Organization of
American States

INTER-AMERICAN COMMITTEE AGAINST TERRORISM (CICTE)

TWELFTH REGULAR SESSION
March 7, 2012
Washington, D.C.

OEA/Ser.L/X.2.12
CICTE/INF.3/12
7 March 2012
Original: English

REMARKS BY SPECIAL GUEST EXPERT – DR. JAMIE SAUNDERS, DIRECTOR, INTERNATIONAL CYBER POLICY, UNITED KINGDOM FOREIGN AND COMMONWEALTH OFFICE OF: GOVERNMENT AND THE PRIVATE SECTOR: WORKING TOGETHER TO STRENGTHEN CYBER SECURITY

(Delivered at the Inaugural Session, held on March 7, 2011)

[Introductory courtesies].

My title is Director of International Cyber Policy at the Foreign and Commonwealth Office. My position was created in recognition that issues of cyber policy are rising up the agendas of multiple international organisations, both global and regional, and feature more and more often in our bilateral relations with other countries. Cyber policy is no longer confined to the realm of the ‘geeks and the spooks’ - it now occupies the attention of politicians, diplomats and lawyers. Foreign Ministries need to respond to that.

The title of this presentation is “Government and the private sector: working together to strengthen cyber security”.

First I will talk about the practical measures that we are taking to develop partnership with the private sector to strengthen cyber security at home. I will then talk about what we are doing to promote the development of cyber policy at the international level, and the important role that the private sector plays in that too. I will talk specifically about the London Cyber Conference of November last year, which brought together over 60 countries, a dozen international organisations and a wide range of representatives of private industry, academia and civil society to discuss a very broad agenda of issues, and how we are planning to take this model forward at the international cyber conferences to be held in Budapest in 2012 and Seoul in 2013.

First, I should outline how we are organised in London to address this enormously complex issue. We start from the point that the rapid development of cyberspace is a good thing. That's worth saying, because I feel that many meetings of this kind, by quite understandably focusing on threats and risks, tend to create a negative view of cyberspace. That is a distorted view. In the UK, we have started with a different emphasis: a clear recognition of the enormous benefits in economic and social terms that we are all seeing from the rapid development of a globally networked world.

Cyberspace increasingly provides the backbone of prosperous economies: it is fostering enhanced economic growth, trade and development around the world. International estimates suggest that for every 10% increase in broadband penetration we can expect an average of 1.3% additional growth in global GDP. Around six per cent of Britain's GDP is generated by the internet – making it larger than the utilities or agriculture sectors1 – and that figure is set to grow with the internet boom predicted to create 365,000 jobs over the next five years2. We want to create new opportunities for businesses – and, incidentally support a thriving cyber-security industry, which is a sector in which British companies have real and internationally acknowledged expertise.

The networked world also holds great promise in terms of global social development. At its best, cyberspace strengthens civil societies: rewarding innovation, connecting individuals and communities, safeguarding civil liberties and enhancing access to education, information and ideas. Public and commercial services can be provided online more cheaply, efficiently and transparently than by traditional means

Greater access to more data, via the internet, enables governments and non-governmental organisations alike to identify and respond to things like public health threats and natural disasters more rapidly and efficiently than ever before. It also facilitates greater involvement by citizens in decision-making, such as planning proposals, and makes it easier to hold national and local government to account.

Without a shared understanding and appreciation of how and why the growth of cyberspace can be such a force for good in the world, we risk designing solutions to the identified (or sometimes just the perceived) threats which, for one reason or another, undermine or even stifle the positive dynamic of freedom and openness that my government believes lies at the heart of its success.

[1] McKinsey, 'Internet Matters: The Net's Sweeping Impact on Growth, Jobs and Prosperity', May 2011

[2] Google, September 2011

But to achieve these positive benefits, of course we need to protect ourselves. Our increasing dependence on digital technologies has given rise to new risks. For example, there are more than 20,000 malicious emails on Government networks each month, 1,000 of which are deliberately targeted. And the Government has an ambitious vision, which we call "Digital by Default", of putting all suitable services to the public online by 2015. That includes payment of pensions, social security and other benefits. Huge sums of public money are at stake – certainly in terms of the efficiency savings we stand to make – but also in terms of the potential for opening up payment systems to fraud. We know that this has been spotted by organised criminal groups, and we are devoting major efforts to prepare for that, because the new systems will stand or fall by whether they are trusted by the public to be secure.

Government response

Our first national cyber-security strategy was published by the previous Labour government in 2009. At that time, we reorganised ourselves to better address the issues, by setting up a new central Office of Cyber Security and Information Assurance to lead, coordinate and drive forward cyber security work across government, and a new Cyber Security Operations Centre to actively monitor the health of cyberspace and coordinate incident response, to provide analysis and briefing on threats against UK networks and users, and to conduct cyber security exercises.

National Cyber Security Programme

After our election in 2010, the new Conservative/Liberal Democrat coalition took that a stage further. The subject of cyber-security attracted attention at the highest political level.

Prime Minister Cameron said:
"Cyber security is a top priority for government and we will work closely with the police, security services, international partners and the private sector to ensure that the UK remains one of the most secure places in the world to do business.
Response to cyber threats was a key part of the comprehensive Strategic Defence and Security Review which the incoming government set in motion.

In October 2010, that Review ranked cyber-security as a "Tier One" national security threat – to put that in context, it means that it was placed in the same bracket as international terrorism. In response, the Government committed £650m over four years to fund a transformative National Cyber-Security Programme. At a time when most areas of public spending are subject to reductions, that sent quite a signal that the government means business.

That Programme is now rolling out. It has a broad remit. It is designed to tackle cyber-crime and theft of intellectual property as well as the sort of cyber-threats which are more popular with our newspaper headline-writers, such as cyber terrorism and cyber-warfare. I'd like to emphasise the priority that we are giving to tackling cybercrime, as something which is hurting individuals, businesses, and ultimately the national economy now, every day. There have been various estimates of how much cyber-crime is costing the UK economy. Frankly, I don't think anyone is sure of the numbers, but they are big! One recent calculation put the annual cost at £27bn – of which £2.2bn attached to government, £3.1bn to individuals in the form of fraud and ID theft, and by far the largest portion - £21bn – to industry in the form of theft of intellectual property, customer data and price-sensitive information. For businesses dependent on IP, and in the worst case nationally, that could affect economic competitiveness. Globally it could be a major inhibitor of international growth and prosperity.

Set against that, while the threat from cyber-terrorism is of course a concern and we must remain vigilant against it, for the moment we assess it to be a less immediate one. Similarly, I would put the well-publicised problem of so-called "hacktivists" in the nuisance category for the moment – although cleaning up the mess left by what one might describe as vandalism in cyberspace can certainly absorb resources which would be much more productively applied elsewhere.

New National Strategy

That is the background to launch in November 2010 of the new National Strategy. I'd now like to run through the key elements of that Strategy, with particular reference to how it relates to the private sector. Because cementing a new partnership with the private sector is at the heart of our approach.

We have always been clear that, just as cyberspace is owned and used by public and private sector, governments, business and individuals alike, so the responsibility for ensuring its stability, safety and security also cannot be for governments alone. With that in mind, we are:

Pioneering a joint public/private sector cyber security 'hub': This will allow the Government and the private sector to exchange actionable information on cyber threats and manage the response to cyber attacks. A pilot began in December with five business sectors - defence, telecoms, finance, pharmaceuticals and energy.

Exploring ways in which government expertise can benefit economic growth. Our government is home to world-class expertise in cyber security. We will explore ways in which that expertise can more directly benefit economic growth and support the development of the UK cyber security sector.

Supporting Small and medium-sized enterprises (SMEs). We are providing targeted support to smaller companiesm, who not have access to the same resources with which to protect themselves as do larger companies. At the same time, we will look to specialist SMEs to develop leading edge cyber security products and services, and to help form the basis of future growth in this sector.

Encouraging industry-led cyber security standards for private sector companies. We want businesses to be able to use this as a competitive edge by promoting themselves as certifiably cyber secure. Our Department for Business, Innovation and Skills will work with domestic, European, global and commercial standards organisations to accelerate this work.

Promoting the UK's cyber security industry abroad: the UK Trade and Investment organisation will work with the security sector's own trade associations to ensure that this increasing domestic strength is leveraged to help UK firms sell abroad.

On prevention and raising public awareness, the strategy sets out commitments to:
Bolster the role of "Get Safe Online". Get Safe Online is a unique partnership between government departments, industry and civil society groups which already provides independent, trustworthy advice on staying safe on the internet. It is promoted through private sector sponsorship as well as government advertising – for example, if you log on to eBay in the UK you see the GSO logo. We

are increasing our investment to make Get Safe Online the single, authoritative place for the public to go, to get the latest information on internet threats and the simple steps they can take to protect themselves.

Develop stamps of official approval – the equivalent of the existing national BSI ‘kitemarks’ or the European-level cE mark - for cyber security software. This will help consumers and businesses navigate the range of cyber security solutions available, allowing them to make more informed choices and avoid unnecessary ‘scareware’.

Seek to agree a set of voluntary 'guiding principles' with Internet Service Providers. This could include seeking agreement with ISPs on the support they might offer to internet users to help them identify, address, and protect themselves from malicious activity on their systems.
On research, education and training, the strategy sets out commitments to:

Identify Centres of Excellence in cyber security research and provide investment to plug any gaps. This will improve our research capabilities and expand the number of people with the highest levels of skills and knowledge in cyber security.
Improve cyber security at all levels of education: so that people are better equipped to go online safely.
Establish a scheme to certify cyber security specialists. The aim is to drive up the skill levels of information assurance and cyber security professionals.

On tackling cyber crime, the Strategy sets out commitments to:
Create a cyber crime unit within the new National Crime Agency: The unit will help deal with the most serious national-level cyber crime and to be part of the response to major national incidents.
Encourage the police and the courts to make more use of existing sanctions for cyber offences: Additional powers are already available when there is strong reason to believe someone is likely to commit further serious cyber crime offences. For example, a range of terms – including restriction on access to the internet and prohibition from using instant messaging services – have been used to restrict the ability of organised criminals to commit online fraud. And I’d note that we have obtained our first conviction under the provisions of our Computer Misuse Act against development, ownership or distribution of hacking tools. So we are getting results already.

Make it easier to report financial cyber crime by establishing a single reporting system for businesses and the public. Our national fraud reporting and advice centre run by the National Fraud Authority will become the central portal for reporting any financially motivated cyber crime.

Expand the use of 'cyber-Specials' to help the police tackle cyber crime. The Metropolitan Police's Police Central e-crime Unit has made groundbreaking use of Police Specials – part time volunteers - with relevant specialist skills to help tackle cyber crime. We will encourage all police forces to follow that lead.

Finally, while as I say we don't currently see cyber-warfare or cyber-terror as the most immediate of the threats we face, we have not ignored what one might call the "hard" end of the cyber-security spectrum. In order to confront significant threats, the strategy sets out commitments to:

Protect the Critical National Infrastructure: the Government's Centre for Protection of National Infrastructure is already working with a network of key companies to ensure that they take the necessary steps to protect critical systems and data. The Government will now work to increase its reach to companies that would not ordinarily be considered part of the critical infrastructure, but collectively represent an important part of our economy and may be particularly vulnerable to cyber-attack. For example, businesses that innovate and develop new intellectual property.

Create a new Defence Cyber Operations Group in the Ministry of Defence which will develop new tactics, techniques and plans to deliver military cyber capabilities.

If you want to follow up, copies of the strategy can be found on the Cabinet Office website. So that is what we are doing nationally in the UK. I'd emphasise that much of this work is not flashy or eye-catching. It involves basic, perhaps boring, actions to strengthen government capacity: sometimes this is just a matter of recruitment and training of suitably- qualified civil servants. But just because these things are routine does not mean they are not necessary: on the contrary, they are fundamental to success.

Coming from the Foreign Office, I naturally also want to say a few words about what Britain is doing on the international scene. Because it is a truism to say that cyberspace in not just international, or transnational, but supranational. Just as the benefits of the networked world are global, so the threats and risks to its resilience transcend geography. While national actions to strengthen cyber-security are necessary, they are not sufficient. Most obviously: the transnational nature of cybercrime can only be met through international cooperation between law enforcement agencies –and the technical challenges it poses call for new and innovative ways for such cooperation to take place.

The London Conference on Cyberspace

It was in response to the diverse strands of international debate on cyber policies that the UK took the initiative to convene the conference which took place in London last November. I'm not going to give a blow-by-blow account of the proceedings: for those who are interested, 95% can now be seen on video links from the FCO website, and key Conference documents are also available online. But I do think it worth describing some of the key aspects.

Put crudely, there is a tension in inter-governmental debates on cyber policy: between those on the one hand who see the answer to the acknowledged threats and risks as lying in new legal treaty regimes and greater state control: of national networks; of international Internet governance; and of online content; and those on the other hand, including the UK, who think that it is its openness, and the rejection of heavy-handed state control in favour of an inclusive, multi-stakeholder, bottom-up, and largely self-regulated model of governance, which has been a key to the phenomenal growth of the Internet and to the economic and social benefits that it offers.

It was from the very outset our intention that the Conference should also involve non-governmental actors as full participants - and not just from the IT industry, but including representatives of business, commerce, academia and civil society who comprise the vast mass of users and beneficiaries of the networked world. It simply made no sense for governments to discuss things like secure and reliable access to networks without ISPs in the room, or for the social benefits of trusted cyberspace or combating cyber-crime to be debated without representatives of NGOs. In the final event, over 200 business, academic and civil society organisations attended; and by streaming most of the debates online and running live Question-and Answer sessions with attending Ministers and others via Twitter, we also engaged ordinary users around the world. And we believe the discussions were all the richer for it.

I believe this is fundamental to developing future models of international cooperation. As with national policymaking, cyberspace is not the exclusive preserve of states: strengthening security in the digital society is a shared responsibility in which the private sector and ordinary users also have vital roles to play. Just as in our own national Cyber Strategy and Cyber Security Programme we have built in consultation with industry from the outset, so we need to maintain the public/private partnering approach to international governance. There was very wide agreement on all sides in London that the multi-stakeholder approach to cyber policy was the right one – indeed the only one likely to be effective.

The London format will, thanks to the generosity of the Hungarian and South Korean governments, be taken forward over the next two years in Budapest and Seoul.

Strengthening international collaboration

I would like to finish with some broader comments on strengthening international collaboration in cyberspace. There have been suggestions that concepts of sovereignty should apply as they do in the physical world. The idea of drawing borders in cyberspace is an interesting subject for academic and legal debate, which I am sure could absorb much intellectual energy. I have no objection to that.

But the UK is more interested in early, practical cooperation against the threats to a trusted operating environment, which cannot wait for theological agreement.

It is this strictly pragmatic desire to make early progress in meeting the challenges to a secure cyberspace which has led the British government to look with caution at proposals for new international conventions governing state behaviour – there have been more ideas floated in the past few months. Let me be clear. We are not opposed to new treaties or conventions on principle. In some specific areas – such as enabling more effective cooperation between law enforcement agencies - formal legal instruments are of real value.

But we see enormous difficulties in pursuing some ambitious overarching international legal construct. Cyberspace has been compared to the sea, as one of the “global commons”. But there are important differences. Since the channels for doing business in cyberspace, unlike the sea lanes, are mainly in private ownership, any legal regime governing activities in cyberspace would require harmonisation with not only existing public but also private national and international, civil and criminal, law, in every country in the world. So the vast complexity of the problem becomes clear. The UN Convention on the Law of the Sea took some 20 years to agree. The Secretary-General of the

ITU has commented that a Convention on the Law of Cyberspace might take as long. I can only agree!

What is more: in the case of the oceans, the operating environment did not change in those 20 years. In cyberspace the pace of technology means that it is changing all the time. Who can say for sure today what the cyber environment will look like in even five years' time, let alone 20? This makes the usual machinery of international collaboration poorly-suited to the cyber environment. Any treaty, even when agreed, would be likely to require constant amendment and modification to keep pace with technical reality; even leaving aside questions of verification of commitments.

Yet the challenges we face, from cyber-crime and other sources, will not wait. We need to establish a basis for greater international cooperation now. To meet the immediate challenge we need to take a pragmatic rather than legalistic approach. Hence Britain's interest in seeking agreement on norms of acceptable behaviour in cyberspace which, while less than legally binding, nevertheless set some benchmarks which carry diplomatic and political weight.

The London Agenda

We were, I think, realistic in our ambitions for the London Conference from the outset. There is no "London Declaration" of norms of acceptable international behaviour – but we never expected, in two days of discussion, to achieve a detailed international consensus on that sort of text. Our intention was to *accelerate and focus the debate*; to get the ball rolling faster - and in the most constructive and productive direction.

I suggest that is what was achieved. We have agreement that the issues are vital to all of our interests. We also have broad support for some basic parameters to frame the debate.

1. We aspire to a future for cyberspace which is not stifled by government control but where innovation and competition flourish and investment and enterprise are rewarded.

2. The Internet must remain open and not become fragmented and ghettoised, with artificial barriers to trade, commerce and the free flow of information and ideas.

3. We are agreed to strive for a model of internet governance in which governments, industry and internet users work together in a collective endeavour, establishing a balance of responsibility.

4. Behaviour that is unacceptable offline is also unacceptable online, whether it is carried out by individuals or governments.

5. More efforts are needed to help developing countries bridge the “digital divide”, so that they reap the full benefits which the networked world offers them for their future prosperity.

6. And specifically, that a concerted and urgent international effort is needed to address the challenge posed by crime in cyber-space, which is a significant threat to economic and social well-being. The idea that there should be no safe havens for cyber-criminals , which all Conference participants accepted, is one which the UK will be pursuing energetically.

Of course, within these broad parameters, there is still much scope for differences of view and interpretation.I don’t underestimate the challenges involved in reaching a wide international consensus on more detailed standards of behaviour.

At bottom, I suggest that a great deal of the debate comes down to questions of *balance*. I very much doubt that anyone here would disagree with the thesis that oppressive state intervention and control of all online activity risks destroying the climate of innovation that has made the Internet such a driver of global economic and social development. Equally, no-one advocates a wholly unregulated cyber environment which places law-abiding users at the mercy of cyber-criminals. That would equally risk undermining trust in cyberspace as a place to do business. And of course, we can all agree that the requirement for states to respect international human rights obligations and other tenets of international law such as the United Nations Charter and the laws of armed conflict applies in cyberspace as it does elsewhere. But within those very important parameters, where each nation draws the precise balance between requirements of public and private security and individual freedom will be a highly political decision, reflecting its individual historical and even cultural experience.

Conclusion

In concluding I return to where I started: we must keep in our minds the enormous potential benefits offered by continued growth of cyberspace as a safe and reliable environment for commerce and academic and social discourse, which helps to build international prosperity and foster understanding between peoples and cultures. If we get the balance wrong between freedom and regulation we will hinder that growth. At the same time, failure to establish some common understanding around principles and standards of behaviour raises the prospect of a multiplicity of fragmented and incoherent regulatory regimes which increase the very transaction costs for business which the networked world has been reducing so dramatically