, their judicial processes and their outward facing contact points. However, we have nationally based legal systems that set out what constitute crime in our countries, which were not necessarily designed to deal with the cross-border nature of online criminality. In the UK, as in other countries, many of the offences defined in the Convention are defined in domestic legislation which may be many years old, and certainly predates the internet age.

What the Convention allows us to do is to identify how we would meet the requirements of each Article in our own way, allowing us to use existing legislation, and provides a definite framework for countries to develop or map their legislation against.

The key advantage that the Convention gives to the countries that are parties to it is that, if they request help from another country, they can be certain that their request can be considered efficiently, and the recipient will have in place the appropriate laws and procedures to assist. This is a significant advantage over a country saying that it has the right legislation, because it means that a country has agreed that not only does it have the right legislation, but that it is equivalent to that for the requesting country.

So what of the future?

I believe that the Convention has been a great achievement by the Council of Europe, and I would like to pay tribute to those who developed it - in particular Professor Kaspersen, who led the expert group that developed it, and also Chris Painter, whose work in the G8 helped to drive it.

The Convention has proved to be effective in a time of great technical change. As an example, at the point where the Convention was opened for signature, the UK had somewhere around 500,000 broadband connections. Now there are more than 18 million used to access a range of services that did not exist 10 years ago.

At the London Conference there was some comment on some of the articles of the Convention, but there was no appetite for an alternative Convention, and that is a view that the UK strongly supports.

We have no desire to change the Convention, but we do want to ensure that it stays relevant, and I would like to ask the Council to make sure that they work with all of the parties to develop additional protocols and other changes as the need arises. We are undertaking a review of our domestic legislation on cyber crime, not with the intention at the outset of changing it, but to check that it is still relevant and effective.

I would also like to encourage the work that the Council has done to reach out to countries across the globe and assist them in developing their legislative framework for tackling cyber crime.

Finally, the UK, as chair of the Council of Europe for the next six months, will strongly support the work to promote the Convention, as we have done in our capacity building work in the past, and we are very happy to share our experience in this area to assist that. I look forward to working with the Council and with countries to drive forward its use. And in so doing deliver greater security for all citizens as well as greater confidence in the digital world that is an intrinsic part of how increasingly we all live our lives.