CRAIG MUNDIE

Chief Research and Strategy Officer of Microsoft Corp.

Craig MUNDIE, Chief Research and Strategy Officer, Microsoft Corp

I actually have a few things that I would emphasise first. One is that Mike Chertoff mentioned attribution. There are many things that are going to require attribution or stronger identity. They range from just wanting to make sure that your bank account is not stolen and pilfered to the degree that it can easily be done today. I think we need to introduce identity mechanisms and we have a whole array of technologies that will allow that to happen.

Historically, Governments have been at the root of issuing identity, starting with your birth certificate, passports and other credentials. We are going to have to create a certain set of credentials that we can proof at a high level and which we can proffer with specific transactions. This means we can say that there is a class of interactions where interaction of guarantees. There is also more of a Wild, Wild West part of the Internet, as is always the case today, where attribution is more difficult.

The second thing we have to do is create something that is probably a bit like the World Health Organisation. As Nathalie mentioned, there is a class of issues on the Internet where these mechanisms propagate just like epidemics do. In fact, we even use the same terminology, virus, for example. Society has realised in epidemiology that there has to be some collaboration, some transparency about when the publication of these problems exists. We also need an ability to intervene, for example, to quarantine people. You can think of the SARS events and others in the physical world.

If you were in an airport and they took your infra-red temperature and they thought that you were too warm, you would be interrogated. If you were deemed to be a threat, you were quarantined; you did not have a choice. Today, we have no consistent set of rules that govern when we should quarantine a machine that is a bad actor on the Internet. Because of that, things propagate and we leave persistent threats in the environment. For example, there are botnets, which are compromised machines that are formed into armies and are then used to launch other attacks.

We should take a few things, particularly botnets and probably seek to create some agreement, like with the World Health Organisation, for the network if you will. We can use it along with some of these identity mechanisms, to start to go in and eliminate some of these specific threats, which are a very large, persistent threat.

I have just one additional thought, which is that today, everybody thinks about safety in this environment as largely a passive defensive mechanism. Your systems may be well-secured, whether you are an enterprise or an individual and you may have anti-malware software or virus-protection software. I describe this to people as the medieval era of Internet. We thought if we built big enough castles that had moats, we would be okay. The bad news is that the Cruise missile is already here.

You need to have a different model of protection. You have to have what we would start to call active defence. This is a place where I think Governments can come together, without it being a universal exercise. They can capitalise a bit on the distributed nature of the network. They can capitalise more on the fact that through collaboration on active-defence environments, they can bind together intelligence activity. They can bind together the ability to respond.

Frankly, within the largest places on the network in terms of capacity, you can use the existing local regulatory environment to create a basis for intervention. However, this thing is too big and too complex to think that you are going to get a simple solution for everything. In a sense, it brings you the question like the one the UN raised just the other day, from Ban Ki-Moon. He said he wants to change the Security Council because it no longer reflects the structure of security as it was when it was created.

I think we need to think very carefully. Do we need what we call the C5, the Cyber Five, or something else? We can come together and say that we cannot fix everything, but at least we can come together to try to work on a class of these problems. We can bring our existing laws and technical capabilities to bear on the problem. We are going to have to start with something like that.