BEIJING – GAC Meeting with Law Enforcement RAA
Sunday, April 07, 2013 – 17:00 to 18:00
ICANN – Beijing, People's Republic of China

CHAIR DRYDEN: Hello again, everyone. If you could take your seats, please, we are ready to begin.

Okay. Let's begin, please.

So our next session is regarding the revisions to the Registrar Accreditation Agreement here at ICANN for application in the generic top-level domain space. And GAC members might recall that there have been a couple of sets of recent revisions posted to the agreement, but I think we may all be struggling a bit to be tracking all the different revisions, and as well as other postings that have been made about other aspects of the gTLD program.

So the good news is that law enforcement has been paying a lot of attention to what's been happening with the negotiations that have led up to these posted revisions and so have come today to present to the GAC about what they have found and to share some views on that with us as government colleagues here in the GAC.

So what I will do next is I will turn over to Troels Oerting from Europol who will lead us into the discussion. And I understand there are a number of law enforcement colleagues here with us, including Bobby Flaim from the FBI to his right and they may want to contribute as well

to our discussions. And I suspect the GAC may have some questions and comments as well once we hear from law enforcement.

So with that, I will hand over to you, please.

TROELS OERTING: Thank you very much, Heather, for this warm welcome. And thank you also to the GAC for inviting law enforcement to this important session.

My name is Troels Oerting. As Heather said, I am the newly appointed chair, head, of the European Cybercrime Centre which covers the European Union's 27 countries which is an area that covers 500 million people without borders and 2.9 million law enforcement agents.

And we have cooperated together with the U.S., together with Australia, Canada, G8 and support other ones to examine what the development in the new gTLD changes will actually imply for policing. And I have also, probably not a surprise for you, when we go online, so do the criminals, unfortunately. And we have already seen, actually, to a greater magnitude than I thought was possible how flexible organized crime already adapts to squeezing out money from crime which is based on the Internet. And it is not just child sexual abuse I am talking about. It's actually gangs who steals our information, who steals our money, who steals our identity and who does a lot of atrocities on the Internet.

I also have to inform you that the classical way of policing will have an end when we are fighting crimes on the Internet, because when we have been fighting crime and organized crime, we have done this for a living for so many years, we've had the normal ways of fighting. We have our borders, we have the way to control crime, we have a lot of

technical evidences. But for the first time, police will be forced with crime that we cannot stop in the classical way. We cannot just send out the police to stop the crime because the crime will actually reach us from far beyond our own countries.

And the perpetrators will not be in reach first, and the perpetrators ability to reach a number of countries at the same time is very, very high.

So we cannot just take us out of it. We cannot just do awareness. We also have to make it unattractive to be a criminal at the Internet. And right now it's actually, I have to say, a free ride.

And it will increase. The crime will increase. When we get more and more penetrated, the Internet will reach regions like Africa, Asia, South America. It will also statistically give us more crime. And the police cannot do as we have always done and just shut down the borders because there will be no traveling. No criminals need to travel because they can actually effect the crime from where they are.

So based on this introduction, I'm very, very happy now to bring you through what has been the history of the new RAA recommendation from law enforcement, and it started as long back as 2009. And I don't know who is actually pushing the button here for the presentation, but here, just to refresh your memory, you can see what has happened step by step, year by year.

So now in 2013, we are at the end of the road, hopefully, after three years of intensive work with you. And thank you very much for this. I hope that we can now conclude something and you can, on the behalf

of the law enforcement community, in order to secure the fundamental rights of the citizen to also operate without being victim of crime at the Internet. You can help us introducing some of the law enforcement recommendations.

So the recommendations goal was to create prevention and attribution. And how? Through due diligence, registrars and registrants; transparency and ability, clear and attributable responsibilities and duties; and a functionable WHOIS.

Next slide, please.

Here you see clear improvements in the new agreement. Abuse points of contact, data retention specification in compliance, which is important also for us with privacy and national rules; specification of privacy and proxy registrations and accreditations, and registrar information specifications. Very, very good improvement. These are really important steps in the right directions.

Unfortunately, it's not complete, in our view, the agreement as it stands, and we would very much like you to consider to actually include some improvements that we have identified.

And the first one is the validation/verification. We simply think that we need a bit more in this area. And we have created a letter from us to the GAC which is addressed to the ICANN Board and which, in more specific terms, we try to identify exactly what we mean.

But we need, actually, a bit more than just to be verified in addition to a phone or e-mail. We need a bit more verification.

It's very, very important for us that we are able to identify perpetrators, we are able to identify the originators, and it is just not enough that you put in an e-mail or phone.

And we also need to have affirmative re-verification. Can't just verify and then you forget about it. There has to be a re-verification process also in order that we make sure that they live up to the standard that we actually acquire.

There was another slide on the second page that we also need, and I think this is very, very important to have a very affirmative and detailed language.

We don't want to have a language which is up to interpretation. It should be clear, straightforward what we mean, and what actually are the conditions in this country that the registrars will sign with ICANN.

So it should be clear and unambiguous language is needed and there needs to be a contractual compliance also, which is in the RAA Section 3.7.7/8.

Now, if I may be so frank and blunt to ask you to continue a few things, to consider them, this is what you should consider. That the new RAA agreement needs to be signed before you launch the gTLD and they go live. It's very, very important that we first have the governance in place, and not afterwards.

So at least if it cannot be before, it should be linked. This is really a recommendation that we urge you to bring forward to the Board. This is very, very important.

Then we also want to -- you to support ICANN's registry amendment requiring that registrars sign the new RAA before they can use them. It's a very, very good amendment. It's already in place, so we don't need to invent or reinvent something. We just need you to support this.

And then, last but not least, that you support the four verification improvements that we have stipulated in the letter and which was also in the previous slide.

It's not a big deal. It's not a big work. Of course there is work, but you cannot just give away, you know, the right to do something without preconditions about that we can find, trace back who is actually responsible for this. So there needs to be a verification process in order that gives a clear indication who it is.

And if we get this, if you support us in this, I think that we also are able to do our job. I don't think we are at the end of the road because the dynamic dimension of the Internet will require that we are always on top of the development here, but this will at least give the law enforcement on the globe -- Russia, China, U.S., European Union, Africa -- tools that they can do their job to prevent all of us being victims of crime and to enjoy the very, very good, positive sides of the Internet, because we will be online all the time in a couple of years from now, and we will go mobile, and we will be census, and we will need also to protect all of us from these criminal organizations who already now are actually taking advantage of the Internet.

Let me give you one example from moneywise. The European Union is losing 106 billion Euros every year in VAT fraud. 60%, 65% can be attributed to organized crime. And this is all done by a computer.

We have in the European Union a loss of 1.6 billion euros in payment card fraud or card not present online. This can be attributed purely to this crime. And now we will skip the credit card system and all payments will be done by mobile devices or by alternative systems using the Internet. We need to be prepared for this. Otherwise, I fear that we end up in a situation that somebody will then require more initiatives to be taken, which might not be in the interest of all of us as citizens in this global village.

Thank you very much for your attention so far, and of course we are open for any questions you might have. And I've been reinforced by a real techie here who knows all the details. So if you have any technical questions, we are fully prepared to answer this.

We are also backed up by U.K. and other ones. So I think we should be prepared.

But what I hope is this was at least, for you, clear and easy and understandable, and a minimalistic approach from law enforcement. We are in the actually asking for that much. It's just a small tweak of the already agreed and adjusted agreement. Just small, small tweaks. Please, on behalf of us bring this forward to the ICANN Board so we can do our jobs.

Thank you very much.

CHAIR DRYDEN: Thank you very much for the presentation.

I see Lebanon.

LEBANON: Thanks. This question is for Heather.

Do we have copies of those letters?

CHAIR DRYDEN: Not at this point, but it will be circulated to us, yes. So it will be circulated.

LEBANON: I mean, it would be tough to make a decision on something, at least during this period, if we haven't seen them, and there are only four more days and we have to go into some of these situations and check with our administrations. So I'm just wondering about the timing.

CHAIR DRYDEN: Thank you for that. I think it's within this longer-term context where these issues have been ongoing and under discussion for some time. So there is some background to the issue. So I expect that will help us once we receive the letter and are able to view the slides as well outlining the specific request coming from law enforcement.

Please.

LEBANON: So I just have misunderstood what we were asked. I thought we were asked to try to consider this before any new gTLDs are issued, or link them. And in that sense, to me this and the new gTLDs are going to be decided based on whatever the outcome of these meetings are. That's why I'm asking the question.

CHAIR DRYDEN: I think there is a timing issue, yes. You're right.

So we have Uganda, then Italy.

UGANDA: Thank you, Chair. and I thank the presenters.

In the introduction you acknowledged that the way crime is being committed now is -- goes beyond borders. And in Uganda we recently passed cyber laws, and only two cases have been tried basing on those laws, and the culprits are not Ugandans but they are from two European countries who actually physically come to Uganda and they commit offenses from there, cyber-related offenses.

So in network globally of capacity building -- of course we are members of INTERPOL. Do you have an arrangement of building capacities within other countries where nationals from -- nationals (indiscernible) domiciled there, they come there, they commit crimes of -- crimes, but not originating from that country.

So do you have a mechanism in place?

Thank you.

CHAIR DRYDEN: Thank you for that.

So next I have Italy.

ITALY: Okay. Thank you, Chair.

My question is concerning the relation of the resellers with the registrars. You used an expression that this relation should not be regulated in a too vague way. So are you -- and I -- Are you proposing or you had already in these discussions with ICANN a more precise idea how to solve this problem? Because of course we know that resellers are numerous and then this create, certainly, a possible way of not respecting so much the registrar's agreement.

CHAIR DRYDEN: Thank you. I think this issue of resellers is probably a quite important one. It's come up previously in discussions in the GAC.

Is this something you would like to respond to?

Thank you.

BOBBY FLAIM: Well, yes. It was something that we wanted to make sure that anyone who registers a domain name is in the full chain of custody. And there had seemed to be a question before with the RAA that resellers or third-

party individuals who were selling domain names were not part or were not captured in the RAA.

So now they are, but one of the things insofar as deficiencies really just concerned language.

We just wanted to make sure that language was more affirmative so that it was very clear and that anyone who reads the contract could instantly tell that everyone is covered.

CHAIR DRYDEN: Thank you. Next I have Australia, then the EU Commission.

AUSTRALIA: Thank you very much for that very clear presentation and update on development in the RAA and what's obviously a very busy time for all of us. This is, obviously, an issue that's been going on for some time and of great interest to GAC for some time and is part of a cluster of broader work including the implementation of the WHOIS review team's recommendations. We have the new expert working group on what I believe is being called gTLD directory services and so on, which I think it's useful to track them all in parallel and to understand how they're all progressing and how all the pieces fit together.

In terms of the timing and the provision of potentially any new GAC advice on this, I think it's useful to recall that the GAC has provided significant amount of advice on some of these areas in the past.

So, to be very clear, you know, we've -- the GAC has previously said that the RAA needs to be finalized before any new gTLDs are delegated.

There's standing GAC advice. We've also advised the board that contracts need to be clear and unambiguous. We -- the WHOIS review team's recommendations also go to a number of the matters which you've mentioned, and the GAC has endorsed those recommendations. So, in terms of resellers, the WHOIS review team was very clear in recommending that there should be a clear and unambiguous contractual chain going all the way from the registry operator to the registrant so that the obligations are very clear where they're passed on and who they apply to. So it may be that there are some new elements, but I think that there is also -- it's also useful to recall that the GAC has already provided advice on all these matters. It's standing GAC advice, essentially.

CHAIR DRYDEN: Thank you, Australia. EU Commission.

EUROPEAN COMMISSION: Thank you very much, Chair. And thank you very much, Troels, for this very interesting presentation. I think we learned a lot, all of us. Just as a point of information, I think it's important to keep in mind that the European registrars already have to go through quite tough verifications. So that is already in place as far as we are concerned. And I also want to underline how important we think it is with legal certainty. So that point is very well taken.

Now, for your three asks, we will need to think about this, of course. And, as you know, negotiations are ongoing. So we will accelerate that to thinking work. Thank you.

CHAIR DRYDEN: Thank you. Lebanon.

LEBANON: Thanks, Australia, for the explanation. But I have a question. For countries like Lebanon, if they wanted access to this data, how do they get it? Once it's implemented, I don't see any reason why Lebanon would object to it. But if the Lebanese authority -- Lebanese law enforcement people want to get access to this data, how do they get it, in case they need it for law enforcement purposes?

BOBBY FLAIM: I'm sorry. Access to which data?

LEBANON: Eventually, you're getting the registrars and registrant to provide data. This data is kept on record somewhere. So, in case you're trailing somebody and you're trying to track somebody, how do -- how is this data made available to people -- to law enforcement people who need to use it?

BOBBY FLAIM: I'll just go by what we do in the United States. If this was certain information they had collected, there's two ways. If it's private information, you would need legal process. You know, if we're talking credit card information, you know, stuff that's not on the Internet. And the WHOIS, that's the publicly available database which would be

available to anyone. So those would be the two pieces of information that we, as law enforcement, would need during investigations. So the first one would be subpoena, legal court order from judge, magistrate. And then the second one is open and publicly accessible.

LEBANON: And that would apply to entities outside your jurisdiction?

BOBBY FLAIM: Yes. It would be dependent upon the laws and processes of the individual country. So, in other words, if you had a registrant in Lebanon that had this information, it would depend on Lebanese law on exactly how the law enforcement would get that information.

LEBANON: If I have somebody in a European country who has done something and I'm following this issue in Lebanon, how would I go about --

BOBBY FLAIM: Yes. That issue becomes more difficult just because of legal processes throughout the world. A lot of countries have signed on to the mutual legal assistance treaty which is where your relative Department of Justice -- say, if it's going from Lebanon to the United States, the Lebanese police would go to their Department of Justice. And then through the legal treaty, they would request the American Department of Justice to go down to the appropriate American jurisdiction.

Unfortunately, to be very honest with you, it's a slow process. That's why we have always argued insofar as the WHOIS to keep it public and accurate so we would not have to seek legal process, because digital evidence disappears very quickly. So that's why the importance of having verified, correct information is all the more important so that we wouldn't delay important investigations.

CHAIR DRYDEN: Thank you. I have Australia again.

AUSTRALIA: Thank you. I just have a question. And I've asked it in a number of previous meetings, and I don't believe we've still received an answer from the board. So I'm wondering if perhaps one of you can illuminate for me where we're at in part 2 of the law enforcement recommendations, the due diligence once. Is there any update?

BOBBY FLAIM: No. Unfortunately, there's no update. Part 2 of the recommendations, just to give you a brief refresher, addressed more of ICANN so that ICANN would do due diligence when they accredited registrars to ensure that they were financially sound, they were incorporated, so on and so forth.

Some of the other recommendations in part 2 were that ICANN would produce an audit report on, you know, complaints that had come in based on, you know, registries, registrars. ICANN did pass or did implement the due diligence on accrediting registrars. So, in other

words, in July of 2011, I believe, they did implement a system where they would do due diligence when they accredited a registrar, meaning they would look into their financial records, incorporation records, so on and so forth. The other three, B, C, and D, we've never heard, unfortunately, anything from ICANN. And we still don't know. I know you, Peter from Australia, have asked that specifically to the board. But we have never gotten any answer.

The other thing, insofar as the due diligence, we haven't heard how that has -- the results of that, in other words, if that has been a successful program, if it has gone well, and exactly what they do for due diligence.

CHAIR DRYDEN: Thank you for that. Next I have Singapore and then the United States.

SINGAPORE: Thank you, Chair. And thank you, team, for the great work you've done and we fully support your effort. I have a question. I think the RAA focused on the compliance by the registrant. We just wonder, in the event where the registrar did not take quick actions, we know that enforcement time is of essence. So, in the event the registrar did not take quick actions, can the registrar intervene to do the enforcement action? Is the language -- we do not know whether in the RAA agreement whether there is a provision that to make it very water tight that, in the event the registrar failed to take quick action, the registry can come in to suspend the name. Is there such a provision in the RAA agreement, or will there be legal complication that registrar will find

that their hands are tied because agreement is entered into by the registrant and registrar and not with the registry? Thank you.

CHAIR DRYDEN: Thank you. Would you like to respond? I can continue through the speaking order, if you like.

BOBBY FLAIM: I'll try to address it. I guess the registrar -- and the language is a little complicated. But what we've tried to do is kind of, with the clarification of some of the language which we referred to in the slides, was ensure that there were set time limits and time specifications on how people would have to act so that you wouldn't get into a point where it was, like, well, we don't know. It's says "timely," but what exactly does "timely" mean? Or it says "reasonable," but we don't know what "reasonable" means. We may have an idea, but it's not very specific.

So with registrars, if they wanted to act as fast as they wanted to, they can because it's the terms of their agreement that they have with the registrant. So they can act as fast as they want.

Now, with this registrar accreditation agreement, I guess some of the requirements that they would be required to do would have certain time limits insofar as, you know, if they saw WHOIS that was incorrect, you know, they would have a certain amount of time to correct that information. But, technically, the way I understand it -- and I could be wrong. But the way I understand it, if they wanted to take down the domain name as fast as they want, they could. Because, if there's a

violation of the terms of their agreement, then they are legally entitled to do that. So does that answer your question, sir?

SINGAPORE: Sorry. My question is can the -- is the registry operator empowered to suspend a domain name in the event the registrar did not take remedial action or did not take action quick enough as required? Thank you.

BOBBY FLAIM: Yes. I'm sorry. Yes. They do that quite often. Yes.

CHAIR DRYDEN: Thank you. I have United States, then U.K.

UNITED STATES OF AMERICA: Thank you, Madam Chair. And thank you, gentlemen, both of you, for bringing us up to date with your perspectives.

For my colleague from Lebanon, if -- so you don't wish to wait, if you want to look at a version of the text that Troels is talking about, I did circulate a U.S. government position on the RAA on March 29th. And it might be a faster search for you to find that. And I would be extremely surprised if our position was somehow any different from the rest of the law enforcement group. So, provided the GAC has sufficient time later in the week, which we know is a challenge, we might want to consider how we signal to the board at least an overarching sort of advice that would urge them to demonstrate a commitment to ensure that the documents would be amended as we have proposed and be required

before the new gTLD -- obviously, before the process gets officially launched with delegations. So I do think the GAC might want to consider language for the communique that kind of reinforces the importance we attach to achieving these objectives at this moment in time. So that, even if we're not agreeing to proposed edits before the end of this meeting -- because I know that might be a challenge for us -- we could agree to language for the communique. Thank you.

CHAIR DRYDEN: Thank you, U.S. And it does seem that we have GAC advice already. So I think in referencing that, that will assist us. And we do have our exchange with the board on Tuesday. So this seems like a likely topic for that. And we will have a preparatory session for that exchange. So that's an opportunity for the GAC to discuss it a bit further before we meet with the board. Okay. United Kingdom, please.

UNITED KINGDOM: Yes. Thank you, Chair. And thanks to Troels and Bobby for the update.

I just wanted to follow up the question from Uganda about capacity building and addressing the problem that they and many other countries have experienced where national audits in another country have been pursuing cyber-criminal activities in their country. And maybe something you might be taking away as a critical issue. It's certainly -- I mean, there are a number of capacity building projects well under way, as you both well know. The U.K. has been contributing directly to this issue. We've also been funding and active in the commonwealth cybercrime initiative where ICANN is a partner along

with U.N. Office of Drugs and Crime and Council of Europe, ITU, and many others. And that is well under way, that initiative. And we're going to have an update on it, actually, in a commonwealth GAC session, which is an open session. So, if anybody here who is not in the GAC wants to get an update on the commonwealth activities in addressing cybercrime, please come along. It's at 12:30 on Tuesday in this room.

There were a number of initiatives going on in capacity building and tackling cybercrime. And ICANN is involved. But I just wanted to sort of underline it's a very important question that Uganda has raised. Thank you.

CHAIR DRYDEN: Thank you, U.K. Okay. At the end of the table, it's a bit hard to see. Chile. Great. Please.

CHILE: Thank you, Heather. Good afternoon. Chile attaches great importance to the work that has been undertaken in this field of action. And I have, along with supporting the words spoken by the U.S. with regards to incorporating as firm and proactive language as possible for this work to be followed through more aggressively, more interactive, more cooperatively, I have two questions.

The first one: Are we anticipating on time the challenges which are being posed in this field of action? Or are we more reactive in this point of time in terms of how we are operating both individually and collectively? That's number one.

And what would be needed for more compelling action? What are the hindrances that are being faced today in the world community that we are not more proactive in something -- in an area of global interaction of trade, movement of people. I was just reading in PBC that the future of warfare will all be done cyberly. It won't be done with ships or airplanes.

So what are your thoughts about how more can we support more aggressively the challenges which you are facing today? Thank you.

CHAIR DRYDEN: Thank you for the question, Chile. Would you like to respond?

TROELS ORTING: Thank you very much, Chile. The wishes from our side are not so much focused on warfare and state-sponsored things. We're fighting crime, ordinary crime in all countries. We are all affected. It doesn't matter where we are. We are all victims of this crime.

I think you're right in the way that we interact. If we do this in the right way, if we actually keep each other up to date. How do you keep yourself up to date? What is going on in your country?

And I think that in the European Union at least would like now to engage much more with the European Union GACs to invite them to EC3 to tell them what's going on so that you can make up your mind and see in reality and not just the buzz words or the newspaper stories but really the cases what is going on. And we also make scenario building. We're trying to see -- you can not see very far in this area, because it

changes so quickly. But we might be able to see two or three years ahead. And we do this together with industry so we can see where do they see the money? What are they trying to develop? And, together with academia, what will be the down side of this? And how do we need to be prepared either with better laws, education, capacity building, which is very, very important, not just for law enforcement but also for judges and prosecutors inside the EU and outside the EU. This is a global thing that we need to do together. This is not something that we can leave -- I agree with the U.K. and Uganda. This is very, very important. I'm also happy to announce that we've been asked by the European Commission to create a list of all the countries where we find is the most important and priority role so that we can use the scarce money in the best possible way. And then we'll, of course, coordinate this with the U.K. so we don't make double efforts in one country. But, if the EU pays here, then the U.K. can take another name, another country on the list. And I think this way we should do it. We need to coordinate this, because we don't have all the trainers and we don't have all the money. And we will not just do this as the European Union because this is not regional crime. This is a global phenomenon. So we have to interact with INTERPOL. And I can also assure you that there's no turf wars between Europe and INTERPOL. There's so much crime there's enough for everybody. So we need, actually, to see if we can in a coherent way build up capacity in order to use all that we have in order to make this new and very, very -- I think very great tool, the Internet, to be also a safe place and not just a secure -- and not just an undersecure place as it is right now. Thank you.

CHAIR DRYDEN: Thank you. Are there any other requests to speak? That seems like a good place to conclude, I think.

And for the GAC, as I mentioned, we have an opportunity to raise this with the board and perhaps to contemplate reinforcing the advice we've already given. And also there's been a comment submitted by the U.S. to the GAC list. So perhaps we can recirculate those or provide those for us to look at as part of our busy agenda this week.

So many thanks to law enforcement and to Troels and Bobby for coming to give us an update regarding the RAA and the process currently under way.

And for the GAC, this concludes our meetings for today. So we reconvene on Tuesday morning. And please don't forget that there's a cross constituency breakfast that we've been invited to on Tuesday morning. So we'll send a reminder to the GAC list about that.

So have a good evening, everyone. And please keep working on your GAC advice drafting and your consulting. Okay?

You're not off the hook. All right. Good night, everyone. Thanks.

[End of Session]