NATHALIE KOSCIUSKO-MORIZET

Minister of State for Forward Planning and Development of the Digital Economy

Ulysse GOSSET

Thank you, Mr Chertoff. We'll now give the floor to the French minister. How do you view the future of cybersecurity and who should oversee the security of Internet networks worldwide?

Nathalie KOSCIUSKO-MORIZET

First, I would again like to emphasise that this is not the only problem. The [issue] of protecting personal information, for example, poses a threat to individuals and, to some extent, companies; these threats are considerable and must be taken into account. It's almost easy to jump on the issue of cybersecurity because people listen, because it evokes war, because it brings up examples from the past few years, from the news. I think that to some extent this issue will be the easiest to resolve or, in any case, the easiest to intellectually understand. Not to resolve perhaps but at least to intellectually understand. Now if we nonetheless want to address this issue, what can we do? Firstly, there are two types of problems. It's true that it's very asymmetrical. These are very asymmetrical threats, and they're threats that involve cyberterrorism being confused with cyberwar even more than in the real world because it can sometimes be very hard to know who is behind the attack.

In fact, cyberwar methods, even when they are carried out by States, use terrorist practices. This consists in using botnets to take over an entire computer network that has been infected so it can be used to massively attack whole sections of the network. This might be done by a State, but it's well understood that it's not very acceptable.

There are two types of methods: the first is to infect computers and launch them on one part of the system or on a specific site all at once. In general, it's an official site, and with this problem [you can] create what's called a denial of service. [You can] bring the network down like that. There's also another method, which is to use more subtle viruses that may be more dangerous but that are less visible. I believe the primary solution is cooperation – cooperation so that we can share information on network weaknesses in order to resolve them together.

And cooperation because the Internet is a profoundly decentralised network that will achieve security by becoming extremely decentralised in nature, not by trying recentralise systems, including protection systems. I'll give you an example. The Internet suffers from all sorts of weaknesses (I share Mr Barrault's viewpoint on this subject) and, at the same time, fewer weakness, to some extent, than there were one or two years ago, due to the replication of root servers. In the past, there were a dozen or so root servers mainly located in the United States and only there. They have now been replicated. They have been virtualised just about everywhere. These are only replicas, so that doesn't resolve the entire problem. But the fact that they were replicated and virtualised means you can withstand an attack or a problem more easily and for a longer time in any case.

The network's decentralised character is in itself protective, and I believe that's what we should have at the global level. We should not only stave off a certain number of attacks in line with the network's decentralised character, but also use the network's decentralised character in keeping with the genuine neuronal network that characterises the Internet.