Legal aspects of Internet governance: International cooperation on cyber-security

IGF 2010
VILNIUS, LITHUANIA
15 SEPTEMBER 10
SESSION 123
0900
INTERNATIONAL COOPERATION ON CYBER SECURITY

****

Note: The following is the output of the real-time captioning taken during Fifth Meeting of the IGF, in Vilnius. Although it is largely accurate, in some cases it may be incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the session, but should not be treated as an authoritative record.

****

International cooperation on cyber security.

>> Okay, good morning and welcome to workshop 123. Simple as ABC my name is David Satola, I'm from the World Bank, I will be moderating this session this morning. We are still waiting for one of our speakers to arrive who I think is getting his credentials now, but we will go ahead with the introductions and the first part of the programme. As you know, this workshop is about the legal aspects of international cooperation on cyber security. We have a wonderful panel this morning. Let me introduce them in the order they will be speaking. Our session will start with a keynote address from Vint Cerf of Google. We will then move to an overview presentation by Mr. Henry Judy. Our speaker concerning aspects of cyber security cooperation in Europe Ivalo Kalfin is getting credentials at the moment so he will be here shortly. We will move onto the Council of Europe where we have Alexander sager speaking about various aspects of the Council of Europe. We will then move to the part of the programme where we will hear responses from national perspectives beginning with Jayantha Fernando from Sri Lanka, and then moving to Andrew McLaughlin from the United States. Then we will be moving into the industry and civil society part of the programme where we will be hearing from Mike Silver of ICANN, John Morris of Center for Democracy and Technology and Bill Smith from PayPal. We will have an open discussion after that, and I think that we will have plenty of time to cover all of that. So without further adieu, I will turn the floor over to Mr. Vint Cerf. Thank you.

>> VINT CERF: Thank you very much, Mr. Chairman. In case anyone is wondering about the head set. If you plug in it turns out you get very good quality sound. I'm not listening to the football game. I am very grateful to have an opportunity to address you on this topic this morning. There is so much to say, and not very much time to say it, so I'm going to summarize my remarks rather heavily.

Let me start out by suggesting to you that cyber security can be divided into two parts, one related to very targeted attacks against specific destinations and the other, the more general problem of bot nets, service attacks, spam and the like and I think it's helpful to keep those two kinds of risks in mind because the mechanisms for response might be different in those two cases. I think we understand that the bot nets that are out there are a consequence of weak operating systems, weak browsers that permit the ingestion of viruses, worms and Trojan horses and the like. There are no easy solutions to those weaknesses, but improvements in operating system design and implementation, improvements in browser design and implementation can be helpful.

Google has tried to be, to contribute to that through the release of its chrome browser, it's two be released chrome operating system and its already released android operating system, all of which are open source. I think that it will be useful to keep in mind that there are different parts of the internet environment that are at risk.

One part lies at the edge of the network, the servers, the laptops, the desk tops and increasingly the mobiles which are

either the producers or consumers of information, and the infrastructure of the net itself, the routers, the domain name system, the servers and the resolvers and the like. To look for a moment at the infrastructure, we know that those infrastructure elements are themselves under regular attack. There is cache poisoning in the domain name system. There are a variety of other kinds of deficiencies. There is hijacking of the internet address space which we will probably see increasingly over time as the IP version 4 address space exhausts. People simply announce that they own a piece of the IP address space and if that gets into the routing system they essentially are able to make use of those addresses. So this is a problem which is being attacked by the use of RPKI, which is digital signing of the assignments of IP addresses which would be understood by the routing system. The Domain Name System security which was mentioned yesterday is another attempt to remove weaknesses in the Domain Name System itself. I would like to suggest to you as a framing thought that while many of these problems are considered crimes against the users of the internet or even the operators of it, that crime is not necessarily the only motivation for building legal frameworks to deal with the security of the net. So while we are, I think, uniformly concerned about fraud, stalking, child pornography, other kinds of abuse which we might generally agree are crimes, we should think of other rationale for creating legal agreements on an international basis. For example, digital signatures. One of the important tools we have for validating information in the net is to use digital signature technology. One question that arises is what is the meaning, what is the significance of a digital signature? Is there any legal framework that explains the utility of a digital signature compared to a wet signature?

If we don't have uniform agreement on some of these concepts, our international agreements that are concluded using digital technology may not have the strength that they need. So here we have other rationale besides criminality to justify the development of legal structures. I think I would like to make two further points and then I will stop, Mr. Chairman. The first one has to do with our tendency to see cyber problems, cyber risks and cyber security in terms of legal abuse, criminality. I would like to suggest that we also consider someone who is under attack as if they had their house on fire. You know that when someone's home or a building starts to burn, generally speaking anyone is allowed to call the fire department to come and put out the fire. We might benefit from thinking a little bit about a cyber fire department. This would be an organisation or a collection of organizations that you could call on if your cyber house is on fire. If you are under attack, if you do not have the capability to respond, it's like being at home with a little garden hose when your house is on fire, need someone with a big hose and a lot of water to help you put it out.

So the idea of using fire department ideas rather than purely law enforcement ideas to help combat the side effects of these cyber attacks may be important. The second thing about this is that you don't necessarily know that it's an attack. Sometimes it's a mistake that someone made, maybe even in your own information technology department, a misconfiguration of something leads to a consequence that looks like an attack, but it's actually something that's happening to yourself caused by your own equipment.

So this leads me to one other observation. The cyber fire department model admits voluntary work. And I hope you are aware that in response to the worm that there has been an ad hoc agreement among a large number of parties across international boundaries to cooperate to combat the confiker worm. This is an important notion of voluntary and ad hoc organizations as opposed to formal constituted organizations to respond to these problems.

Finally, I want to suggest to you that terms like cyber warfare and cyber war create a kind of mind set which I do not believe is entirely constructive. The problems that we face with the vulnerabilities in the internet are not the same as national warfare. We don't have the bad guys wearing uniforms. They don't announce themselves and show up at battle lines anywhere. It's more like a guerilla warfare problem.

So the term warfare and the tactics and strategy that go along with it may turn out not to be helpful in thinking about how to respond to these problems.

So I would like to suggest to you that we not use that metaphor at least without very, very careful thought. The final point I want to make, especially along those lines, is that war is a very important decision, and attribution of an attack is very, very important when you make such decisions. It's not clear how easy it is going to be to identify the source of a particular attack. And until you have clarity as to attribution, I think it's very dangerous to take national decisions with regard to response to cyber attacks. And so here I would urge great caution and I would strongly endorse multilateral and multistakeholder discussions to come up with good tactics for dealing with these problems. Thank you very much, Mr. Chairman, for allowing me to take time this morning. I look forward to the remainder of our workshop.

>> DAVID SATOLA: Thank you very much, Vint. I am happy to announce that the last member of our speaking panel has

just arrived, welcome, Mr. Kalfin. We will now proceed to Mr. Henry Judy who will give a brief overview of our workshop background paper, and then we will move onto the rest of the session. I will set up the power point slides here.

>> HENRY JUDY: We had tried doing this earlier, and it ripped out the cords. (Laughter) I can't see the slides, so there we go. Okay. Well, maybe I have them memorized so I can work it out that way. Good morning. My job is to quickly summarize the background paper focusing on its structure and the questions that it asks. I'm not presenting personal views except for one thought at the end. The paper is available at an address that will be on the final slide.

Which version do you have? Oh, great! Okay. I will work on it from here. Up at the top of the background paper is an extensive disclaimer which basically says that its authors are not responsible for it in any way nor their organizations. It's on every page. I would like also to start with a brief acknowledgment. The paper was based initially on some research that I had done, but that it was in a format that was not entirely appropriate down, not as loud? Oh, okay. That will do. That will do.

But it was not in an entirely appropriate format for this venue and it was completely reworked by Jim Densey of CDT who did a masterful job, and he could not be here, he is represented by his colleague, John Morris over here. But I want to acknowledge the excellent work that Jim did.

The workshop theme is essentially legal aspects of cross border efforts that address the tensions among a number of concerns. First, cyber security issues, protection of human rights and values, protection of vital economic interests, and addressing complex technical issues that are involved such as the problem of attribution which Vint mentioned.

The paper's outline goes along the final lines. It starts with a number of developments that have been the basis for the heightened concern, and then national, international, and organizational responses to those concerns. And essentially there is the law enforcement response, cyber crime, the corporate and governmental response dealing with building and defending more secure networks. There is the military and diplomatic response dealing with cyber war issues that Vint mentioned. Then there are the issues of how do you on a national basis and on an international basis structure responses to these matters, and finally, there is an exhibit which contains extensive bibliographic references. I'm not going to spend a lot of time on recent developments that prompted recent concerns, we know about major data breaches, malware, espionage, cyber crime and the like. Let me talk, just to put on the table, about the law enforcement response particularly cyber crime.

There have been several instruments that directly deal with that, the Council of Europe, Budapest convention and the like. There are a number of indirect efforts dealing with cyber crime such as re examining privacy laws, some hundred countries have adopted some form of cyber crime legislation, often based on the Budapest Convention, however, a recent U.N. crime conference was unsuccessful at negotiating a global cyber crime treaty, and one of the issues is, you know, why.

So some questions for conversation under that heading is how the disagreements that were involved can be bridged to balance different interests, rights and values, rapidly developing technology, local limitations on resources and expertise, the existence of nations, states that serve as safe havens, and the dynamics and incentives that exist for a nation to serve as a safe haven.

As far as building and defending more secure networks, the corporate and governmental response, I think it's important to take into account that the critical infrastructure is actually in three hands. There is the private sector, the government and quasi governmental entities and then part of the internet that are effectively in both hands because of the extensive connectivity between them.

Responses include the work of various international bodies, ICANNs, promotion of the security extensions in DNS sect, the work of the various CERTs. The questions involved are should pro sections for governmental networks be extended to privately owned networks or should private sector manage its own intrusion and detection systems? For example, in the United States, there is a programme called Einstein which protects the federal network and it has the ability to be extended to the private network to private entities should the government extend its umbrella in effect to portions of critical infrastructure that are in private hands. If so, should that be legally compelled, should it be incented? How do you delineate where the edge of the umbrella is?

And then what are the legal effects of transborder data flows that have the protection extended over the servers that contain them. Is any protection provided by having a third party audit the behavior of others. You wind up with, you know, Horace's question of who shall guard the guards themselves. In the military and diplomatic response is the cyber war issue. In January of 2012, the ITU general secretary suggested that there be a treaty in which nations would agree not to make the

first cyber strike against one another.

Recently in NATO they have agreed to revise their strategic concept to determine which kind of cyber attack, which level of cyber attack would trigger the obligation of collective response under section 5 of the NATO treaty. There are a variety of issues presented under the UN charter involving obligations of self defense. And some of the questions that are involved are exactly the questions that Vint put on the table, that is putting aside issues of proportionality and necessity, how does one distinguish between military and civilian targets? What are the implications if somebody distributed deliberately the stuxnet virus that affects scatis systems that control your infrastructure. What issues surround the use by a nation state of non governmental proxies such as bot net operators.

There are a variety of obvious economic concerns, the negative effects of cyber crime and cyber war. There are also the economic effects of cyber defense. Cyber defense is extremely costly and it often results in the bulkization of networks and database. What are the economic effects of governmental demands for access to encrypted information? How can you protect trade secrets. How can lawyers and doctors and accountants maintain the confidentiality of their records?

I want to turn now quickly to structuring national responses as the issue. The U.S. has, for example, its comprehensive national cyber security initiative. There is a European programme for critical infrastructure, protection. There are various programs in other countries, but the questions for consideration include what are the most effective means of promoting coordination and cooperation on the national level? How far should governments go in regulating the private sector in the name of improving cyber security? What are the relative roles of civilian agencies, National Security Agencies, ministries for trade, commerce, and communication. When I want to turn now to the heading of promoting international cyber security. This is important because fundamentally no nation can achieve adequate cyber security on its own, regional and international cooperation are necessary. There are various efforts in that regard by the EU, Council of Europe, there are various efforts at the UN. That raises immediately the kinds of question that's would be involved in a cyber security treaty, what are the key issues that need to be involved? What are the added what's the added value of such a treaty? What are the risks of a treaty? What are incremental step that's can be taken to break through the problems that have arisen and the fundamental problem of how would such treaty compliance be verified? One needs to reconcile different versions of or visions of cyber security. Some see that as essentially a matter of state security. Others see it as a matter of internet governance with balancing various interests including national security, human rights and economic development interests.

You know, what are the best venues for dealing with this? What are the role of international or intergovernmental organizations? What are the role of regional organizations? What kind of supporting efforts can be made within the business community?

I like to turn now briefly to the issue of non state actors and safe havens. The issue that's presented is that cyber crimes can be considered to rise to a level of use of force, that's the term in the UN charter that amount to cyber war crimes at least in the view of some. We are not dealing, at least in these comments with that kind of use of force, but rather the interplay of the articles in the UN charter that deal with an obligation not to use, not to interfere with the territorial integrity of others, but at the same time, a collective right of self defense.

There is a recent proposal. It was made by the U.S. council on foreign relations, and it suggested seeking an international agreement to ban denial of service attacks. The url of the article in which that is done is in the slides. And this is argued to have certain advantages. It deals with a specific problem, not complicated by intelligence collection. You know, they are, denial of service attacks are essentially bruit force attacks so they don't require networks to be penetrated, only sabotaged. It provides a good concrete first step to build on. Most denial of service attacks are carried out by criminals for the purposes of extortion, and it would be a very good opportunity to check out the bonafides of a partner who sign such an agreement.

With that, Mr. Chairman, I would like to conclude, and just since people can't see the slides here, I would like to give the address of the whole background paper HTTP://BIT.LY/9xAdAV. Thank you, Mr. Chairman.

>> DAVID SATOLA: Thank you very much, Hank. With that overview of our programme as provided in the background paper, I'd like to now move to the regional responses to these various issues, and I'd like to begin with Mr. Ivalo Kalfin of the European Parliament. Mr. Kalfin, the floor is yours.

>> IVALO KALFIN: Thank you very much, Mr. Chair. I think we need to talk about sound security, not only cyber security in this environment. But I really would like to congratulate and thank very much the organizers and supporters of this event because the cyber security is an issue which is quite unevenly tackled and dealt with in the different parts of the world. And

as it was mentioned already, the international cooperation in that field is indeed an important one. I am happy that ICANN is involved with dealing in cyber security issues. I have been working quite directly or indirectly, like George Sadoski, for the development not only of internet but also the international co op race. I will start by saying I have quite an approach of what is happening in the European Union with cyber security. Cyber security is an issue which is not properly enough tackled within the European Union, which is not dealt with appropriately with the community policies, and which even meets different understanding in the different countries across the European Union.

And at the same time, the union is trusting very much on the development of the information and communication technologies, on the development of the digital agenda, the way it is called in the EU, for promoting economy, for promoting the social progress, for the promotion and development of European Union. Why the cyber security issue is not a very high profile issue when this is debated within the European Union might be a question with various answers, and you would certainly hear different answers if you ask different people from the European Union.

The fact is that in some member states you have excellent national systems for cyber security and cyber crime prevention. You have other countries where you have just nominal actions in that field, the question of CERTs, for example, and you have other countries who, that consider this is not an issue which is considered to be very high on the priorities. And they particularly don't devise any policies in that field.

There were several attempts within the European Union to deal with the cyber security issue. All of them failed because of these different understanding about what is the cyber security and to what extent the European Union should apply the community methods not the national organisation methods in order to tackle the issue of cyber security. There is an agency, the European Network Information Security Agency, ENISA, that has been created and at the time of creation of this agency, there were quite considerable disputes within the union about the role and the need of such an institution. The result is that the agency is very nicely based in the Greek island of Crete. It has a temporary mandate. It is doing an excellent job in coordinating national efforts and national cert but it doesn't have the political clout. In the last year or so, months even, there are some positive developments. This is the adoption of the critical information infrastructure and protection directive, which is a major step forward in terms of setting European wide policies for cyber security. This is also the creation of special position, commission also attending the internet government forum, and she is, I mean, her portfolio is directed to deal with the digital agenda, anything related to the development of ICT's and the digital development of Europe.

And from several conversations we had with Commissioner Cross, I am quite comfortable she understands the high priority and the importance of cyber security. We have several things to solve in the European Union, but ideally, I would just sketch what I believe is very much needed in order to enhance cooperation. And these are three things, first is to create the position of cyber security coordinator. I would make a parallel with the U.S. experience, but I think this is one of the good experiences and such a position would very much help the development of these issues in the European Union. Second, there should be a very clear and comprehensive strategy on the fighting cyber crime and protecting cyberspace and thirdly, the European Union needs to become a factor in the international corporation on cyber security.

At the present moment, there is no personalization, there is not a person who you would say this is the cyber security person within the European Union. All of you, I'm sure you have the experience of many international where you see excellent representatives from member states but you don't see a representative from the European Union talking about European Union policies and European Union commitments in the international cooperation on cyber security.

So these three elements I think are very important. They have to be devised in the very near future. The way to do that is still, I mean, we have the formal reasons still in the months to come. There will be a vote in the parliament on the digital agenda, there will be a vision promoted by the European Commission on the digital agenda and the development of the digital technologies in the European Union. This is one of the opportunities to deal with cyber security issue.

The second one is the discussion about the mandate of ENISA, the European Information Security Agency, it's mandate is expiring. From what I understand in the European Commission, the idea is first to simply prolong the mandate in order to have more time to discuss about the role of this agency. And that makes me optimistic because such an agency needs to have a very strong political backing and a very important role horizontal role in setting the policies of the European Union.

So we have these chances. They will come by the end of this year, and I really hope that the European Union would be able to properly tackle these issues.

Again, I have to tell you that we are still in the phase of awareness of speaking about the importance of these issues, of asking to commit also finances because cyber security without the proper financial backing is also not something which is

realizable. This is very much like the insurance, that's an additional cost, but you know why you take that additional cost, and I think it's very important to consider the prevention in cyber security as a top priority in the European Union, not so much the reaction to cyber security.

So these are issues that are going to be tackled, and, again, I think that like this one, experts and people like the ones that talk today are very crucial and in order to help promote and give an impetus to this debate within the European Union. Mr. Chair, I won't speak very long, I just wanted to point this issue, maybe on a rather critical note, that I think there are plenty of thing that's need to be done at the European Union level, thank you very much.

>> DAVID SATOLA: Thank you Mr. Kalfin. Mr. Kalfin, I understand you may have to leave the session early? No. Okay. Fine. Then we will reserve questions until later. Thank you.

I'd like to now move onto the Council of Europe to hear their perspective, and we will talk with Dr. Ralph Favo.

>> RALPH FAVO: Thank you Mr. Chairman. As you can see from my second slide, the Council of Europe has been quite active in trying to develop documents, conventions, et cetera, in the field of cyber security and cyber crime. The most important document is very obviously the cyber crime convention or Budapest Convention. Alexander Sager is going to address the convention in a few minutes. There are other conventions dealing with cyber security as well as well as recommendations and sources which I'm not going to look at during my presentation.

I would like indeed to address the most recent initiative and this most recent initiative goes back to the resolution on internet governance and critical internet resources which has been adopted at the occasion of the conference in May 2009. The resolution refers to a shared presentability of the 47 Council of Europe member states to take reasonable members through multilateral corporation to insure the ongoing functioning of the internet and the consequence that the delivery of the public service to which all persons under their jurisdiction are entitled.

On the basis of this resolution, the steering committee on the media and new communications services has appointed an expert group, and advisory group on cross border internet capacity for persons. I am a member of this group, and I would like to let you know what we are doing. It's ongoing work, we are not yet half the way through all of the problems, therefore, input, of course, from the audience is very welcome.

The interim paper which is available addresses four topics according to the mandate of the expert group, namely generally protection of internet resources and transnational management of critical internet resources. Furthermore, protection of cross flow internet traffic and the prevention of and response to cyber attacks. The paper would be available from the secretariat if anybody should be interested in this paper, but as I said, I am not going through the paper, but I would rather concentrate on the cyber security issue which is maybe 25% of the work of the expert group.

The first item I would like to address as you can hopefully see from this slide is public awareness. Why do I want to address public awareness? Very traditionally, security is a state matter, and this is somehow a consequence of the old concept of state sovereignty which already enrollment times allocated a use of to the nation states. However, needless to say that this concept is not any more viable. Cooperation is needed in a global environment. The internet is a global information system, and, therefore, security interests cannot anymore be dealt with on a national level.

So we need to change previous paradigm, and in particular, we need to come away from the traditional concept of having cyber security or security issues dealt with within a small group of people having military functions or related functions. So more public awareness is indeed needed, and this means, of course, that the exchange of information about structures, about contents of cyber security measures should be and this would equally mean that participation in the development and implementation of internet use, education, and public awareness programs, promotion and facilitation of dialogue with stakeholders is a target which should be achieved.

As has been already said by Vint in his introductory remarks, not only states and even less not only military services are concerned, but we do have a lot of civilian cyber security issues. We see the situation that infrastructure is to a far extent controlled by the private sector. Politics play a role, and if reasonable measures should be introduced, then a more broad caution including public awareness of the measures is needed. This leads me to my second aspect, namely prevention.

While I do not have to repeat what you already know very obviously, states, of course, should ascertain whether activities involving race of causing significant transboundary experiences are taking place within their jurisdiction, assess the adverse effects or consequences that such activities may have, and provide timely notification and relevant information to potentially affected states.

States should exchange relevant information and enter into consultation with the view of achieving mutually acceptable solutions adopting measures to prevent or respond to cyber attacks or other activities which may cause significant transboundary interference with internet resources or at any event to minimize risk thereof. How can this be done? How would it be possible to establish that kind of international cooperation when preparing this workshop I thought that some kind of special network could be established, let's say the persons involved in this network would be experts from various fields, and also from various sectors. So living according to the principle of multistakeholderrisms, when listening to Vint this morning, I liked very much the new term of the cyber fire brigade. This seems to be a convincing term to show that we need some kind of new organisation of new network, and obviously in traditional times we do have a fire brigade for probably each and every municipality. This would not be as which should be implemented in cyberspace, we would have to establish some kind of global fire brigade or at least different fire brigades being connected through a line which could be activated in case of an incident.

Then, I'm turning to a third aspect which I call capacity building and I would like to use this term in a very broad sense. Capacity building, of course, also encompasses the question how responses to cyber attacks could look like, but could and should be done not only in way of a counter attack, but by exchanging information in a way that the effects of cyber attacks could be mitigated, in my opinion, mitigation of damages is probably much more important than just to start a counter attack causing even further damages.

And the second element in this context is, of course, responsibility and liability. This topic I know is very sensitive. Nevertheless, I do think that we have some kind of a precedence coming from other fields. We know liability provisions from international agreements in the field of environmental protection, think, for example, of damages caused by hazardous waste, think of damages caused in natural catastrophe, et cetera, and furthermore, we have draft articles of the international law commission on state's responsibility at these draft articles also contain provisions on liability. The work of the expert group in this field is not that much advanced that they are going to propose specific groups, but we should think what analogy we could show to other norms in different fields. Summarizing my thoughts, what challenges are coming up in the near future, first of all, the question which I mentioned, how can we implement multistakeholderrism also in the field of cyber security?

How can we involve all sectors, all relevant players in the field? What strategy could be chosen for this cyber fire brigade.

The second aspect, the understanding of Sovereignty has to be changed. Traditional and notion of Sovereignty has overcome and we have to move to a new and more adequate understanding of Sovereignty, and finally, we should start a dialogue to the extent that international norms on liability may have to be developed knowing that this is, of course, politically a very sensitive topic. Thank you for your attention. Thank you, Mr. Chairman.

>> DAVID SATOLA: Thank you. Now, I will turn the floor now to Alexander Sager also from the Council of Europe. Thank you.

>> ALEXANDER SAGER: I had one slide, it's only one, but, still, if it could come to the screen. Thank you for inviting me to speak here for two, three minutes. I would doubt that if we talk about cyber crime, and if we talk about cyber security, whether we talk exactly about the same things. I think we have to make some conceptual distinctions here. When we talk about cyber security, we talk primarily about protecting information technologies. If we talk about cyber crime, we talk about criminal justice responses. We talk about protecting the security, yes, the confidentiality, and availability of computer data and systems of people, and we talk about the rights of people.

We talk very much about procedural law. We talk about safeguards and conditions in procedural law to prevent abuse, and many other things.

I would also fully agree with Vint Cerf who talked about the mind set if we talk about cyber war and that sort of things. As long as we cannot attribute attacks clearly, it helps to talk about cyber crime because it helps deescalate a situation. We can take something down from a national defense, I war level to the issue of let's try to find the criminals behind this. Let's try to take criminal justice measures, and if we can attribute, maybe at some point we have to go farther than that.

Nevertheless cyber crime, cyber security have many things in common in many different institutions to deal with different aspects, we will need to work together at a national level, people, institutions dealing with ICT security, have to work more with criminal justice authorities, and at the international levels institutions like ITU need to work more with organizations like the Council of Europe.

There has been some reference made to discussions about international treaties, new treaties developing and so on. We believe that the instruments and tools to deal with cyber crime are basically already available. We have for cyber crime the Budapest convention. We have models of public private corporation, we have tools for protecting children, we have very effective tools, well, sometimes more, sometimes less effective tools for international cooperation, and so on. The key challenge we see, the key problem that we see is the that these tools are not fully implemented in all regions of the world. Just to show that we have been talking much about Europe, there has been somebody from the European Union parliament., but just to indicate that with regard to the Budapest Convention we have been working with Sri Lanka. In the last two months alone we have been working with Cambodia on the cyber crime legislation, with countries in North Africa on the cyber crime legislation, we have worked in Mexico a few weeks ago with six or seven countries of Latin America on the cyber crime legislation. Next week I will be in Indonesia to condition on cyber crime legislation and today Australia and Argentina will be formally invited to the Budapest convention. We are a regional organisation, but we are developing instruments that can be applied globally and that includes in particular the Budapest convention. So the core problem that we see is that, as I said, the existing tools and instruments are not fully applied or the pragmatic way ahead would be to insure full implementation of what exists already.

Reasons include that there is a limited understanding, sometimes a limited interest at leadership levels, at political leadership levels. I truly question how many political leaders are at the IGF. I think the number is very limited. That is part of the problem. We also see that as a lag of capacity to implement in terms of training programs, institution building, et cetera. At the United Nations Crime Congress in Brazil in April this year, this was clearly confirmed for everybody. There was no agreement on a new treaty, but there was full agreement that capacity building has to be given priority.

So what we need is enhanced capacity building also through development cooperation. We have to acknowledge that measures against cyber crime will contribute to rule of law, human rights, democracy, social economic progress, good governance and so on. I'm very happy, I must say, that this workshop has been co organized by the World Bank because not so long when I invited the World Bank to come to the octopus of the council of Europe said actually cyber crime is not of interest. Maybe it was a mistake to invite me to this. So I think it is important that official development agencies also get stronger involved in supporting countries around the world in measures against cyber crime. As I said, the tools and instruments are available, but they need to be applied.

Another element that I would like to point out to you without coming to a concluding point and a conclusion on that is at the Council of Europe, we have a lot of experience with monitoring. We develop standards, we develop treaties, but we also say that monitoring mechanisms to see, to make sure that countries comply with those standards. And I'm wondering whether we should not think in terms of reviewing monetary mechanism for cyber crime. We have some experience with corruption, money laundering, there is also the experience of the financial action task force that we may seek inspiration from, but this is something we should discuss more.

There will be an opportunity to discuss it more and I advertise my own workshop this afternoon at 2:15 in room four there will be a workshop on cyber crime. There is a leaflet here I can circulate and those coming to the workshop will get a free copy of the Budapest convention on cyber crime. Thank you.

>> DAVID SATOLA: Thank you Alexander. Before we move onto the country portion of the programme, let me assure you, Alexander, if you had invited me, I would have come. Because we are quite active in the area of promoting measures to combat cyber crime in our borrowing countries. With that, let me move on to the national portion beginning with Jayantha Fernando, and I will turn the floor to you and get your slides up in just one second.

>> JAYANTHA FERNANDO: Thank you. Thank you, Chairman. Thank you, David, for inviting me for this forum to give an overview of where our things stand in Sri Lanka. I have too many slides, so the intention of my presentation here is to let the audience have a glimpse of where we stand in terms of development initiatives and the kind of measures we have taken in terms of the laws relating to ICT. And then perhaps give an overview of how international cooperation can help. So that is the substance of what I'm going to say.

And moving on, Sri Lanka's position currently has been improving rapidly, and in terms of where we stand, the ICT development sector has gradually over the last, two, three years, has reached the level where it is the fifth largest revenue earner for the country. And in terms of BP or location index in the global services location index, we are ranked 16 amongst the top 50, amongst the top 50, which means we are amongst the first 20 emerging cities in the location index.

Now, in terms of measuring where we are, we rely on the global economic forum, the world economic forum, the global information technology report, and if you go to the specific details there, you will see that the index has been improving rapidly, especially over the last four to five years, and moving on, all of this has been the result of broadly constituted multistakeholder driven ICT development programme supported by the World Bank known as the eSri Lanka development project. And the objective of this programme is to take the relevance of ICT to every village and every city and every vista and transform the way government works and also thinks. That's a very hard task to achieve given the climate for which we are originating.

The programme itself was started in January 2005 and has progressed immensely well, and all of the broad band in this slide moving on, there are multiple programs in it, all integrates together, and the centre piece besides eGovernment, infrastructure developing capacity in private sector and in government and also creating and addressing the rural leads we have a centre piece known as a policy, leadership and institutional development under which several law reforms were undertaken. The objective of that centre the IT policy is create policy lead and implement ambitious ICT programme.

In terms of where we are, in terms of ICT located legislation, I agree with Dr. Vint Cerf's statement that crime is not only recent motive to have legislation in place, and in that context, we have very unique set of precedence that we can share.

We have adopted, we were the first to adopt the electronic conducting convention known as the U.N. Convention on the use of conventions and international contracts and adopting best practices we have enacted electronic transactions act that provides a technology neutral framework for the use of digital signatures and electronic signatures, et cetera.

Now, in terms of preventive measures to combat cyber threats, crimes, et cetera, we have enacted the payment devices ant the computer crimes act and at the moment we are trying to address child pornography issues by replacing the entire legislation with a new act. Now, in doing all of this, we also face numerous challenges, and I would move onto the challenges quickly, and then the challenges, I think, were discussed across the table by many other speakers before, so I will not send too much time about that, but to say how what kind of measures have been taken to address them.

So we are developing forensic tools and embarking on capacity building efforts and developing the necessary tools for cyber crime measures to be addressed in a significant manner and trying to be an example for the region. And in that plight, we have established a set of institutional measures manifested in the Sri Lanka cert established in November 2006 handling roughly 10 indents a month and from inception, it has addressed 315 incidents and we were instrumental in creating this entity as a private sector model so we can hire the best talent from the private sector and include them in a government enterprise. And I will admit when I was writing the first memorandum to create this entity there was a lot of eyebrows raised but that was one way in which we could drive this initiative to sustain and maintain with a unique pool of talent absorbed into this entity with good salaries, et cetera.

Interestingly, this entity, the Sri Lanka cert was one of the first to get AP CERT, and now they are part of the global first community. Now, how can international cooperation help?

I have identified three broad areas in terms of establishing the necessary legislative framework and then building awareness and capacity building, and thirdly, cross border enforcement and judicial cooperation and in that context, I would like to come into a follow up to what Alexander said, the importance of the Budapest Convention and how it has helped us. And given a bit of your view of what the donor programs can do, and in that plight, I must say that international cooperation more from a donor perspective has been tremendously helpful, not forgetting the role of the private sector. Now, in terms of the first three, that is in terms of legislative practices, best practices, and developing capacity and providing a framework for mutual judicial cooperation and enforcement cooperation, we in Sri Lanka look at Budapest convention as a best practice model and I'm grateful to the bureau for the support and the overarching help extending at a time of need five years ago when they were looking at best practice model. They looked at it and said look here consider this a as best option, and here we are able to talk about it as a best practice model and we absorbed its principles into our national law and at the moment our cabinet of ministers is considering and a discussion is ongoing in Sri Lanka as to whether we should sign it and the results of the discussion is so far positive and we are hopeful that sometime during this year or next year we will be able to sign up with a convention which is opened to non European states.

One factor I want to emphasize, a significant factor arising from the convention is that in the Commonwealth of Nations, I'm talking about the British Commonwealth, we are part of the British Commonwealth, Sri Lanka was a colony of British years ago, in the British Commonwealth there is an international instrument known as legal assistance in criminal matters.

Interestingly part five deals with criminal evidence, electronic evidence, et cetera, gathering electronic evidence and mutual assistance cooperation in that kind of subject. And at the moment, this scheme is being reviewed and being considered,

and member states are looking at amending it and in doing so, they are drawing on the best practices embodied in the Council of Europe convention.

Then in terms of other types of cooperation that we can rely on, I want to emphasize the significant support provided to us by the World Bank. I mentioned at the beginning that the entire Sri Lanka development programme, the ICT development initiative that set the stage for ICT development to take off in Sri Lanka going back six years ago included important component, and that was entirely supported through the World Bank private sector development team. And the Sri Lanka government is extremely grateful for their support and through that support, we were able to draw on best practices, participate in international forum, and even move onto the level of establishing a very dynamic Sri Lanka CERT that has become a global best practice and currently the World Bank has given us to establish currency for the police department that will hopefully help to address and deal with cyber security issues from investigation perspective.

Then from the private sector perspective, my find point I want to highlight is the measures and support afforded to this fourth process through Microsoft. Microsoft came to us and helped Sri Lanka sign onto what is known as the security cooperation programme, the CSP that has helped us to be part of the global private sector forum addressing and dealing with these issues, and then the ICANN that has provided through law enforcement due diligence review process that insured some kind of uniformity in terms of how the issues are dealt with from point of DNS. So finally some key take home messages I would like to share with you.

Firstly, the results of the Sri Lanka forum was not by extent, it was by design. It was included in the oral ICT development road map, which was thankfully supported by the World Bank. And the inclusion of this as an agenda item in a development assistance programme helped us significantly. So I would urge multilateral donors who support development initiatives who are supporting development initiatives to include the law reform component in their efforts and in that plight I am happy to see other countries in the region, Pakistan, we have a member of parliament from Bangladesh seated across the table. They are all taking efforts against Pakistan is leading the way in some areas, so is Bangladesh and we have India, which is a very interesting country that has taken a lead role in getting certain laws in place in this collection.

Finally, my parting message is that the development cooperation afforded to us has helped Sri Lanka, and our agency, the ICT agency of Sri Lanka to be positioned, to be in a position to lead the process not only to the acquisition of the Council of Europe on crime but several other international treaties we are looking at. Thank you very much.

>> DAVID SATOLA: Thank you very much Jayantha. I would like to turn the floor to Erick Iriarte to get his perspective from the Latin America perspective. Thank you.

Erick, if I could ask you to take five or six minutes.

>> ERICK IRIARTE: Five or six minutes to start. Okay. An interesting thing being Latin American in this group is I tried to put a perspective of what is happening in our region. The first thing is our problem is not about revelation itself. In Latin America, we have in older countries a different kind of relation about crimes and about civil crimes too that happen in the past ten years.

The problem is what kind of revelation we have the quality of revelation we have and third is we don't have Harmonization of that revelation. That means that for some countries like Peru, we have regulation against spam but only if spam is inside the country. If somebody uses a server in Bolivia, our neighbor, the law is not enough to try to persecute the crime.

When our countries try to develop a regional agreement for Latin America and Caribbean about cyber crime, one of the more difficult problems is each country especially in criminal law they want to have their Sovereignty to decide what is crime, what is not a crime, when the court could be part of note of a process how the police could act and prosecute a crime or something like that.

So finally, we arrive to some table like that, and we don't arrive to no place.

Five years ago Latin America decided to create a political document and all it like information society like Europe but the Latin America version. One of the goals was to request to all countries in Latin America to signature the Budapest agreement. That was the goal in 2005. Five years later not one country sign it. Some of the countries approach to that Europe council community to see about that agreement and try to sign it. I know that Panama, Dominican Republic, Chile, also Argentina are interested, but it's not really active in our document base.

Second, the problem is not necessarily our difference of point of view. We can have access to create a regional legislation, but this regional legislation need to be alongside with the either regions and it's not clear how we don't have in the world

any kind of regulation international treaty for all of the countries. If you have only one country that don't sign that kind of agreement, that country will be penalized for the crimes. So the question is who will put the bell to the cat, who will put the country or region who will take the decision so say we can advance in that way to have this kind of treaty? The Budapest treaty is the best approach right now.

We are agree in the region in the political level to sign Budapest. The problem is when you put that to the local ministers or to the local policemen or to the local communities and say we are not agree with you, we believe that our law is so strong our doctrine about crime is so strong we can implement something different.

In the past ten years around 90 different bills were passed in Peru, no one compared from in the law, but the same case happened in all of the countries in Latin America. So each one of the parliaments have a different point of view of why this is crime or why this is not. The problem is about harmonization. And the principle problem is we can live without that revelation because our criminal codes analyze the minority of the crime without the part of the internet or without the technology issues. So internet is a fraud.

So our don't want to see any case that have any aspect of technology, why? Because they don't understand. And we don't have neither a capacity building process to help them to create that capacities to resolve that case with the laws existing. One of the principle countries in our region is Brazil. And Brazil have around 2,000 resolutions in the court about cyber crime in different levels about different aspects including child pornography, fraud, and other kinds of crimes and they don't have a specific revelation about cyber crime. If they can I mean the lawyers, the community, how is it not possible to make that same in another countries region. Finally, I come from the LACTLD, the American association, our communities mix in the same person in Honduras, the same institution, the CERT, the IP registry and other things so that means when that organisation don't help in the process to the development or don't be complicated to help in the process to promote regulation about cyber security or cyber security, the process will be only one side, only one vision, and it is a vision of the state that want to regular laid and only regulate a process, but don't understand that the process of regulation and information society things are mutual stakeholder.

Right, because this is the style to do the things of the states. They come to listen but don't necessarily create the regulation with the others. This is another kind of process. Finally, and I have something more to say, but we will have time in the next IGF, I hope, we will have a next IGF, when a country tries to resolve the problem a cyber security appear a lot of private companies or civil society organisation or itself some people from inside the government to say I am the specialist in cyber crime, I am the specialist in cyber war, I am the specialist in something to try to sell not necessarily a product or not necessarily a service, want to try to sell an idea, an approach. The problem is when this approach only sees one part of the problem, how we can resolve the other parts of the problem. It's necessary to implement policies first and then create regulation, a problem of our freedom in Latin America is we create regulation without policies. And this is a big problem.

Without organisation that are strong in our country that can make the policies about information society, not alone, involved in the international policy of development, our problem for that, I am a lawyer, the lawyer that the regulation allow information societies, we believe that we start a war. So before us is nothing. So we need to create cyber crime we need to create electronic signature and we don't understand that before us we have a lot of regulations that could be useful if we develop the capacities in the person that make the decision. How is that process created in the past ten years? Maybe I have more questions than answers, but the reality is we don't work together in a mutual stakeholder approach with the government with the private sector and civil society first in great policies and then great regulation, we will continue talking about cyber crime, cyber war, cyber security in the next 20 years.

>> DAVID SATOLA: Erick, thank you very much. Andrew, if I could please call on you to give your reactions and the U.S. perspective, thank you.

>> ANDREW McLAUGHLIN: Thank you very much. So let me start is this all right? How is that? Better? So let me start by telling an anecdote about why I think this problem is hard. The anecdote is that a few years ago I used to teach a class on internet law and one of the things I would do with the law students was have them take on what's in the Anglo Saxon legal system or tort problem, torts are the laws of civil remedies, when I punch Vint he gets to sue me and for how much.

One of the torts you learn about in law school is trespass. So trespass is the idea that if I walk onto somebody else's land, I have violated their right to control and enjoy their own land.

And the problem for the students was to translate that into a digitally networked environment. So nay digitally networked

environment, we have the idea that there can be such a thing as trespass. In other words, I can go and do something to somebody else's laptop or server or router and it feels like trespass. The problem though is that I'm not physically doing anything other than sending a set of commands to that machine. That machine is digitally networked. It is intended to sit on the network and receive commands from other people and then respond to them.

And so the notion of trespass kind of falls apart. From a legal perspective trying to figure out legally how to describe hacking, cyber crime, violations of cyber security, it's actually quite difficult in a traditional legal architecture. All that I'm doing as a hacker or as a malefactor is sending a set of commands to another machine and that machine is responding.

That machine is responding in ways that the owner of the machine might not like if he or she thought about it or were presented with a question do you want to send all of the contents of your hard drive off to this remote server, but the machine is simply reacting.

Anyway, the reason I say that is that it just captures the reality that the legal frameworks and legal models that we have before don't really fit the cyber security cyber crime area well. And I want to say at the outset that it seems to me essential to break this problem down into different pieces, Vint, other have said, you know, suggested distinctions that we draw, the distinction that I want to draw from my remarks is between network security, meaning the security of the machines that compose the network itself, protocol and standard security, which is the ways in which we exchange information across the network that everybody agrees to use, and application layer security, which is software security, the software that runs on those machines, these are three different problems and I think it's generally helpful to think about internet related issues in a layered model, physical infrastructure, the software that runs them and then the applications that live on top.

And so the issue that we have got, frankly, is that we often talk about cyber security in this kind of lumpy fashion, and ignore the fact that much of what we are dealing with, frankly, is buggy code and end systems. So buggy code at the application layer is driving a vast percentage of the opportunities for violations of cyber security, cyber crime and so forth. And I'm going to come back to how to deal with that, but before I do that, at the network layer alone, one of the things that the confiker working group that Vint mentioned before pointed out and documented well in the course of their efforts that sort of tangentially documented across the network infrastructure globally, there are all kinds of brain dead operational thing that's people are not doing.

So to pull out three examples that they identified, many edge routers are not doing what's called ingress filtering. There is an ITFBCT document that specify that's there are ranges of IP addresses that are not publicly routable so edge routers and networks should not in fact be accepting packets that claim to be from those IP ranges. Second, our edge routers, which is to say machines that hand traffic off between autonomous systems are often given publicly routable IP addresses, this is contrary to best common practices. You should be using link local addressing which is to say not publicly routed addresses for two machines talking to each other to hand traffic off between networks or autonomous systems. Third, we find routers on the internet or using factory default password and user ID's. These are things that any network administrator ought to be doing and a big part of the problem we face is that people aren't doing what they are supposed to.

So you have got a human problem, a behavioral problem, and then the software equivalent of that which is software being written in ways that are properly described as buggy.

So metaphorically then the model I want to resist or argue against is the perimeter defense model. Very often in governmental circle there is this tendency to think in terms of the fortress or castle that what we are trying to deal with is a world in which my laptop here can communicate with a vast array of servers across multiple network paths and the idea that I can somehow secure is either through the network or through some kind of magical piece of software on my own laptop is just fantasy.

So the problem that we are dealing with really is the externalities, that buggy code and bad practice on the network create for everybody else, externalities across national boundaries, across organizational boundaries. Because everybody has been going along today, I'm going to spare you the recitation of the president's plan. The president commissioned and then released last year cyber security strategy. I have got a couple of notes here that I was going to go through, but you can just look it up, you can use Bing or the search engine of your choice to find it, type cyber security strategy, and I think you will get it, but one of the things I wanted to highlight is that a fundamental component of a resilience strategy as opposed to a perimeter defense strategy is innovation, game changing innovation around the way that we do operating systems and network machine software. Innovation around authentication and identity services, and also I want to talk just briefly about international cooperation.

So one of the things that I think is particularly important, if you accept my model that a resilience rather than a perimeter

defense strategy is necessary, is you need to, we need to fundamentally reengineer and rearchitect over the long term the way we do end system software. For example, operating systems. So within the U.S. government, we have identified a couple of different priority areas for research and development. Two I want to mention are something called moving target defense. So this is the idea that the operating system and its interfaces to the net need to be constantly changing in ways that the people that I want to interact with can predict, and that nobody else can predict. So predictable to me and my chosen interlockers, unpredictable to everybody else. Right now your lap top or desk top or mobile phone tends to have a static configuration so if somebody can identify vulnerabilities in the configuration, a moving target defense software approach to make unpredictability your friend. Another one that is quite interesting for work is insurance markets for cyber security.

One of the things we need to do is change behavior. Very good tool for changing behavior is to create an insurance market where you pay more the riskier you pay, you pay less the less risky you behave. We need an actuarial table for cyber security, we need to able to price risk and the only way you can price risk is if you have data about the monetary consequences about particularly risky behaviors. There has been a lot of discussion about software liability and for many good reasons it's a terrible idea to impose strict liability on software writers t would kill off open source software development and a lot of good private sector innovation would be disincented. Nevertheless there are behaviors associated with the implementation of software and behaviors associated with the management of a network that could be maintained with a properly functioning insurance market.

>> I think a layers model is useful. I want to mention a couple of things that the protocol and the network layer, which are examples of the kind of multistakeholder cooperative collaborative effort that is necessary to actually improve security in practice. One is the DNS Security Extensions that we have talked about, DNSSEC. It is a standard that was developed through the Internet Engineering Task Force but it's deployment and adoption depend upon the activities of network operators and the managers of networks everywhere in the world. Everybody running a network or machine on the network has to implement DNSSEC. It's not going to be done for you. The technologies and tools out there but it has to be implemented if we are going to secure the relaying of DNS data for transactions as we heard yesterday that number in the hundreds of billions every day. A related set of problems has to do with the security of the exchange of routing information across the network. So right now, we have basically still a trust based system for ISP's to announce which machines are properly routed on their networks and this is something called a process that used something called BGP or border gate pay protocol and one of the things has been a problem is people can announce routes that are not fully there. There is a famous case of You Tube being diverted to a small one day crushing the network capacity in that country, and messing up that service.

So it's a known bug. There is a set of fixes that are under way called a registry PKI or RPKI model where you would have an authoritative digitally signed table of routes, so that ISP's would at least be able to know when they are getting a claimed route as opposed to somebody else trying to hijack it. This is something else that is a good idea, should happen but will take multistakeholder cooperation among the protocol and network layers and the application writers in order to make this thing happen. Those are just some thoughts to be provocative and to speak at a higher level about the problems as we see it. The fundamental point is that if we are going to achieve resilience rather than false perimeter security across the network, it absolutely requires multistakeholder cooperation of the sort that we are attempting to model at the IGF this week. Thank you very much.

>> DAVID SATOLA: Thank you very much, Andrew. I would like to now quickly move onto the industry and civil society portion of the programme. We are running a little short on time. We have some extra time between the end of our session and the next session so I propose that we maximize that, but I would still like to move swiftly through the programme. So my next speaker is Mike Silver from ICANN. Mike, if we could get ICANN's perspective on this. Thank you.

>> Michael Silver. I have been asked by my colleague, John Crain, to step in. John works on the technical side, he felt as a board member and as a lawyer possibly I would have a better perspective, but I would like to pick up on what Vint and Andrew have been talking about, which is it is very useful to have law enforcement involved. All of the international cooperation, all of the government cooperation we are talking about is certainly useful, because if we want to now start beating Vint's analogy a little bit farther, once the fire has happened, it's useful to get the arson investigators out there and

find out who caused it, try and impose some sort of liability, civil or criminal, on the appropriate parties, throw them in jail and, you know, you can have your sense of retribution and feel good about it. It doesn't put out the fire. Better have the sprinkler systems, better to have the fire brigade and smoke alarms so that the loss is minimized. Then you can worry about, and I'm not minimizing what my colleagues are talking about. I think it's very important to have the international collaboration, the government collaboration around law enforcement and prosecution, but without the underlying capability to detect early, respond quickly and call out your friends to assist, the damage is going to be far higher. And certainly within the legal system I come from, if you are looking at a civil liability, then there is an obligation to take steps to prevent harm to yourself. So you can't simply stand there and watch your house burn and then lay the blame on somebody else, you have got to take steps and I think that's where as ICANN as a coordinator of global naming and numbering resources, we play a critical role because we do sit very close to the middle of the spider web through which many of these internet pipes go and we interact on a daily basis with the people who either operator in turn actually assign the names and numbers that are used throughout that internet network. On that basis, our critical aspect is preventive work and emergency response. And if we have time a little later, John will speak to it, but our real feeling is that policy event investigation and prosecution is absolutely critical to try and deter future events, but in a world where a lot of the cyber crime we are talking about is ends with a shotgun approach at the world as a whole rather than specific victims, identifying and prosecuting may be extremely difficult if not impossible.

Far more important to work using some of the ideas that Andrea has mentioned, looking at the fire brigade analogy, but also working with an informal trusted relationships that have been established and ways to mitigate, I'm sorry, firstly, ways to pick up issues as they are developing, and then to start mitigating within the trusted environment those issues and that's where we play the majority of our role. The one thing seen as there are so many governmental or quasigovernmental associations around the world, one thing I would like to add onto what Andrew was saying and it was a comment made at the launch of the impact organisation a number of years ago, that governments in most countries tend to procure a very significant portion of the RCT goods and services within that country.

Why don't you use government procurement as a way to actually drive security initiatives within your country? To actually get people to do proper evaluations on the operating systems, on the applications, on the hardware that you are using, and actually require the vendors who want to sell to government in your country to actually go through some sort of security screening. That way you will know you will at left get a more resilient product or service rather than what you are getting at the moment, which is based possibly on quality, but more than likely just on price.

And we all know the price of trying to fix something after the fact once the attack has happened, once the embarrassment or unfortunately the damage has occurred is far greater than actually paying the cost up front of actually buying the right sort of equipment, the right sort of service that could with stand and could actually possibly with stand the attack without any scarring whatsoever. John, is there anything you want to add?

>> JOHN CRAIN: Hi, I'm John Crain, senior director of security stability and the last part of my title is resiliency, so I agree strongly with what Andrew is saying. One of the things I wanted to say is there is a lot of collaboration going on at this moment in the private sector. We talked about confiker but there are many other trust networks where people deal with not necessarily dealing with prosecution of crime or trying to get people put in prison for the crimes they do, but what we deal with a lot is mitigating and obstructing the criminals, and then what we find is we do want to pass these things off to the criminal system, we find there isn't much of one there. It's not about laws so much in my experience but about a lack of law enforcement personnel who are well trained. If my house gets broken into, there is probably in the city I was born in England a few thousands police officers that could come and do an investigation and understand that, you know, the brick went from one side of the window and not the other, so I was probably doing fraud and I wasn't actually broken into.

If I have a cyber event, there might be only one or two police officers in that area that can actually help me. So what we find a lot, and we have great relations with law enforcement, we see them at ICANN meetings all of the time now, which is fantastic, the police officer on the street who needs to deal with or the police officer on the pipe, I guess, in this case, being that it's the internet, they are not there. So having the laws is great, but we also need the resources to go and prosecute and follow up on criminal investigations.

>> DAVID SATOLA: Great, thank you very much. If I could now turn to Bill Smith from PayPal.

>> WILLIAM SMITH: I guess I'm on now. So I want to thank the organizers of the event, the chair, and actually everyone in the room for being here. I will try and be as brief as I can. Comments I had prepared have already been, many of them have already been spoken, so I will echo some, but try and hit mostly the points that have yet to be made.

One thing I would like to do is defining the problem. It's a useful thing generally. The common definition of cyber security is the protection of data in systems and especially those connected to the internet. That's a, you know, that is my sort of synthesis of a number of definitions and boiling it down, I don't believe we want to discuss cyber war, things like that here. They are critical issues, but we need to focus on things we can deal with.

Rather than offering a different definition, I'm going to suggest that there are five qualities we need to think about, security, which is the degree of protection from danger, loss, damage, and criminal activity. The criminal activity is only one piece of security.

Stability, consistency, the ability to remain, maintain or restore equilibrium, so think of a building, how can it with stand a hurricane? Resilience, so also think of a building in a hurricane, it has to move because if it doesn't, it will break. So you want it to move, but you want it to come back.

So flexibility, the ability to recover from and adjust to environmental changes. Reliability I think is important, the ability to function as expected under real world conditions but also under stress, significant stress, and continuity which the lack of interest interruption and disconnect. One way to be very secure on the internet is disconnect from it is going to be very hard, very difficult for someone to distribute malware to you. It can be done, but it's difficult.

In terms of specifying solutions to this type of problem, we need to consider time. Vint fire brigade or volunteer fire department, they respond quickly. So we need short term solutions and long term as well. So we need to be able to respond not in days or weeks when there is a damage, loss, criminal activity, but in seconds or minutes. And long term is not weeks or month, I would argue, but it's generations.

Thing that's we are putting in place today have to go for decades. And in addition, because they need to go so long, they need to demonstrate qualities that they are designed to support. They have to be resilient. They have to be stable. I think many of the things we currently have are, due display those qualities, but we need to reach out and do some other things.

So as we know, protecting systems requires rapid response, and they are very complex situations. Those responses are difficult enough when the problem is locally contained or regionally contained, but they are magnified dramatically when we cross Sovereign borders. And that's an issue that I believe does need to be addressed. We are seeing more data breaches, spam, phishing, malware especially those crossing international boundaries but we still have the requirement for rapid response if we are going to support the qualities, the five things I mentioned, but at the same time we have to protect individual rights. We shouldn't be so, so concerned about catching the criminal in my mind, and this is where Vint, I think, fire brigade analogy is very effective, but rather minimizing the loss, the damage. That's the first thing that we should do, and if we, if possible, we then need to switch over to, as was mentioned by the gentleman from ICANN, then we switch over to the arson investigation.

But, you know, the thing that we certainly at PayPal are interested in initially, is, okay, how do we prevent phishing attacks, things like that. That's not the only thing we worry about. Now, we have to implement solutions. It's been said, and I actually think it's true that our current policies and systems are really straining to meet the needs that we have. All the incidents that we see are on the rise. They are rising dramatically. I think most everyone in the room would probably be familiar with the network effect, and we are seeing that with cyber security. We have got a network effect.

There are some who point to these failures as indicative of a structural failure with the overall internet governance model and they are calling for change. I think change can be beneficial, but first, let's work within the system that we have before we replace it. Evolution, not revolution.

Cyber security is a 21st century problem. I think we should look for 21st century solutions. We can build on historical models like volunteer fire fighting, but in this case the volunteer firefighters have to be able to cross national boundaries and they have to be able to do so on a moment's notice. And I believe that we have a number of mechanisms in place that do facilitate or enhancing cyber security and fighting cyber crime, but do they really encourage the individuals and the institutions to offer assistance, okay, or are they designed to codify acceptable use and behavior and the formal treaty based enforcement models? I think personally, I'm not speaking for PayPal here, I think we have spent an awful lot of time on the formal treaty based mechanisms and not enough on the ad hoc volunteer fire fighting models. Those actually, if we look at confiker and things like that, are where we have had a lot of success.

So what can you do? Well, you can park in forum like this. You can collaborate with government, business, individual,

okay, a multistakeholder model and advocate, go back into your sphere of influence and advocate that we do things like protect our edge systems, do the simple thing that's we all know we should be doing, and don't compromise. All right? Don't accept compromises in the space.

So in conclusion, I think the internet community has demonstrated an ability to provide a stable, reliable, resilient platform, and it's facilitated advancements far beyond its original design goals. I think that the models that were used to develop it from a technical perspective, openness, individual participation, experimentation, voluntary deployment, I think we can use those as well as we deal with some of the other issues like the legal issues, legal implications, and that if our solutions, if we attempt to find solutions to these internet problems, or problems caused by the internet or issues that are around it and we attempt to do it through mechanisms that are considerably different from the architectural model of the internet, we are destined to fail. Thank you.

>> DAVID SATOLA: Bill, thank you very much. We are now to our last speaker, last but certainly not least, John Morris from the centre of democracy and technology in Washington, D.C. to give a civil society perspective on these issues. John, thank you.

>> JOHN MORRIS: Thanks, David, I will try to run through, very, very, quickly so we have a just a few minutes to talk. I have a few slides but they are not all that critical. My perspective, the civil society perspective is obviously cyber security is a critical, critical problem that we all need to, all need to address, but it is not just a problem of industry and a problem of government. It is a problem of citizens.

And the citizens in crafting problems, we have to be very sensitive to the concerns of citizens. Citizens themselves have cyber security concerns. I mean, they are the victim of phishing attacks, they are the victim of denial service attacks at times where they can't get access to critical banking sites or other sites. I mean, their personal business has moved on line.

So they certainly want cyber security to be solved, but on the other hand, they also are very concerned to protect their own privacy, and to protect their own free speech rights and to protect their own due process rights and so although certainly we very strongly support international cooperation to address cyber security and naturally an essential way to try to address the problem, we can't do it by ignoring either human rights, international human rights or constitutional rights within a national system. So, you know, a couple of things that particularly concern us, you know, government mandates, imposed mandates about cyber security, we think are very, very problematic. Cyber security requires, you know, focused solutions, looking at the actual risk in specific sectors. So, you know, the security requirements that you might impose on a command to control network for a power grid are different than the security requirements that you might impose on a social networking service, and I mean, just because you want to make sure that everyone is authenticated before they access the command and control grid for the power network, you don't need to make sure everyone is authenticated to access social networking. So we shouldn't allow solutions to certain problems to be imposed more broadly than necessary ultimately resulting in harm to individual rights. So design mandates and one size fits all solutions are very problematic. And although we do want government to be involved, we think that private networks really should be primarily responsible as I think most people here have I think most people here have assumed to guard their own networks. Some problems with cyber security network mandates, let me check through a few quickly, they are very bad for innovation.

If you mandate, you know, a set of solutions, people are going to stop looking for other solutions. They are bad for competition. If you mandate a set of solutions that may raise barriers to entry to markets, because only big providers. I mean, Google may be able to follow some mandate to protect its network in a particular way because it can afford to, but an upstart, a new competitor to Google may not initially be able to afford to do that. And also government mandates are bad for security. And the government obviously doesn't have a monopoly on smart people. Private enterprise has lots of smart people and they should be encouraged to look for the solutions. And industry can design their defenses to the specific risks that their specific industries face. And industries can respond more quickly sometimes than governments can to new risks, and ultimately uniform security measures sometimes make attractive targets.

And then, you know, final, kind of concluding thought is, you know, governments need to in any response to cyber security threats they need to make sure that they are complying with their own national laws and with rights of due process, rights of free speech and privacy, you know, cyber security should not be used as a pretext for internet regulation or restrictions that are not necessary for the particular requirement.

There is a case study I was going to talk about that I'm involved in the U.S. in terms of responding to bot nets. I think I will just briefly mention that in looking at what ISP's should do to respond to compromised computers and their network, there are lots of privacy concerns, free speech concerns, privacy concerns with ISP surveillance of users activities, you know, we need to figure out a way to identify bot nets but we need to be sensitive to avoiding undue surveillance and one response to bot nets is to cut off the user and that may be essential in some context, but that raises significant concerns with users getting their internet access cut off. So I mean to the extent that we go to a cyber fire brigade, which I think is a I have intriguing idea that Vint has proposed, I am hopeful that we do it following the model in the United States where a lot of volunteer fire departments are run by citizens and are at least supervised by citizens, and that may not work for cyber security to have local citizen fire brigades, but I certainly hope that we have citizen oversight to any fire brigades that we organize. Thanks.

>> DAVID SATOLA: John Morris, short but sweet. Thank you very much. You have brought us back on time, at least for the presentation part of the session. I think we should, if the panel is willing to stay in the room for a few minutes to take questions, I will set a limit of 10 minutes for questions because we do need to make space for the other panel coming in following this. I would also like to say in response to a few questions that have been posed while the programme has been proceeding that we will be posting our background paper and the presentations made here to the we will have a URL in our workshop report, and that will be posted to the IGF web site.
So I would take questions from the floor, and if you could briefly introduce yourself and if you have a question to a particular person, please direct it to that person. So I will start with the gentleman here.

>> Hello, my name is Vito, I for the Ministry of Defense before everybody starts saying here is the defense guy, here is security and defense, I worked for five years at the ministry of informatics. I was involved in information and society programs so I know about freedom of expression and freedom of the internet. I can appreciate that. The internet has become a very dangerous place. I take issue with some of the comments made about cyber warfare, cyber attack, it's not a good term to use, not constructive.
Well, look what happens in Estonia in 2007, look what happened in Georgia, there you had a military attack coincided with a cyber area tack. How does one address that in this world? Cyber attack is too much of an attractive tool for governments that want to reach a foreign policy objective or a military objective to support a military objective as we saw in Georgia where even diesel generator companies were blocked when people needed portable power.
It's too attractive, the non attribution part of it is the most attractive. I also take issue with Mr. Cerf of Google, I beg to differ with such a large organisation that bot nets can be targeted. You can rent a bot net for 100 Euros a day to target whoever you want you can go into Facebook or some sort of social network and raise yourself as cyber Army, offer to unload software and do your fighting or protest for you. So we are not in a time where Lithuania for, example in the old days you can use the door unlocked.

>> Those times have changed. We live in cities. If we think of a city where we have a street system, the grids, highway system, compare that as an analogy trying to work in the fire brigade, that's a good idea, but to a highway system, what do we have today? We have traffic lights. We have state police patrolling, we have rules and regulations. If we have that analogy to the internet today, nobody would have been able to come to this meeting because everybody would be doing what they want to do on the streets. There are no traffic lights, there are no rules, there are no regulations. So in closing, a very good idea fire brigade. NATO has offered to its member states MOU with the cyber defense management authority for sending rapid reaction brigades to a member state, Lithuania is one of the four or five member states that have signed this, so that idea as a model may be worth looking at. But in addition to the confiker work group, there should be a work group to study what happened in Estonia and what happened in Georgia. I think there are many varied lessons to be learned.
Thank you.

>> DAVID SATOLA: Thank you very much. Responses from the panel?

>> Thank you, I would like to respond as briefly as I can. I don't disagree with you that there are abuses that take the internet into national or international conflict, and your example of Estonia is a good one. My concern was not to treat all

such things in that way. And so suggest other constructive methods for response. So we are not really in great disagreement.

There are already proposals that you have heard about for international agreements with regard to abusive use of the internet for national purposes. So I don't think you and I are in disagreement. I think we need to approach this on multiple fronts at the same time.

>> DAVID SATOLA: Alejandro.

>> I would like to thank you for putting together a good panel and the breadth of subjects is very impressive. I would like to make a comment and ask panelists for reaction. In the IGF book that has been distributed with your registration, I'm sorry, I am Alejandro Pisante. I am Twittering out live for this session. In my contribution to the book it's a short chapter, when studying the past sessions of the IGF related to security issues, I found that there is a huge time there is not a total disconnect but a huge time lag between what's discussed in the internet community, what's discussed by operators of networks or petitioners of security or the national CERTs, and what is discussed in the IGF, and then there is a further time lag which can be studied from the first sessions of the IGF to how these discussions feedback into the other communities, whether it be government communities, parliaments, enacting laws and so forth or the technical community.

I am very much inclined to revise that figure. The time lag I wrote down is about two years. But hearing, for example, Andrew McLaughlin who is a knowledgeable person in this field speaking about abandoning the perimeter defense paradigm and seeing that it appears to be new to some participants tells you that this is about a seven year time lag. That paradigm was abandoned and replaced by that defense in depth concept seven to ten years ago in that community. If governments or companies or civil society organizations are discovering this at this stage, we have to move forward with a framing of the subject real fast, and I would ask for responses from the panelists to this view and to the view that the concepts have become very fuzzy as the session went along. We don't know if we are speaking of cyber security as individuals, individuals security, whether these are lumped under, grouped together as public security issues which are issues for the police, or whether we are looking at attacks to national assets and we are beginning to look at national security, whether you call it cyber war, I agree that cyber war is a very bad framing. Attacks to national assets because they are defined as a countries or government's assets that's well defined independent of who is responsible. So I would like to know responses here.

>> DAVID SATOLA: I think we should allow Andrew response to the seven year time lag.

>> ANDREW McLAUGHLIN: Alex is totally right. Maybe even a little more complicated than that which, I don't know anybody in governmental circles who would advocate a perimeter defense model. The problem is that the technologies that they are deploying are that. So it's a funny thing, like maybe there is one more step here, which is that the rhetoric has to infect the discussion virally and then there is a lag time between the actual implementation.

I think that, you know, the rhetoric of resilience is now so ubiquitous as to be kind of a cliché, but the actual steps people are taking are not in fact resilience oriented steps people are looking for intermediaries to take the burden off of end users, regimes to standardize or mandate particular security solutions. These are not consistent with the concept of resilience. They are still the things that are dominating policy discussions.

>> DAVID SATOLA: Erick, very quickly and then we have one last question quickly.

>> ERICK IRIARTE: I only want to add that when we talking about security, it's not only about preying enemies, sometimes a could be a problem for security. For that the organisation of with ISOC work together in development capacities through the attack response programme course. In the past three years, John Crain here is the leader of that group, the ccTLD's around the world are preparing for those activities. The security is very useful in a community in case of earthquake in Chile and Haiti was the first point to start against that kind of problem so the security is also again not against somebody.

>> DAVID SATOLA: Excellent point, thank you.

>> My name is Steve Ryan I'm the general counsel of the American registry of internet numbers one of the IRR's, and I want to say there is a critical interface between law enforcement and non governmental organizations that has developed very satisfactorily over the last several years, so, for example, in our region, we interact directly with the 21 sovereign nations, law enforcement agencies, so the Royal Canadian Mounted Police, and our organisation have a liaison where the non governmental organisation that keeps the who is database for our region we provide the authentication in criminal courts for them to identify criminal activity, and then when law enforcement identifies for us information, we can act not in an improper way, but in a proper way to under our own authority to revoke internet protocol numbers if, for example, the person has lied to us, committed fraud in the application procedure which is something we have authority over. So that cooperation is occurring on each continent right now, with each of the RIR's, want I want to talk about that because we didn't talk about the cooperation of NGO's and states which I think is developing attractively in part through this multistakeholder approach.

>> DAVID SATOLA: With that, we will conclude. I would like to thank our panel very much, and the audience, especially those who were standing the whole time for their perseverance and patience. Thank you all again and look for our documents at the IGF web site.
((Applause

* * * * * * * *