Senior politicians are beginning to see the importance of cyberspace governance, but current international treaties need updating.

Ahead of the UK Cyberspace Conference in London on 1-2 November, **Peter Sommer** *welcomes the British Foreign Secretary's interest in cyber space and cyber security policies, but fears that current international cyberspace treaties that are too vague and generalised for success.*

Cyber Security was identified as one of four Tier One risks in the Strategic Defence and Security Review of October 2010. The review stated that the Government should introduce a national cyber security programme to "close the gap between the requirements of a modern digital economy and the rapidly growing risks associated with cyber space". The Tier One designation is not simply based on fear of sophisticated cyber-attack; it reflects the heavy dependence of the UK economy on complex interlocking semi-self-managing computer systems and networks. From Just-In-Time manufacturing and distribution to the extensive use of web-based e-commerce and e-transactions, the UK has no way back to a simpler clerical and manual way of doing things; and the route to increased national prosperity is ever greater dependency on these systems and networks.

Even before the Review, the previous government had produced a Cyber Security Strategy of the United Kingdom. Its vision was for citizens, business and government to be able enjoy the benefits of a "safe, secure and resilient cyber space: working together, at home and overseas, to understand and address the risks, to reduce the benefits to criminals and terrorists, and to seize opportunities in cyber space to enhance the UK's overall security and resilience." In this view, shared by the current coalition government, resilience, the national ability to withstand and recover is a key feature.

International conventions have limits

The London Conference on Cyberspace is an attempt to address the international dimensions, not the strategy as a whole. "International dimensions", which is what the FCO is in business to handle, tends to mean treaties and conventions. However most observers have concluded that it is far too early to hope for anything as concrete. For a start there are obvious problems of defining terms such as "cyberspace", "cyberattack" and "cyberweapon". Next, any enforceable arms control treaty needs an inspection mechanism: satellite imagery will identify suspected missile launch pads and nuclear installation, but a cyber attack can be mounted from a mere handful of computers which in turn will typically harness many other innocent machines to act in concert – how will you distinguish any small office from a cyber-attack unit? Again, treaties are between nation states but in cyber-space, sub-state-actors, hacktivists, idealogues, "patriotic hackers", "recreational hackers" and criminals are all capable of inflicting substantial damage.

The existing CyberCrime Convention (the Treaty of Budapest) is approaching its limits. Russia won't sign and has suggested a wholly new treaty based around the United Nations and to include terrorism, but there is a suspicion that it fears a loss of sovereignty. Some developing countries appear to be hostile because they played no part on the design of the treaty and see it as yet another covert form of Western neo-colonialism.

Cyberspace behaviour norms have Hague's support

Hence the decision by Hague and the Conference organisers to by-pass any thought of a full-blown treaty, in favour of the identification and recognition of international norms of behaviour in cyberspace. In his speech last February, Hague suggested seven:

- The need for governments to act proportionately in cyberspace and in accordance with national and international law;
- The need for everyone to have the ability – in terms of skills, technology, confidence and opportunity – to access cyberspace;
- The need for users of cyberspace to show tolerance and respect for diversity of language, culture and ideas;
- Ensuring that cyberspace remains open to innovation and the free flow of ideas, information and

expression;

- The need to respect individual rights of privacy and to provide proper protection to intellectual property;
- The need for us all to work collectively to tackle the threat from criminals acting online;
- And the promotion of a competitive environment which ensures a fair return on investment in network, services and content.

Hague noted that "as liberal democracies we have a compelling interest in supporting democratic ideals in cyberspace, and working to convince others of this vision. When we talk about defending ourselves against cyber threats, we also mean the threat against individual rights to freedom of expression that is posed by states blocking internet communications. The free flow of ideas and information is an essential underpinning of liberty." It is clear that Hague's vision is for the UK to be at the forefront of efforts to safeguard freedom of expression on the internet.

However, taking these sentiments forward means that at points they impinge on a number of extremely well-developed but unresolved debates about the alternative futures for cyberspace. Will there be many more controls over the Internet in a bid to reduce "bad" activity or will the open model prevail, with its greater opportunities for innovation? Will future Internet governance continue on the current evolutionary consensual structure around the Internet Engineering Task Force as the developer of technical infrastructure and protocols and ICANN as the co-ordinator and registrar of the Internet's unique identifiers, or will it move to a nation state dominated model? How far should Internet facilities providers be asked to monitor activity of their users, both for law enforcement purposes and to protect intellectual property? What will/should happen to net neutrality – the principle that there should be no restrictions by ISPs or governments on consumer's access – no multi-speed Internet based on who you are or what you do. Related to that: how are the public networks to be fairly funded?

Obtaining agreement to Hague's wide-ranging norms may be as difficult as getting a sign-up to a treaty. Too many national and commercial interests are threatened. A number of countries will be alert to, as they see it, attempts to enforce Western values.

The options: apply the law of war, or extend norms?

There are, however, two alternative routes to the international cyber security problem which have greater chances of success, partly because the ambitions are more focussed and limited.

The first is to explore how far existing international law and the law of war can be applied, relatively unaltered, to cyber issues. That is the aim of the Tallinn Manual Initiative. Although sponsored by the NATO Cooperative Cyber Defence Centre of Excellence (based in Tallinn, Estonia) the compilers, all legal experts, act in a personal capacity. A reviewable version is expected in 2012.

The second is to stick with the idea of norms but to identify specific situations where there is likely to be extensive mutual interest. A fairly obvious idea is to seek to protect medical and similar facilities from cyber attack in much the same way as the Red Cross/Crescent etc is widely respected in war zones. The problem of identifying such medical computer systems (a painted-on red symbol won't quite work) could be resolved by ICANN – it could authorise a specialist registry to issue a specific domain name, or it could reserve a bank if IP addresses. There is also a strong mutual benefit in keeping going the fundamental structure of the Internet – the root servers, the main continental exchanges, the main undersea cables and so on. A clearly articulated norm here would be relatively easy to construct. The East-West Institute, a global think tank founded in 1980 and which has attracted very high level corporate sponsorship has suggested more along these lines: protection for "International Priority Communications", "ICT Development Supply Chain Integrity", "Emergency Response Coordination for the Financial Sector". A more ambitious but still achievable suggestion from EWI is "Cyber Conflict Rules of Engagement": this might tie in with the Tallinn Manual work.

At one level the London Conference on Cyberspace is very welcome; it shows that senior politicians are beginning to see the importance of getting to grips with cyberspace governance. But, based on its agenda so far, it also seems to indicate that politicians and diplomats have a great deal of catching up to do. The evolution of cyberspace, along with the growth of a globalised economy, is one of the mechanisms by which the role of the nation state is being slowly eroded. At the same time it is may be too much to expect some nation states easily to accept what they see as Western notions of "freedom" simply because the issues arise in a slightly new from via the Internet, Warm, well-intentioned widely-based statements favouring idealised circumstances are not going to be enough.

The London Conference on Cyberspace will take place 1st – 2nd November 2011 at the QEII Conference Centre in Westminster. For more information and to view the outline agenda see the conference website.