SCOTT CHARNEY

Corporate Vice President, Trustworthy Computing of Microsoft

Jim HOAGLAND, Associate Editor, Chief Foreign Correspondent of the *Washington Post*

I think this is an answer we can build on as we can go along here. There is a thing we are trying to do here. This is to identify, in these areas of new technology, exactly what can be done by international bodies in the form of global governance, to prevent these kinds of catastrophes.

Next, we will discuss the technology of cyber security and cyberspace. I have to tell you, I am a little more interested in the subject this week than I was last week. This week, I became the victim of identity theft through the Internet for the first time in my life. I think I joined a huge crowd. Tell us what trustworthy computing is, what Microsoft's role in it is and how you see the threats that are posed.

Scott CHARNEY, Corporate Vice President, Trustworthy Computing of Microsoft

It is actually very interesting to be asked to be on a panel that merged technology and the nuclear area. Technology continues to surprise me, regarding how it relates to almost everything else in human society. The Microsoft Trustworthy-Computing Initiative was about building secure, private and reliable software. About 10 years ago, our Chairman Bill Gates started it. It is our 10th anniversary on 15 January. If technology was going to be successfully embedded in every single aspect of our lives, it had to be secure, private and reliable. It had to be as dependable as energy and as dependable as the telephone. However of course, technology was not.

There are actually a few interesting parallels with the nuclear area. First of all, the Internet was actually built to withstand nuclear attack. That is why it was designed by the US military. Its predecessor, the Advanced Research Projects Agency Network (ARPANET), was designed so that if a nuclear bomb took out a city, communications could just route around it. 40 years later, you see software being used to cripple centrifuges at a plant that is used to make nuclear material. It is built to avoid nuclear attack and used to potentially avoid nuclear proliferation.

The other interesting thing is that if there is some sort of cataclysmic event, it is increasingly clear to people that the Internet will be a major part of any response process. The reason for that is that when you think of any major catastrophes today, like Katrina, or what happened in Japan, the wire-line and cellular networks get overloaded very quickly. Additionally, the traditional networks allow first responders to engage in voice communications. However, the Internet actually provides a much richer environment.

When Hurricane Katrina hit the United States, one of the problems was that there was so much flooding in New Orleans that a lot of the street signs were under water. People trying to respond, even in boats, did not know where they were. However, if you did not just think about having your cellphone, but rather a Smartphone, you would not only have voice communications, but data communications, mapping services and GPS location data. Suddenly, when first responders go to respond, they can look at a hand-held device and see where they are, relative to other things that are around. They can engage in communications on the same device.

The Internet is going to play a huge role, in protecting people when there are cataclysmic events. It will also play a huge role as we think about how we adjust to all these new crises. One other thing I would say is that there has been a lot of rhetoric over the years that terrorists will take down the Internet. In my view, that is a much hyped statement that is not supported by the facts. First of all, the Internet is not one network; it is a network of networks. In fact, terrorist organisations use the Internet for communications, fundraising and other things.

Secondly, it is actually very hard to take down the Internet because it is massively distributed and not governed from any central source. That does not mean that organisations will not attack parts of the Internet like the banking system, the power grid or some subset, in order to cause damage. There is a big challenge that we have with the Internet and I will end my opening remarks with this. There are a lot of different actors with a lot of different motives on the Internet. You have cyber criminals; you have terrorist organisations and you have nation states engaging in cyber espionage and potentially, cyber warfare. The problem is that while you have all these actors, with all these different motives, the attacks look the same: bits are bits, packets are packets.

In the traditional world, if someone went into a bank to rob it, I can tell you that it is probably a criminal and his motive is probably money. If you saw a fighter jet take down a civilian jet liner, which once happened years ago, you knew it was nation-state activity. Why? It is because civilians do not have access to fighter jets. However, everyone has access to computers; everyone has access to the Internet, so you have an asymmetric warfare problem. It is so hard to know where the attack is coming from. A denial-of-service attack on a Government or on a bank could be anything from an organised activity to a lone actor to a nation-state activity. It is very hard to do attribution.

Jim HOAGLAND, Associate Editor, Chief Foreign Correspondent of the *Washington Post*

Scott, Director General Amano had to deal with a real nightmare this year in Fukushima. Describe for us what your nightmare is in the cyber world. What is a plausible, but currently almost-unimaginable disaster?

Scott CHARNEY, Corporate Vice President, Trustworthy Computing of Microsoft

I think the biggest thing that people need to start to appreciate in more detail is that the Internet is now connecting everyone's life. It is the social fabric. When the personal computers first came out, the idea was that there would be a computer on a desktop. Everyone's home and desk would have a computer. However, it was really embraced because of the push by enterprises to drive up work productivity.

Today, of course, people are using communications technologies in every aspect of their life all the time. You can see this with the Arab Spring. As a result of that, what has happened is, we have got rid of the systems that would support regular human activity in the absence of the availability of machines. For example, if you go for health care, if the computers are gone, there may be no paper records.

I will give you a real-life example of this. I was on a Defence Science Board Taskforce in software assurance in the United States. Many Governments with sophisticated militaries in the world have something akin to Blue-Force Tracking. Basically, all your equipment and your people have chips; you have colours and you can look at these maps. If it is red, it is the enemy and if it is blue, it is you. Somebody said to me, 'You know, the worst thing that could happen is that someone could switch the colours.' I said, 'Actually, that is not the worst thing that will happen. You will only shoot your own people once. Then you will know that your data is not good.'

The problem is; nobody has binoculars any more. If you remember the old movies about World War II, the generals would stand in the hills with the binoculars and see where everyone was. No-one is carrying binoculars and the medical professionals do not have paper records any more. We have become so dependent on technology and we have not maintained fallback systems. What would be the worst-case scenario? If the power grid goes out, then everything else fails. If telecom goes out, then there is a cascading effect on the banks. There are many effects.