DEBATE

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

The point that you mentioned earlier, in passing, was particularly noticeable. That is about the danger of a nuclear plant being attacked through computers. Mr Amano, talk about what your agency does to prevent that. Is that something you are actively working on, or is that something that lies solely in the hands of a national Government? If you know, what are national Governments doing to protect nuclear plants?

Yukiya AMANO, Director General of the IAEA

We are doing something. We are training people against cyber attacks to nuclear power plants. We recognise that this is one of the dangers for nuclear power plants.

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

You are training nuclear plant operators, or your own people.

Yukiya AMANO, Director General of the IAEA

Of course, we train our own people and we train people from member states, either Government experts, or people working in this field. Sometimes, they work in private companies. We gather them and we provide courses to help them prepare for cyber attacks. However, this is a new thing and we need to put further efforts into getting people prepared for such possibilities and dangers.

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

What is the outcome that you fear most, regarding a cyber attack on a nuclear plant? What could happen?

Yukiya AMANO, Director General of the IAEA

The nuclear power-plant centrifuges and enrichment facilities are very sensitive to cyber attacks. The operating systems of nuclear power plants will be quite sensitive. Regarding disturbing their operating systems, in the past, there were analogue, but nowadays, most operation rooms are computerised. Attacks to these operations systems would be the most serious ones.

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

Scott, how would you answer the same question?

Scott CHARNEY, Corporate Vice President, Trustworthy Computing of Microsoft

There have already been demonstrations done, where people have caused machinery to overheat and catch fire, for example. There have been attacks where control systems have been operated in ways that were not approved or intended by the owner of the system. I think those comments are exactly right. However, I would suggest that you need a structured process for thinking about what you are worried about and how to fix it. First of all, you have to build up to that model. For anything that you build that either has or even has not got IT, you need a good threat model. This means you have to understand what it is you possess and what you are trying to protect. What would a bad actor do to disrupt your operation? Based on those threat models, you then apply a set of controls.

The challenge is always that this is risk management, not risk elimination. We cannot eliminate risk in the physical world either; planes still crash. The challenge when you talk about risk management in cyber space is that it is very hard to quantify the amount of risk mitigation you get from applying a certain control. I have seen this thing with companies all my life. I can say, ‘Here is the set of controls and here is how much it will cost you to add one of those controls. There is people time, machinery time and product licensing. Then, the potential buyer will say, ‘If I spend that much money, how much risk have I mitigated? Is it more than that amount of money?’ The problem is; we cannot quantify cyber risk in dollars and cents in that way. It is a very hard risk-management decision for business executives to make.

Yukiya AMANO, Director General of the IAEA

I would like to add a few words. In dealing with the Fukushima Daiichi accident, one of the most frustrating times was in the first two or three days. During that time, we tried to get the information from Japan. We established contact with the Japanese authorities, but we could not get enough information. The reason is that all the instruments of the reactors were knocked out by the tsunami. There was a complete blackout and we could not get a minimum of information. We did not know what was happening and we could not inform our people or the media about what was happening. If the same thing happens, not from a tsunami, but from a cyber attack, we would be in the same situation. That would be a very dangerous situation.

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

I think this idea of the threat model is very important. It is not generally known, but I believe it is a fact that US nuclear plants have been hardened today to withstand an aeroplane crashing into them. This is obviously a result of 11 September. I am glad you brought us back to Fukushima, because I wanted to continue our conversation on that. Does the radiation from Fukushima represent a threat to any country other than Japan?

Yukiya AMANO, Director General of the IAEA

I do not think so. When we discuss radiation, we have to outline two things. If you are exposed to very strong radiation for a long time from a short distance, that is dangerous and you may even be killed. That could happen at the site or through a nuclear explosion. This is called the deterministic effect. If you are distant from the site, offsite, let us say, 20, 30 or 50km away, you may be exposed to radiation. If you are exposed to such an environment for a long time, in 10 or 20 years' time, you may have cancer. That is a question for people within a range of 20, 30 or 50km radius.

We have monitored radiation levels all over the world. We have detected some change, but the change or fluctuation was minuscule and it is far from affecting human health. The human body is made to be resistant to radiation which exists everywhere in nature, including in this room. Radiation comes from stone, concrete, space and everywhere. I can tell you that radiation increases caused by the Fukushima Daiichi accident in distant countries do not affect human health.

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

Then how do you explain this fact? As a German friend put it to me right after Fukushima, from the reaction and the hysteria in Germany, you would have thought those reactors were in Darmstadt, rather than Fukushima.

Yukiya AMANO, Director General of the IAEA

This is a question of confidence. As radiation cannot be seen, people have a psychological fear and this is a very serious problem. After the Fukushima Daiichi accident, I got a letter from a person whom I do not know. He said that he bought a radio that was made in China. Later, he found that one part of it was made in Japan and he asked me if he could listen to it. I wanted to tell him, 'If you do not eat the radio, you are safe,' but I did not say that.

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

How much of a threat does the radiation represent to Japan? This is particularly given the fact that Japanese officials have been quoted as saying that it will be decades before people can move back into that vicinity.

Yukiya AMANO, Director General of the IAEA

It depends on the area. In order to identify this, we had to make a contamination map. There are so-called hot spots, where levels of radioactivity are rather high. It is better not to go there, or to decontaminate the soil. In some types of food, the radiation levels are high, but the Government is monitoring it. Actually, if you do not keep eating it, it will not have a negative impact on health, but if the Government gives a warning (not to eat something), it is better not to eat it.

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

I have two last questions on this subject. What do you think the future of nuclear power is in Japan?

Yukiya AMANO, Director General of the IAEA

That is very difficult to foresee and there is uncertainty. It is understandable that people have strong fears. As a result of the accident, people within a 20km or 30km radius have been forced to evacuate. The accident has not yet come to an end. It seems to me that constructing new nuclear power plants would be difficult.

However, we are now having discussions with the Japanese Government. Japan is now conducting so-called stress tests to examine whether the nuclear power plants could withstand severe national hazards like tsunamis, earthquakes or floods. The IAEA is prepared to re-examine this and we have done. If they resume the operation of nuclear power plants, it is better to do it after safety is ensured by the Government and perhaps reviewed by the IAEA.

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

That was my second question. How soon do you think you will be able to give such assurance?

Yukiya AMANO, Director General of the IAEA

We are waiting to go and it does not take much time. This is essentially a computer model and they can do it in a few weeks, or a couple of months at most. If we are given the chance, the opportunity, we can do it rather quickly. We can send a mission to help Japanese operators and authorities. It does not take years; it will take a maximum of weeks or months.

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

Scott, I want you to talk a little bit at some point about the role of private corporations in providing national and international security and whether or not you have a role to play in global governance. I should have mentioned at the beginning that Scott served for a long time in the Justice Department's section for cyber crime. Could you talk a little bit about the difference between cyber crime and cyber terrorism? What needs to be done by private corporations, by national Governments and perhaps by some international body you can help us identify, that would have a role?

Scott CHARNEY, Corporate Vice President, Trustworthy Computing of Microsoft

The Internet is very challenging from a governance model. Governments all around the world are now devising cyber-security strategies. The reason it is so challenging for Government is that normally, when Government undertakes issues of this level of import, they often have more control over the assets in question. There is an interesting comparison here. If you think back to the Cold War in nuclear weapons, Governments designed, maintained and kept their fingers on the triggers of nuclear weapons. From that context, they had both responsibility for national security and control of the critical asset.

The interesting thing about the Internet is that it was designed and deployed and is still maintained roughly 85-90% by the private sector. As the cyber-crime problem has grown and as Governments have gotten more concerned about terrorism and cyber warfare, Governments have essentially said, 'We have this responsibility, which is our traditional responsibility, to protect public safety and national security. However, we do not control the asset.' The asset is designed, deployed and maintained by the private sector.

As a result of that, most of the Governments in the world have focused on establishing what they call a private-public partnership. This is partnership between Government and industry to protect the Internet. To be blunt, in the early years of this partnership, we were focusing on the wrong thing. Government and industry focused heavily on information sharing. The theory was that industry had a lot of information about its systems, vulnerabilities and threats. The Government has a lot of information about adversaries. If we all just shared this information, things would be better.

It did not work; people did not share the information. Governments do not share information because sometimes, they are protecting sources and methods. They think the information is too sensitive to share. Industry does not share information because, to be blunt, running around and talking about vulnerabilities in your products is not a good way to engender confidence in the market and enhance your reputation. Then there is the question that even if we shared this information, what are we actually going to do with it?

Therefore, over time, I have come to rethink the public-private partnership. I have another model, which I have been encouraging Governments to adopt. This is the way I think about it now. Markets do provide some level of security. We actually provide a level of security that customers demand and pay for. That is called market force. We also do a little bit more, because we have a sense of public responsibility and corporate citizenship.

That said, markets do not provide security at national-security and public-safety levels. You cannot make a market case for the Cold War. Therefore, when you need something at that level, it is usually achieved through some other mechanism, like Government action. Knowing that to be true, what I have been saying to Governments is, the way to think about public-private partnership is as follows. See what security the market will give you and what the vendors will give you. Figure out what you need in terms of national security and public safety and let us figure out together how to bridge the gap.

In that sense, the Government has a lot of tools in its arsenal. It is part of standard-setting bodies, so it can set standards. In most countries in the world, the Government is the single largest purchaser of IT. If they make it a requirement for purchasing, that is driving the market. Then Governments can regulate; they can if they need to. The real key is to figure out how to establish that governance model.

The other thing about the governance model which is important is that the Internet has thrived in part because it has no governance model. No-one is in charge of the Internet. You have an internet engineering taskforce that works on standards. You have the Internet Corporation for Assigned Names and Numbers (ICANN), which manages the domain-name system. However, since the US Government took it out of the military domain and decided it should be a public resource, the Internet has always been run through a collaborative process. The challenge for Governments is that when they have problems, they usually think in terms of command-and-control structures. There is no command-and-control structure for the Internet.

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

How would you characterise the Government response to what you are describing, from say the US Government and the European Government?

Scott CHARNEY, Corporate Vice President, Trustworthy Computing of Microsoft

I think they have got better. They have worked together to develop consistent and harmonised cyber-security strategies and they are working on international strategies as well. Having said that, they are faced with a couple of huge challenges. One is that it is really hard to do attribution on the Internet. I cannot highlight how important this is. I am going to use the US as an example, since I spent time in the Justice Department.

Most Governments are the same way. There are different threats that Governments worry about. They worry about crime; they worry about intelligence gathering, they worry about warfare. For each of those elements, they have different agencies that deal with the problem. They have law-enforcement agencies; they have intelligence agencies and they have military agencies. The authority those agencies can use is different. They have criminal authority to do wire taps and gather evidence; they have espionage authority and they have military authority.

The agency you use and what authority you rely on depends on two things; who is attacking and why. If it is a criminal, you use a law-enforcement agency with law-enforcement authority. If you think someone is collecting intelligence from your military system, use your intelligence agencies with intelligence authority. If someone is dropping kinetic bombs on you, use your military and your military authority. It all depends on who is attacking and why. What are the two things you do not know in an Internet attack: who is attacking and why. They are stuck.

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

Is there a feasible military response to an attack that would take down the national power grid and the markets and financial structure of a country? Let us take the United States again as an example. What could the United States do militarily in that scenario?

Scott CHARNEY, Corporate Vice President, Trustworthy Computing of Microsoft

There are two buckets of military action. Arguably, there is cyber action you can take. Some of it is defensive, like dropping packets. Some of it can be offensive, shooting packets back. However, you can also take kinetic action. One of the interesting problems in the Internet space though is the problem of targeting. Let us suppose you have a nuclear facility and there is a denial of service launched against your power grid. Packets are coming from all over the world and you decide you are going to shoot back with packets.

The way the criminals work today is that they take over thousands of consumer machines. They are called botnets; they take over thousands of consumer machines and they point them at the target. Then they shoot at the target. If you shoot back, you will take out a lot of consumer machines, but you will not take out the person who is attacking you. They will reconstitute a new botnet and go again. It is hard to give attribution; it is hard to know who to shoot at.

The other thing I should say is that you see more and more language about cyber warfare. However, I am increasingly reading things where people are challenging the notion of cyber warfare. What I mean by that is this. If you look at the history of warfare, when countries engage in war, if it is not to defend themselves, it is to get territory resources or some political advantage. It is very unlikely, at least today, that simply by sending packets across the Internet, you will topple a regime, extract mineral resources or anything like that. There is a growing body of thought that cyber attack in the cyber-warfare context is more likely to be done in conjunction with kinetic activity than just on a standalone basis.

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

We still have a lot of thinking to do before we come to a cyber NATO. There is one last topic, Mr Amano, because we move to questions and answers. That is a topic that ran through the previous panel's discussion as well: Iran. This year, your agency has put out a remarkably candid description of Iran's continuing effort to militarise its nuclear programme. How is it that you were able to get this report out? What accounts for the difference in tone between this report and previous reports?

Yukiya AMANO, Director General of the IAEA

This Iranian nuclear issue is a very complicated one, with a long history. However, if I put it in a very simple way, Iran is a member of the Non-Proliferation Treaty and we have a comprehensive safeguards agreement. That is the verification system between Iran and the IAEA. Regarding nuclear material and facilities that Iran declared, we can verify that they are staying within peaceful purposes. However, it is like a half moon - half the activities are bright and there is a shady side. We do not know - we do not have the full knowledge of - what they are doing without informing us. There is some information that indicates that Iran has engaged in activities that are relevant to the development of nuclear explosive devices.

As we are receiving more information to that effect, we have to try to cross check, double check and triple check the information. As we do not have access to these facilities, we cannot say this with 100% confidence. However, it is a fact that we have very serious concerns. If that is the case, I thought it was time for us alert the world. The IAEA's objective is not to deliver a guilty verdict. Our objective is to prevent the proliferation of nuclear weapons. If there is information that indicates some risks, I thought it would be better to share the information and alert the world.

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

How long before they develop the bomb?

Yukiya AMANO, Director General of the IAEA

It is difficult to say. We are not giving a military outlook.

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

I understand.

Michael ANCRAM, Former Deputy Leader, Conservative Party, United Kingdom

My name is Michael Ancram, from the United Kingdom. I have two questions; I suppose the first is a comment. Every time I hear the question of nuclear safety talked about, there is a great tendency to try and reassure people that it is not as bad as people think it is. I come from Scotland. 26 years after the Chernobyl nuclear disaster, which happened 1,000 miles away, there are still parts of agricultural land where livestock cannot be sold off that land. This is because it is still contaminated by caesium that did not come directly from the plant, but came in rainclouds over a period of time. How do we actually make sure that if we have another accident like that, we can do something about controlling the amount of radiation that is carried meteorologically over a very large area?

The second question is a slightly technical question. The attack on Iran, though we may not know who did it, was carried out by a worm called Stuxnet. However, a worm is not a virus; I am told it is much easier for people to make. It can be inserted into one machine; over a period of time, it can find its way to the target machine that it has been programmed to find. Once it gets there, it can lie dormant for a certain number of years, if necessary, certainly for months. This is until the moment for it to be triggered comes. You do not know it is there; it is almost undetectable. Over the last two years, how many worms of that sort do you think have actually been created and inserted?

Yukiya AMANO, Director General of the IAEA

Regarding the first question, we cannot say that nuclear power plants are 100% safe. There is a possibility of accidents. However, in order to prevent them, we have to develop multiple defences. This time, it was caused by a tsunami, which went beyond estimates. There are various ways to protect the reactors from such huge natural disasters. Now, after Fukushima Daiichi, we are taking measures and we are trying to enhance the safety of nuclear power plants. Nuclear power plants are much safer for the current generation than the previous nuclear power plants. The future reactors, which are called Generation Four, are ones in which safety features are the most important elements.

We are developing a safety culture, strengthening the regulatory bodies, training people to do better operations, using better design and better construction. Therefore, I think we can minimise the risk of accidents. In the case of Fukushima Daiichi, the lessons learned from Chernobyl were very useful. That is why the Japanese Government could evacuate people, so they would not be exposed to radiation. The IAEA sent a mission to decontaminate the land. There are over 60 technologies to decontaminate the land and facility. Again, we cannot guarantee it 100%, but there are ways to reduce the risk to a minimum. If it unfortunately happens, again, there are ways to reduce the risks.

The next question is about Stuxnet. We have visited the enrichment facilities in Natanz in Iran. However, our objective is to ensure that nuclear materials and facilities are not diverted for military purposes and are still used for peaceful purposes. Our objective is not to study how effective or how ineffective Stuxnet is. Our knowledge of the effects of Stuxnet is very limited.

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

Scott, why not join in on that? Give us the professional view of Stuxnet.

Scott CHARNEY, Corporate Vice President, Trustworthy Computing of Microsoft

I would say two things. One is that in terms of how much software is lying dormant in the world, if I came up with a number, it would be sheer speculation. Having said that, I would point out two things that people need to remember. One is that for all of its stealth, Stuxnet was revealed, as much malware often is. Remember that when malware traverses a network, people are running intrusion-detection systems, egress monitoring and other things and it is often detected.

Second, there are practical challenges with deploying sleeper code. Nothing is impossible, of course, but here is the problem. Machines get updated with some regularity. Machines get replaced; hardware fails. Operating systems get upgraded; applications get patched. As a result of that, if you were thinking about planting some code that you might be able to trigger 3-5 years from now, the odds that that code would be there unimpaired in 3-5 years depends on the system.

There are long lived systems. You look at regular bank ATM machines; when they install them, they expect them to run for 20-25 years. However, for other things, like personal computers, PCs and servers, for example, that are running systems, their lifespan is a lot shorter. Usually, they are depreciated and replaced within 3-5 years. It is a challenging environment, both for the offence and the defence.

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

From what you have read about Stuxnet, are there any characteristics of this virus that would tell us where it probably came from?

Scott CHARNEY, Corporate Vice President, Trustworthy Computing of Microsoft

There has been public analysis. However, to be frank, I think more of the analysis regarding origin related to what the target was and what the motives could have been, as opposed to the authoring of the code. Over the years, some researchers have tried to fingerprint malware. Just as a certain author writes a certain way and a certain painter paints a certain way, code writers have a style. People have at times tried to fingerprint style. The problem is that unlike language, when you are writing a novel and you can choose to write in a flowery way or in a very factual way, code has syntax. You have to write it a certain way, or it just will not compile and execute. However still, as I said, over the years, some researchers have looked for uniqueness in code writing, as part of their efforts to identify source.

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

There is an Ernest Hemmingway among code programmers out there somewhere.

Jean de Kervasdoué, Professor of Public Health, CNAM

I am Jean de Kervasdoué, Professor of Public Health. I think we should debate on what a catastrophe is. I am surprised that nobody has tried to remember that the largest disaster in the last two years was certainly not Fukushima. It was the flood in Pakistan, which as you remember, flooded an area larger than Austria. 20 million people were displaced and 10,000 people died. We are speaking about nuclear energy with fear that is well founded. I could come back to that, regarding the consequences of what happened after Chernobyl. However, we do not speak about air pollution in China. 400,000 people die of air pollution in China. Certainly, coal mining is much more dangerous in one year than the entire civil atomic industry since it began to exist.

As you know, there is a WHO report on the deaths in Chernobyl. The number of people we can count is 56. The number of people who might die or have their lives cut short as a result of Chernobyl rises from 14,000 to 16,000 in 50 years. This is according to the estimates of WHO. You can check. The coalmining industry kills 20,000 people a year. What do we call a catastrophe? I think we have taken a very [inaudible] definition of what could be a catastrophe.

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

I appreciate the additions that you have made to our list of catastrophes and I think your point is a good one. What we are trying to do here is deal with two subjects that are very much on people's minds. Perhaps that is what the media also deals with. I accept your remark and the criticism implied.

Stewart PATRICK, Senior fellow and Director of the program on international institutions and global governance at the Council on Foreign Relations (CFR)

I am Stewart Patrick, from the Council on Foreign Relations. I have two questions; the first is to Mr Amano. You mentioned the fear that Iran, for instance, might be diverting some of its nuclear material to a weapons programme. What is the status of discussions about creating an international nuclear-fuel bank, which obviously would help to deal with some of these problems?

Then I have a question to Mr Charney. I was wondering about something. You mentioned some of the advantages of the fact that we have had cyberspace. You mentioned the fact that the Internet is governed loosely by private corporations and the role of ICANN etc. However, I wonder if we are not we are in for a major collision course with Governments. These Governments often share different values. At an earlier discussion, Thierry de Montbrial talked about some of the growing diversity out there in the world.

When it comes to Internet security or cyberspace security, there are several different risks that you discussed. There is obviously cyber crime, which unites many Governments. There is cyber espionage and cyber war. This includes a question of whether one should have a Treaty governing what the potential uses are and the legitimate uses are, along the lines of the laws of war. However, another big one is the question of human rights and the openness of the Internet. Previously, Secretary of State Hillary Clinton laid into countries that go against the US vision of an open, private and largely anonymous Internet. This is something that even countries that are democracies like India are beginning to contemplate. Could you speak about that dilemma?

Yukiya AMANO, Director General of the IAEA

I will answer the question about the nuclear-fuel bank. I would like to very briefly explain what a nuclear-fuel bank is and what the current status of its progress is. Particularly in recent years, more countries have shown an interest in nuclear power generation. If that is the case, more nuclear fuel will be needed. It is normal that these countries, who are considering introducing nuclear power, worry about the shortage of nuclear fuel. The idea of a nuclear-fuel bank is to establish a kind of bank to get prepared for a situation in which the supply of nuclear fuel is disturbed, for non-commercial reasons.

We have received a couple of proposals to that effect. One is from Russia and they have proposed the establishment of an international bank of nuclear fuel. It was adopted by the Board of Governors, the decision-making body of the IAEA. The decision was made some two years ago and low enriched uranium is stored under IAEA safeguards. Now, it is operational. This nuclear-fuel bank exists.

Another idea is to establish an IAEA nuclear-fuel bank. Again, the basic decision has already been made. Now, we are in the process of implementing that decision. We have invited countries to host the nuclear-fuel bank. One country applied and expressed its intention to host the nuclear-fuel bank. We are now making necessary preparations for the procurement of low enriched uranium and concluding the agreement and other things. We have already secured the necessary funds to purchase the low enriched uranium. We have another scheme, proposed by the United Kingdom, to give a guarantee for the procurement of enriched uranium. For now, we have one international fuel bank and one guarantee system and another IAEA nuclear-fuel bank system is under preparation.

Scott CHARNEY, Corporate Vice President, Trustworthy Computing of Microsoft

Let me turn to your questions. First of all, there was your question; you talked about cyber crime, cyber espionage, cyber warfare and freedom of expression. This just highlights how transformative the Internet is in everything that we do now. In the past, there have been countries; Russia in particular has long proposed a cyber-warfare treaty of sorts. Other countries have been reluctant, in part because of the inability to achieve any verification on that kind of treaty.

Having said that, there are now also discussions about whether there should be a Geneva Convention for the Internet. It is a really important point that in traditional warfare, the battlefield is nature made and on the Internet, the battlefield is manmade. Most of the battlefield, to be successful in battle, may involve using the communication pipes, mostly of the private sector. In some places, telecom is still nationalised. It also involves taking out private-sector assets.

The challenge for countries, for the private sector and for citizens is that the Internet is a shared and integrated domain. You have individuals, companies and Government sharing this domain. They also share it in terms of activity; there is free speech, espionage packets and potentially warfare packets. These things are integrated in a way that you cannot tease them apart. You used to fly balloons or you put a big red cross on top of the building saying that this is private space. You cannot bomb here because of disproportionate damage to civilians. The challenge on the Internet is that it all looks alike; they are all just IP addresses. While people have started to look at the laws of armed conflict and the Geneva Convention relative to cyberspace, it is hard to apply.

With regard to freedom of expression, in fact, Microsoft is part of the Global Network Initiative (GNI). This is a group of companies and non-Governmental organisations that are committed to protecting free speech and freedom of association on the Internet. The real challenge is that free speech is not a place; it is a continuum. At one end of the continuum, you have the United States and the First Amendment. Virtually any pre-restriction on speech is out. You have other countries, including democratic countries, that regulate speech a lot more. Germany, Canada and the UK have hate-speech laws, neo-Nazi laws and other things that they apply. Then you have repressive regimes.

At the end of the day, these are about cultural differences regarding free speech and this is also about what form of Government you have and who got to decide. As you can imagine, that is quite a contentious point. I can tell you that when I chaired the G8 sub-group on high-tech crime, the G8 was developing a whole set of principles around cyber crime. What would happen is, we would agree on all these crime-fighting things. Then the other countries would say to the US delegation, ‘We are now going to talk about restricting speech. You should go and have some coffee.’ What they would do is; they would draft an agreement and an addendum. We all signed the agreement; we all or most signed the addendum, but the US did not, because restrictions on speech would violate the constitution.

I will add one more thing. I have always been amazed. Very often, you come to a problem with a mindset and you do not think about some other variation on the theme. As part of GNI, a lot of people are worried about freedom of expression and free speech on the Internet and not censoring or restricting speech. However, in the Arab Spring, the Egyptian Government directed Vodafone to affirmatively send a message that was propaganda-like. Vodafone would have lost their licence if it did not send it. They did two things; they sent the message, but they were also transparent and said, ‘The Government told us to send this message, so that is why we sent it.’ However, it is not just about restricting speech. You can compel speech too and that is a different problem, but a serious one.

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

I think this has been a very rich discussion; this is a great point to end it on. If we can establish a really credible fuel bank, I can think of no greater contribution to global governance than that. I want to thank our speakers for an excellent programme tonight. I want to thank you, in the audience, for staying on till the bitter end.