MICHAEL CHERTOFF

Former Secretary for Homelands Security, United States of America

Steven Erlanger, Paris Bureau Chief, *New York Times*

It seems to me that one of the things which is clear here is that the Internet is an enormous challenge to sovereignty. We are trying to talk about governance, but in fact, it undermines governance. If we look at the other main topic of this conference, which is the financial crisis, we can see very quickly what slow instruments Governments are. They do not react quickly; they do not, in the end, keep up with the markets. The best people do not always go into our regulatory agencies.

We have the same problem here. You have, as we heard last night, 900 million Internet users in China, but they cannot see anything that they want to see. We know that China is selling Internet-blocking software to Iran. Governments are struggling to control what is out there. We know that Al-Qaeda communicates with its cells through the Internet, through Hotmail, through Google Mail and through coded messages. How do we control this?

It seems to me that we really do need action, when we talk about governance and Governments. Perhaps here, I am speaking as an American. We do need to think and perhaps talk a little more about how vulnerable we are and the questions of cyber war and cyber security. We saw it in Estonia; we saw it a bit with Georgia. We are very vulnerable; things can be shut down very quickly.

I think we are also very lucky; we have the former American Secretary for Homeland Security, Michael Chertoff, in the audience. He has obviously spent quite a lot of time worrying about these questions. I hope you do not mind, but before we go to questions, I have arranged with him to tell us about his own worries and experiences for a few minutes.

Michael Chertoff

Thank you everybody, for letting me intervene. As you know, we have been looking at the issue of cyber security in the United States for a number of years. Starting in 2007-08, a comprehensive cyber-security strategy was put together, which was launched under the prior administration and continues under the current administration.

Broadly speaking, there are three security challenges that we face on the Internet. One is the issue of cyber crime; people are well aware of that. The dimensions are enormous; we have had thefts of literally tens of millions of credit-card numbers, which have had a huge impact on people. Beyond that, there is economic espionage and state espionage. There are enormous quantities of data that are stolen. Everybody knows about the Google attack earlier this year, but that is only one example of the kind of economic impact this has on our businesses and on our Governments.

The third issue, which I think is the most disturbing, is the one that Steve talked about and that is the issue of cyber attacks and cyber warfare. In 2007, Estonia suffered a denial-of-service attack. There were cyber attacks surrounding what happened in Georgia in 2008. There have been stories in the paper recently about a worm that appears to attack

control systems in certain kinds of Siemens machinery. That underscores the danger of an attack that would not merely overwhelm a network, but would actually destroy a network. It is one that might manage critical infrastructure.

We are facing a circumstance in which the Internet allows people to potentially have a catastrophic, destructive effect. This is not only on the Internet itself, but on the real-world systems that depend on the Internet. Here is the challenge. I think Craig was correct in talking about the asymmetry. He referred to the fact that kind of destruction that used to be reserved for a nation state can now be carried out by a group or even an individual with sufficient capability.

However, the same principle also creates a problem of attribution. In other words, we do not necessarily know who carries out an attack, or who causes an attack. Often, the attack is mounted through third-parties, through servers that are hijacked by people for their own purposes. We have had circumstances where there is a suspicion that a Government has launched an attack, but the Government denies. They say it is a bunch of kids or a bunch of people who are acting on their own.

This makes it very difficult to raise the kind of regime of governance that we are used to. For example, in the arms area or in the area of space, in the good old days of the Cold War, we knew who the actors were that could carry out a nuclear attack. We built a doctrine and a series of international rules that governed what would happen in the area of nuclear arms and yielded a very stable environment. The problem is, because of the asymmetry, we cannot do that with the same ease in cyberspace.

The question I put to the panel is this. There are some people who are sceptical about doing any kind of international agreement on cyber warfare. Their belief is that it is unverifiable and that a country can sign up to an agreement and can simply deny that they are actually violating the agreement. There are people who believe that given the prevalence of espionage on the Internet, there is not going to be sufficient interest.

Others believe that we can probably reach some agreement on some areas that all countries would view as off-limits for cyber warfare. I put myself in this category. Examples include destroying our global financial system, which would hurt everybody. Again, the question is, how do you police it? Who has the responsibility to make sure that the servers in one's own country are not used for attacks? What do we do if a country is incapable of managing its own domain? Can other countries come in and defend themselves? There are a lot of complicated questions. The challenging question I raise for the panel is; what do you see as the future of this kind of international arms-control regime in the context of cyberspace?