GNSO – ICANN Nairobi Meeting
Forum on DNS Abuse
11 March 2010 at 16:00 local time

Note: The following is the output of transcribing at the Forum on DNS Abuse held in Nairobi on Thursday 11 March at 16:00 Local time. Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record.

Coordinator: Please go ahead.

Margie Milam: Hello everyone, we're going to start now with the forum on DNS abuse and I'd like to introduce our moderator Alice Munyua from the Communications Commissions at Kenya and I'm going to turn it over to her.

Alice Munyua: Thank you very much. I'm with the communications commission of Kenya and also with the KENIC, Kenya's ccTLD manager and I would like to welcome you all to this session that's going to be dealing with DNS, domain name system abuse.

As a way of introduction, just to note that our region, Kenya especially we have two fiber optic cables landed sometime last year towards the end of last year which means for us there's a certain level of increased access demand and by extension increased access to the internet.

And with this there's a lot of opportunities that are going to be provided for but also there are many opportunities as well for cyber crime, exposure to cyber crime in the region, not just in Kenya but to other east African countries that are being served by this fiber optic cable.

And in that way Kenya has begun to prepare itself for this and one of the ways we have prepared ourselves is from a legal perspective where we have

the Kenya Communications Amendment Act that has taken recognition of our dot KE end position to facilitate security and stability of our ccTLD as well as the establishment of certification authority for digital signatures.

We also are currently deploying new internet technologies, DNSSEC is one of the examples as well as ITD6. Through the Ministry of Information and Communication the ITD6 initiative as well as DNSSEC at the dot KE ccTLD registry.

Others, the establishment of the east African cyber security task force and Kenya is currently heading that working group, that is looking specifically at the establishment of national CERTs and regional CERTs.

So quite a number of effort going at both the national and regional level and we are going to be hearing some of them from the four panelists, we've asked for this session.

And the first speaker is going to be McTim, consultant on African internet infrastructure and internet governance issues. And then we'll hear from Nii Quanor, a former ICANN board member and then Muriuki Mureithi who is the Kenya ICT action network and last Yurie Ito who assisted Kenya and KENIC with the capacity building workshop on cyber security.

So I'll hand over the mic to the first speaker, McTim.

McTim: Hello everyone. I was asked to do this presentation about three days ago, and I thought oh, DNS abuse from a Kenya perspective, that should be a pretty short presentation.

And it turns out it is, I had no evidence, no data of my own. I haven't read a DNS server in east Africa in two years. So I did a survey, I asked around operators, ccTLDs, half a dozen of them, root server operators.

And basically I found out that my theory was pretty correct, we don't really have much DNS abuse. Do I have slides? Oh right, good, there we go.

So my favorite quote came from dot co.za, yeah, we have some but it's under the radar, which is sort of the consensus. In fact I just got a mail, a very short mail I want to read you from AfriNIC and they said, the guys don't really have anything useful, sorry.

As in nothing, nothing that operators have on record, nothing that their monitoring tools have picked up and that's not uncommon. We didn't really ever see a directed attack in the DNS either to our infrastructure or to the several routes or gTLDs that are hosted in the ZA, and when we had the great attack on the roots circa '07 there was barely a blip on any cat copies in ZA.

So that's sort of cements my thinking that it's not really an issue here. And then the last slide we'll get to maybe why and pick it over to the Masai here who will talk more about that.

As Alice said we've got DNSSEC planning, sorry, but no actual deployments yet and as we'll see later, DNSSEC is not going to protect us against the kind of cyber crime that we're experiencing.

Which mostly out of band attacks, so this is one of my carriers, the regional carrier, the only regional carrier sent me a snippet from his name server log and this is basically what everybody sees.

Occasional port scans, automated querying mostly from Eastern Europe and former Soviet states and China. Next, so what we have is out of band attacks. I mean last year we had four African ccTLDs targeted.

You may have heard about it, the headline in the media was Google hacked in Uganda. Well it was really a log in attack against the registry interface and they were able to change some records.

They were SQL injection in fact, so in Kenya and Zambia we see brute force password attacks against the registry into the - but again the DNS curve and DNSSEC and I'm not going to get into that, we have this holy war going on in the DNS ops list.

I'm not going to get into that but neither of them will prevent this kind of out of band attack. Next slide, yeah. So the rear servers said we're all localized in the region.

But that's (aft) who said we're really happy and it's working well in serving the Kenyan community very well, it's just a few hundred meters away here.

And they block traffic and they rate limit traffic in the dot KE registry rate limits, ten queries from a certain IP address.

But they don't see any packet floods here at the F node in Nairobi. What's interesting, and they don't see any in Johannesburg either, it's the same traffic pattern as globally.

We can have the next slide, what I found interesting about this courtesy of JoWow, you see we have (kicksbee) on the bottom, sort of 50 packets per second kind of thing and then Johannesburg the traffic is double.

But what's interest is as JoWow pointed out in Johannesburg in the top you have to look at a sine wave, or sort of here in (kicksbee), we have a sine wave and it's more abrupt, it's more a K wave at the top.

And I think this may be a cultural thing, people getting to work precisely on time and here maybe we have traffic jams or something.

But they are not reporting any specific DNS attacks or abuse from F root server. Next slide is K and I took this off the K Website. I did reach the K root operators.

And they said the same thing, sorry McTim, we've got nothing for you, because it's a local node. If you - this is very difficult to see, at the very top you see a purple line and under that there is an almost imperceptible yellow line.

That is the traffic at (Tix) in Arusha and I think it servers Dar Es Salaam as well but again they are not receiving any noticeable DNS events.

Next slide please, anyway so we do have cyber crime, most people access the internet via cyber cafes, internet cafes. And they run XP and it's in quotes because it's you know not paid for XP, not pirated XP.

So there are unpatched versions of XP and other security holes. You get people bringing their USB sticks, where's mine, and those things were the first vector in east Africa for malware.

But we did have some cafes that were hit fairly hard by cotton picker, but it's mostly banks here in east Africa and other financial services, organizations that are targets of cyber crime.

And on the right you see a quote from the local civil society, ICT list, I kicked in that list that Alice is part of from someone who is listening in this room to someone boast about the east African cyber security task force.

Well they were just describing it, they weren't boasting. And at the same time on that list we were talking about the birth certificate Website being flagged by Firefox as a malware site.

So it does happen but it's not DNS in band. Next, so mitigation, as Alice said Kenya's looking at DNS sec and others are as well, but as in the rest of the world, very little business case for it.

It's something that's useful but it will be difficult for us to get African name server operators to actually deploy it.

And we've got CERTs and C CERTs being created and in the last year, there's been a real ground swell of support for that. Team (Saru) has really done a lot of work in the last year and gotten a lot of people excited about it.

The main mitigation and the Masai can speak to this more is that we have ongoing trainings for over a decade by the African network operators group, AfriNIC does trainings.

ISOC does training, we have a Kenyan, (Michuki), who most of you know who's doing a good deal of training around Africa and globally in this regard.

And of course NSRC contributes to these trainings as well. So we're always doing capacity training but it's just a (fee in tac), we're always going to be rolling the boulder up the hill.

And of course we have this east African cyber security task force which I know nothing about, but I do know that the awareness is increasing. And it is a concern, especially in corporates security.

They're starting to spend money on security. I think that's my last slide. No, this is my last slide, so I started asking Kenyans and Ugandans and Tanzanians and other people a series of questions and I'm not going to read them because I hate when people just read their slides.

But I think all of them are fairly valid, all of them have a part in terms of the DNS abuse. We don't do that much monitoring, security doesn't have the highest of priorities.

And we're - we don't have the mind set to do cyber crime yet. We might, but we like softer targets. And you know I'm sorry, but east Africa we like immediate gratification, you know?

We would rather steal somebody's (unintelligible) mobile money than spend the time trying to figure out how to do it by the DNS. I've seen some evidence of that, but I think it's a matter of yes, we're a bit isolated via satellite and so we're less attractive targets to botnet herders.

And I don't think we've seen any evidence that fiber to the world has made us less secure. Probably makes us more vulnerable but we haven't seen any evidence of it.

So I think that Nii's going to take over from here and talk about the rest of it.

Alice Munyua: Thank you very much McTim, in fact we're going to ask why you think we don't have you know any incidents of DNS abuse but I think you brought it up would be many factors.

And the issue of increased fiber, I think the assumption that we will have increased capacity and you know perhaps increased capacity in you know DNS abuse as well, but you know I'd like to hear from Nii Quanor who will address the challenges, original challenges facing Africa.

Nii Quanor: Very much. I'm very pleased that McTim set the scene appropriately, but I will look at the following regional issues which I think we need to factor in.

One might observer that in our region, we may not even be aware that some of these things are happening in the sense that even if it's happening it's not with our critical systems and therefore we are not feeling like totally taken out.

But I'm sure that there are enterprises that are suffering from some forms of DNS misuse or abuse. The region is typically resource constrained and you can imagine all kinds of ways, what I see in the bandwidth that may be saving you for now but postponing the problem for tomorrow.

But at the same time the more severe challenge is the technical capacity in guarding these systems and I'm not sure we yet have critical mass. You're right, we've trained well over 1000 at least through AfriNIC but it's still not enough for the size of networks that we're beginning to see.

And the group of the networks are also often times over 100% a year and that demands a certain level of maturity in managing networks. Next please.

Now the natural challenge is you know sometimes DNS can fool you, right, in the sense that it so good it works.

So you tend to take it for granted and then you don't look around for issues about it. And that may be an aspect of the problem.

We have of course lack of appreciable skills in this area and for that matter we have you know few incidence response schemes or even reporting schemes.

We also are relatively weak in terms of information sharing, not because we don't want to share but because we are running different quarters and focusing to an extent and not reduce in the effort to build a role.

So we need to understand what it would take to you know expand or mix it up a little bit. We also in some regard have some degree of you know lack of

trust in that you don't often see law enforcement people meeting with end users except when - and researchers and so forth.

And all those things need to be broken down to an extent. We need to encourage the operator, the researchers, the enforcement, the policy regime and so on regulated especially end users to be discussed in these issues, even if it is closed or half closed. Next please.

Now the kinds of things I think would help would be that we haven't quite focused you know the DNS side of issues within the CERTs themselves, okay?

At the same time the CERTs do perform similar functions as one would want for DNS, there's no real known community practices that are documented that we could share across in the region.

Now we need to actually build a community around DNS operators. There's an attempt going on with AFTLD for the CCs but in general we need to let people feel that there is a committee of people who are addressing DNS related issues.

And have them then evolve those practices that may be of interest. Now that's a group, may participate as a point of contact within the existing CERTs because I don't think in Africa where we are just beginning to start building CERTs to have an (unintelligible) CERTs.

You know it would be too hard for us, we may not even have the resources, so it would be much better to organize a community and channel it through their listing CERTs. Now operators should include a DNS issues in their acceptable use policies, so that people will begin to get informed from routine - in a routine way.

Next please. Now another thing that might help is that sometimes ccTLDs are you know constrained in their ability to support ICANN. But they may be able to support ICANN in a larger realm by investing what amount they have in strengthening their local security activities in their CCs as an example.

In essence I'm suggesting that the same contributions they may be making to ICANN should be channeled more into strengthening the security and building the community of you know response teams around the (unintelligible) that they are working on.

Next please, now some tools may help, you know for instance now that we are still working on building capacity, in the short term it might help to get tools that - some make it easier to manage DNS, DNSSEC and so forth, so DNSSEC in the box may be useful.

Having some (unintelligible) that will you know reduce the amount of knowledge required you know before you could at least monitor or manage that systems may also be of help.

Next please. Now with respect to the regional organization for ccTLDs, they've been trying to build capacity for the operators for some time now and they've benefited as was mentioned in ICANN (unintelligible) SLC, AFNOG training and so on.

But on their own in April 2009, the organize indeed an important security related registry related training in Arusha Tanzania and it is the hope that more of those within that community towards strengthening the security of the names services at the edge.

Next please. Now with respect to certain Africa you can see that we are very much in the infancy. According to this site they are forenamed includes Kenya which is very good South Africa acting more issues and Tunisia.

But I'm aware also of very strong activity in Egypt, I'm also aware of activity that has started in Ghana and (unintelligible) in many other countries are now beginning to you know address this issue.

What will be useful is clear you might say blueprint, guidelines, approaches, that can be readily you know you might say adopted for the particular locations that they are working in.

So that would be something that would be useful. Now I also think that it's better to act the DNS CERT as a function of this new CERT because we don't have critical mass yet.

Next please. There are also some environmental issues. Of course you know given the challenges we have in Haiti and also in Chile I think by now we should begin to accept that the planning for disaster is probably the best thing that we can do with respect to our DNS systems.

And remember you know disasters don't only come as you know force major, you know let's say natural you know defects and so on. They can also come from the policy environment.

In the policy environment is not one that appreciates multi stakeholder approaches, the bottom up approaches, that would be continuous interference in the work of the DNS operators and so on.

So we need to factor a lot of scope of you might say 50 that we need to accord the DNS services that we operate, meaning let's make sure that they can operate freely, according to their own rules and regulations set up by their community.

And run a less secure it and make sure that nobody is able to tamper with them. Next please. So with that I say thank you.

Alice Munyua: Thank you very much Nii for that regional perspective. I now hand over to Muriuki Mureithi with the Kenya ITC Action Network. He's going to be looking at specific cyber crimes in Kenya, against someone in Kenya.

Muriuki Mureithi: Thank you Alice. As the DNS abused commit crimes against women and specifically in Kenya, we went out to try to answer that question. And the answer is a big yes.

So what ever they provide now is some of the findings through this process. We are going through a two stage process, first one is to try to get the body of (notage) published, allow this issue, specifically cyber crime against women.

And then from there we also - we are going to (field) to be able to get the (sitters) at the local level and then see how we can extrapolate this to the region and perhaps compare with the global norm.

We bring this - we wanted to launch this on Monday but it's being the International Women's Day and so this was a contradiction to the cause of women of International Women's Day.

We are three people such as doing it and one of the (unintelligible) is me, is the chair of this session. Next slide, okay. So the - sorry, please go back. The objective of this is four fold, first we wanted to understand the world of the perpetrator.

Who is the perpetrator? What are the features of those perpetrators? What motivates the perpetrator? And once we understand the perpetrator then we can ask ourselves what tools can we put regulatory, technical to avoid this occurrence.

Next was in order to see or understand the world of the victim, that is objective number two, and then look at what we are doing as a community,

as a country in terms of mitigating against this or reducing the instance of this crime against half of our population.

And then come up with some proposals, next please. Now is this legal? Yes, when you looked at what is published we saw yes, and all of them are hiding behind the internet.

Hiding behind the internet to commit crimes or various victims and some of this that we found was specifically against women which is very bad. We saw a case in India, it's been prosecuted, we also saw a US.

We also saw in some cases our own country which would be documenting later. Thank you - next. Now I would like us to look at the world of the perpetrator. Who is this perpetrator and what are his features.

Next, so in doing this we also possibly wanted to define what is cyber crime and we are looking at three categories, again of the government, for example cyber warfare, against property, for example in (unintelligible), against a person, the child and the woman.

Now our forecast is against the woman and not the rest. Next please, the initial crime that we saw is - can be cyber harassment and this can be sexual, can be racial, can be religious, and all this results in violation of privacy with cyber space grants to a woman to use.

To develop herself and move on, and then cyber stalking as online harassment using the internet, email and other electronic communication devices to stalk another person.

So this is the scope we are looking at. Next please. Next slide, yeah, and in doing this one thing that we found is a tool of choice. It is either email, it is internet stalking and can also be computer stalking as illustrated there.

Next please. So the first thing we ask ourselves, how did this begin? And as illustrated in the charts, you can see clearly how it has been, how it has all started.

And from the email, contributed about 6% of that cyber crime against women, message boards 15.5%, instant messages and others, 13.25%. Now you notice that the forum was 0.5 and MySpace 0.5%. This is because the data that we put out here is between 2000 and 2008.

I suspect that as we - as the data is updated to the current year and perhaps onward we may see more contribution by the forum and other social networks. Now all this data has been collected from US Websites working to hurt online abuse.

Next please. The other thing is who are the perpetrators? And who are the victims? The harassers, 49.5 are men but also women are significant contributor being up to 28.5%, the last 21.5 was unknown.

Now this is (sir) reporting. Now out of the 21.5 we are not quite sure how many of these are women. Now when you go to the side of the victim, it is clearly the woman. Yes, a quarter of them are men, but three quarters clearly are women.

And therefore this clearly demonstrates that, it's a case against women. Now (unintelligible) is that 49% of the cases, the victim knew the harasser who was an ex-boyfriend, ex-girlfriend.

And for 10.25% of the online was an online acquaintance. Now in about three quarters of the cases the cyber stalking did not result in off line threats.

However, that 30% is significant if it is going to result in threats in real life. Next please. We also wanted to know who is this who is stalking? Who is this

and they found a lot of documentation allowed that the origin of those who were stalking.

It can be the rejected stalker, they knew each other and the relationship was terminated, that partner is not happy and then uses the facility of our internet to continue to do - commit this crime against the woman.

Those others are seeking for intimacy but then they perhaps don't have the social skills to be able to achieve this. In competent suitors others are (unintelligible) stalkers and others are predatory stalkers.

And they are looking for information (unintelligible) and so forth. Next please. The motivation of the stalkers varies.

Can be sexual harassment, which is most prevalent, obsession (fall off), others are (unintelligible) and hits, others are only evil trips, they want to show off, the ability to harass, to use the power of the internet to harass others.

Next please. How about the prevalence of this? It is prevalent, some (unintelligible) indicated that up to 2% in a (unintelligible) among women were stalked at one point or another. Anecdotal evidence because this data is difficult to collect indicates that this is a global phenomenon, is not just restricted to the developed world, is only that internet is more (unintelligible) in those countries.

But it's also coming in to the developing countries, Kenya included. It's happening in Kenya and we're able to implement some cases which we'll be putting together as soon as we write our report. Next.

And with that, thank you. Wanted to give you a glimpse of what we are doing and the contribution that we want to make in safer use of the internet for our women. Thank you.

Alice Munyua: Thank you very much Muriuki. I'll now hand it off to Yurie Ito who will report the results of the first ICANN joint cyber security workshop that was held here.

Yurie Ito: Thank you Alice. Good afternoon, my name is Yurie Ito, I am working for ICANN security team. I would like to give a quick update about our DNS collaborative response work.

So at the security team we have a strategic plan to work with computer (unintelligible) response team on instant response, especially working on raising awareness on DNS security at national CERT levels. But the reality, DNS security awareness level at this national CERT level is very, very different.

I myself actually coming from a CERT community before joining ICANN security team I was working for eight years at Japan's national CERT team, JP CERT as operational director.

So seeing the CERT community and the awareness level some CERTs have DNS specialized experts resource, working very closely with the TLD operators community.

Some CERTs are not, some region there is no national CERTs and those are ccTLD operators are also resource constrained. So the levels are very different. So we are working closely with the CERT community.

This time we have this joined workshop on security awareness, DNS security workshop with the forum of instant response security teams first. And we have this joint session with the first at ICANN security team with CCK hosting this workshop.

We had 35 students from Kenya, Tanzania, Rungi and Nigeria and we've helped set up east African CERT and also provide technical hands on class on data security and other technical matters.

So it went very, very good and I got a very good positive feedback. It is a great news that these regions are working on now to establishing the national CERT, also when they are establishing the CERT they are aware of the DNS security issues and also mechanism to working with the ccTLD community.

Other things working with the CERT community, we are planning to conduct a survey on ccTLD and national CERT collaboration. As I just mentioned, the collaboration level is very different in regions divided with countries.

So what we're trying to do is conduct a survey and find out you know how many ccTLDs are actually have a good point of contact on instant response to its national CERTs or even their instant response mechanism in that country.

So we're trying to conduct that survey. Also we're planning to conduct the DNS security workshop at the first general meeting in June this year.

So this is not only approaching to the recent constrained regions but the global CERT community we're approaching to them and asking - they're raising their awareness of DNS security.

We are continuing collaboration in stopping spread of configure as well as lesson learned and follow up (apple). And also continue to have security team instant reporting mechanism to identify potential systemic DNS instance.

So within the ICANN security team we have the community collaborated response mechanism and we have reporting point actually, if you go into ICANN's Website and go into the security group, we have this reporting point, security (highs) and ops that ICANN.org.

You can report the instance and threat you see and when we identify the given you know reported incidents or threats are affecting to a larger scale, large scale effecting threat or incident, we have a mechanism to (activize) this community collaborative response.

And working with the stakeholders and collaborators to work in response to a threat or this instance. Lastly ICANN security stability and resilience strategic plan is published at ICANN's Website.

And in this (tunnel) Nii raised the issue in Africa region there's the technical expertise resource constraint problem. One of the strategic forum's plan is included the business case, the concept of the DNS CERT.

And we hear the community just like Nii mentioned the difficulties to access to the response resources and tools and technical expertise from those regions.

So the DNS CERT mission is designed to bridge the technical resource to those less resource operators to the core response resource or technical network.

We are aware of those AFNOG, African network operators mailing lists are active and those many operators are on and actively discussing the issues, so there are infrastructure or the information sharing we're hoping that we could, DNS CERT could bridge those (unintelligible) operators to other technical resource out there.

So those plans are on -listed on ICANN's Website. And under the public review period right now. So with that, Alice?

Alice Munyua: Thank you. Thank you very much, I think we open up for questions.

Margie Milam: I'm going to read some questions from the chat. Eric Brunner-Williams had a question actually for Nii but I don't - I'll read it, maybe someone else can answer the question or we can follow up with him later.

His question is, is the introductory registry operator core sufficient or are there other areas of civil society that should also be - that we should also be educating? And I don't know if anyone on the panel wants to address that.

McTim: Sorry, Nii had to duck out for the ISOC meeting but we had a chat before hand and I agreed to answer his questions. Yes, there are other areas that we should be training on.

We need to reach out to students, universities, they have no clue. The professors don't do this sort of network training, need to get more of those types of people to act on AfriNIC training.

The core registry folks, they're pretty (cluefull), but they're always bringing new staff on, so they need to go to TLD trainings for instance.

We had - before this week in Nairobi we had afTLD week, IROC training and I'm not sure if it included SROC, the security aspect of it, but it should - future ones should.

So at AFNOG we sort of you come in, you're a newbie and you take the track zero and then the next time you come back you take the next track and then the next time you come back take the more advanced level.

And the next time you come back you teach, so each one teach one. And that's what we need to replicate in all of our efforts in terms of training.

The short answer is yes, we need - yes, the core registry people are good, then they leave and they go somewhere else, we need to train new people. Training is a never ending task.

Alice Munyua: Thank you McTim. Are there any other questions from the phone? Okay, please state your name and - yes, thank you.

(Eric): Hi, thanks. My name is (Eric) (unintelligible) and (unintelligible) TLDs a comment and a question. There - a few minutes ago talking about earthquake in Latin America and I read a lot of those documents of ICANN (unintelligible) and response program, but always we are focused in the knowledge and response.

And really the problems are very common in technology, learning both case was personal disease and personal communications, the problems. In the case of Haiti some people from the ccTLD and this is knowing the manual or how you respond for the (unintelligible) of things.

And there is the technical person for that system and in the case of Chile the problem was communication between the members we don't have any (consulting) but the communication was impossible to doing even in the same city.

So they can (unintelligible) to respond correctly because they can't coordinate their response. So how is prepare that kind of system when have some angle like that, when the real problem sometimes is the person behind that.

And the second is a question, and it's about the women and for Nii is how does Budapest (redeem) or cyber crime really could resolve some of the problematic and especially in the case of effect of woman's cyber crime? Thanks.

Alice Munyua: Thank you (Eric), Muriuki do you want to respond to that?

Muriuki Mureithi: Thank you very much for that question. This is an ongoing activity and so this is something that we will be looking at. But first of all we want to understand

the dynamic behind it and as you noted we were able to identify first of all the world of the perpetrator.

What we didn't present now because of time, because we are only given ten minutes, we also have information about the world of the victim. The world of that woman who was being attacked, what are their features, what are their - how does this person react or respond to that and what are the long term impact on that?

And then something else that didn't show now again because of time is what is a society doing, what is a international committee doing, what are the local registration like our legislator from within this country doing to (wend) that.

So as we do this we will be looking at the international frameworks, therefore the Budapest's, are there initiatives like the European Union and so forth and so on because we can not be able to isolate and see the Kenyan laws are sufficient for the Kenyan (uman), it's not true.

We have to engage our (ligration) in relation to the proper (aggression). So I would expect that shortly by the time we complete this we will be able to plug in the international legislator framework as well as the local regulatory framework and of course the process of this (to be) as much as possible want to engage the international community, ICANN and we really have to be given this opportunity.

And other agencies in the ICT sector, so thank you.

Alice Munyua: Thank you Muriuki (unintelligible).

Yurie Ito: So there's a question about our recent response and it's not only the technical problems totally agree, and there's always the people behind it. We tend to forget that it's the people doing this.

So it's not only the technical training solve the problem. But - and also efficient instant response, timely instant response always important.

Training is important, communication to constituency or end users even, very important. Raise the transparency about the risk is very important as well to raise the awareness.

Maybe law enforcement, working with the law enforcement and deterrent could work too. So there are multi-layer of things we need to do as a community.

So it's you know a problem will never be solved in one layer, but has to be worked in response and a variety of function and layers and layers together.

Margie Milam: I have another question from Eric Brunner-Williams. He asks why is a centralized CERT a better choice than funding hires and training in the periphery? Probably a question for Yurie, but why is a centralized CERT a better choice than funding hires and training in the periphery?

Yurie Ito: So after we had this configure and it's not really a centralized response mechanism, that if you take - if you read the DNS business case, the proposed business case or DNS concept is not the centralized CERT, it is more facilitation mechanism to work with the global operators and CERT for all other players, stakeholders.

After experience the configure response community asked the ad hoc volunteer base of response useful for short time period of very logistic response.

But sustainable, for example configure response is not finished yet. Configure effective PCs are out there still but out there and we need to clean the eco system, we need to clean this spot.

So operations are not finished yet. We need a sustainable facilitator to make the mechanism to work with the community to do a long term resilient response to a threat and instance.

So that's why we're proposing this CERT. Also again not - this CERT is not about the centralization but again this CERT is designed to work with a distributed CERT committee or distributed regional TLD association, so regional TLD operators using - liaising to regional network operators group, TLD group, CERT group and then and also fiber security response community.

And then bridge those groups and make the community work together, that's what we are proposing.

Margie Milam: I think McTim you have more comments?

McTim: I just wanted to answer Eric I think from an African perspective. And what Yurie said is pretty spot on. I mean we like to have the intelligence at the edges of the network so they can react and that's a good idea.

But for us in Africa we don't have a lot of cash, so having independent CERT in every economy is just not going to work. So we've got to work together with the ccTLD and the country over here in Kenya for example (kicked in that) or the KENIC or sorry the CCK.

There are people in each economy that are active and interested and knowledgeable about these issues and we need to leverage their presence and their interest instead of building a separate CERT in each economy from scratch.

We'll never be able to afford that.

Alice Munyua: Thank you, we have one last question.

Margie Milam: And I think it addresses some of the issues you just raised, this is again from Eric. He asks what is a business case for not starting by paying the costs incurred during the configure event from April to December of last year?

Sure, I'll repeat it again. What is the business case for not starting by paying the costs of the ccTLDs incurred during the configure event from April to December of last year?

Margie Milam: Please make sure you go to the microphone so everybody can hear even on the remote participation.

Greg Rattray: Hi, this is Greg Rattray, ICANN's chief internet security advisor. So I believe Eric's referring to the fact that the configure worm required steps by ccTLD operators in order to block the domain names that the worm was used to propagate those steps had costs.

You know and - you know I think the perspective that we have is that you know to the decentralized model of how DNS security will be achieved, you know that part of the - part of what you do when you run a registry or a registrar or in ICANN's operation of its own IT infrastructure is you know have to build in the ability to deal with these situations.

So the costs you know need to - cost to mitigate configure or distribute it, you know I think the notion that ICANN isn't going to run a centralized security program where everything is funded from the center and you know costs are reimbursable.

I think we want to enable everybody as much as possible, but we do see that the costs for something like configure remediation are born by the entities that have to you know take action in that situation. Thank you.

Alice Munyua: Thank you very much. I'd like to give the panelists a few minutes, two minutes each to make concluding remarks starting with McTim.

Sorry, there's another speaker, one last question.

Warren Kumari: Warren Kumari, Google and this is a comment not a question. I just wanted to thank ICANN for and compliment them on their recent security initiative. I think the ICANN security staff is doing a great job.

Yuri Ito: Thank you.

McTim: Sorry, I've got a question for you, do you have any plans to deploy DNS security on 4.4.4.4.8.8.8.8 or DNS curve or any other - have you invented any other cool DNS security tools for us?

I mean you invent all these incredibly cool tools that we all use every day, so what have you got for us in terms of DNS abuse?

Warren Kumari: Sorry, can't really talk about that at the moment. But you can make some guesses.

McTim: I have no concluding remarks except to comment - to add to the comments on Eric's question. The cost for people who run cyber café's are substantial.

And they are passed down to the consumer but they typically are not connected in this world and don't - they're not on DNS ops, they're not on the DNSSEC deployment list.

So you've got to reach out to those people and try and bring them into the community because they are the private sector and they are the ones who provide the majority of access to the internet for people in Africa.

So yeah, they're footing the bill and passing those costs on to consumers.

Muriuki Mureithi: Thank you Alice. Mine is just to express frustration, frustration, frustration. A lot of effort to add on and are starting crimes against governments, against property with very little effort against the person who drives forth those systems.

Yes, a lot of effort against the child's, child pornography, but as you have seen this pieces that is available for the woman is being invaded in a space where she thought she was safe against the threats that she gets in the world.

Now all the events we have called people to come let us dialogue, let us learn about this women don't come, men don't come and so it's becoming our biggest challenge.

So one thing we're asking ourselves, why the apathy? I hope as we move on perhaps we're going to get better responses. Thank you.

Alice Munyua: Thank you Muriuki. Yurie Ito?

Yurie Ito: Thank you. I think the committees are you know working hard on security to really make - you know try and make the safe and secure internet infrastructure and that would allow the very innovative and you know creative internet infrastructure, you know global infrastructure.

I think at the ICANN you know security team were working with the community to try and identify all the - you know there are lots and lots of - Eric identified many layers to the problem, we tried to identify the problems and identify who is the best players to solve that problem together.

And then collaboratively try to respond to the issues, problems. So it's very community collaborative way of initiatives. So there's proposed DNS CERT or

community collaborated risk funds that we are working with you know existing response community is really for that.

And so there's - I am glad that this workshop with the (unintelligible) and ICANN and CCK offset the outreaching and raising awareness at your DNS security workshop went really good.

And see those operators and players in African regions are very active identifying the issues and working with us. Thank you very much.

Alice Munyua: Thank you.

(Eric): I would like to say that the regional organization of ccTLDs are working very hard with ISOC, with ICANN to have two kinds of workshops continually around the world, one about security to be prepared for this and security issues.

The helping of ICANN in this process helping have better ccTLDs with better service and prepare for this kind of thing, so it's important that's said, and now the community are in coordination for that.

Also we need to start to include the law enforcement in some way, in some moment. But we're beginning that process and never look, all the four original initiative of ccTLDs.

Alice Munyua: Thank you very much (Eric). I'd like to thank all the panelists and all those who've interrupted them through the various questions. We heard about the various initiatives and also the challenges.

And to thank you ICANN for giving us a report on the ICANN and fast join security is a way of beginning to build capacity in the region.

I will conclude this session and move on to the next now where we're going to be looking at concrete responses from law enforcement and private sector, thank you.

Man: Thank you Alice.

Alice Munyua: Okay, the first speaker for this session is Lesley Cowley from Nominet. Lesley, thank you.

Lesley Cowley: Thank you Alice. Okay, we have the technology. I'd like to start with some brief general comments and then move on to tell you about a police operation we were involved with at the end of last year.

So to start with I can't get up on the stage without mentioning some inflammatory statements on domain name security that have been made this week.

And I feel that those have been particularly unhelpful. For me security remains a core strategic and operational priority and it remains that way for just about every registry CEO and registrar that I talk to.

And for many others within this community. And believe you I talk with a lot of them. Nominet is strongly committed to working with all internet stakeholders, and when I say stakeholders that's shorthand for everyone involved in the domain name system and for end users, registrars, government, civil society, etcetera.

And we're committed to working with all of those to ensure the safe and stable operation of the domain name system. And when I say deliver on that, we deliver on that by actions like our involvement in the Conflicker response, the introduction of the phishing lock and by DNS signing dot UK just earlier this week.

So trust in the internet and in our respective country codes domains is pretty important for both Nominet and for other country code managers. And we're very committed to making the internet a safe place or as safe as it can be for end users.

So it's important to keep any security concerns in context. Dot UK is quite a growing country code, there's now 8.4 million domains and many of those are legitimate and they're engaged in legal and proper activities.

But of course not all of them are. And where there are investigations about improper or illegal activity, we work with the law enforcement bodies in the UK to help identify and then remit that activity, whether that be through illegal or fake Websites.

That has always been the case, it's not our role to investigate but it is our role to take fast, effective and responsible action to help protect consumers and end users.

So let me tell you about the police operation. The UK Met police, the metropolitan police have a central e-crime unit. And they launched an operation called operation Papworth just before Christmas in December last year.

I'm not sure why it was called operation Papworth but Papworth is a well known hospital within the UK. Operator Papworth was targeting Web sites run by organized criminal networks which on the face of it was setting some pretty cool designer items such as Ugg boots which were the thing to have at Christmas.

And jewelry from Tiffany & Co. rather cheaper than the genuine Tiffany & Co. I suspect. They were very convincing Websites and many innocent online shoppers were actually duped into making what appeared to be great buys.

They either received nothing at all or they actually received counterfeit products and as part of their very long operation, the policy carried out a comprehensive investigation which included checks that these were not genuine business sites.

But the victims who thought they were genuine business sites risked criminals stealing their identity, credit cards, banking details, addresses, etcetera for misuse elsewhere.

And this is thought to have generated millions of pounds for the gangs which is then recycled to fund other illegal and criminal activity.

So this operation was about targeting the criminal misuse of the UK domain name system. And the idea was about making it much more difficult for those criminals and preventing harm to British citizens who believed they should be safe when trading on line.

As a result of the investigation we received a clear instruction from the police to take down 1219 dot co dot UK domain names. When we received the instruction we worked very closely with our registrars and the vast majority of them were able to take some very quick action themselves to respond.

Had the registry or the registrars not acted quickly and responsibly, the consequences to UK consumers could have been enormous and the intelligence that the piece had showed that the vast majority of those sites were registered from Asia.

So despite they're being dot UK names there's no residency requirements, and anyway they were registered using false or misleading details. This was in breach of our registration terms and conditions but more importantly it almost made it impossible for UK victims to complain about those goods or the non-receipt of goods.

Finally also made it very difficult for UK Trading Standards who wanted the enforcement agencies with in the UK to take action.

What they would normally do is turn up at your business premises. I have to say we were somewhat surprised at the huge amount of media interest n this operation.

Perhaps is the was the brand names that made it a high profile story, perhaps it was because so many people now buy their Christmas presents on line.

And I have to say that some of the staff at Nominet were rather excited when a sky news team turned up at our building. I was not so excited because it meant I had to do a live interview and I had not washed my hair.

But we did find that the publicity enabled us to talk about our commitment for making the internet safe place for all users and to working for the benefit of all stakeholders. And I think it's very important that registries who have a similar commitment and a similar public purpose are actually able to demonstrate that with similar responses.

Thank you.

Alice Munyua: Thank you very much Lesley. Our next speaker is Shaundra Watson who will describe FTS's efforts in shutting down the notorious internet service provider 3FN which was involved in spam, phishing and distributing malicious electronic content.

And she's on now, thank you.

Margie Milam: Shaundra you can go ahead.

Shaundra Watson: Okay thank you, good afternoon - sorry that I was unable to join you in Nairobi but it's still a pleasure to participate in what's turning out to be a very interesting town discussion.

Today I would like to highlight the FTC's high tech enforcement activity but as a preliminary matter I should note that the views I express are my own and do not necessarily reflect those of the commission or any individual commissioner.

Next slide, what is the FTC? To begin I'd like to provide a brief overview of the FTC just for people who may not be as familiar with those in the US. The FTC is the only general jurisdiction (unintelligible) protection agency in the United States.

It's an independent agency headquartered in Washington DC and we have eight regional offices around the country. And we have the ability to enforce various laws in both federal court and administrative litigation.

Next slide, the principle statute that the FTC enforces is the FTC Act and in particular section five of the FTC Act prohibits unfair deceptive acts or practices and are affecting commerce.

But in addition to the FTC Act there are a number of other consumer protection statutes that the FTC enforces, and I just listed a few to show you the broad range of issues that we handle from children online, privacy protection to the Can Spam Act which prohibits among other things sending a false or misleading commercial emails with deceptive subject headings.

The violations go on and on there. The Gramm-Leach-Bliley Act which requires financial institutions to among other things safeguard consumer personal financial information, the fair credit reporting act, telemarketing.

So we really do a range of different things. Next slide, but today I'd really like to focus on some of the high tech, quote unquote high tech work that the FTC has done.

And even in that area there really is a broad range of issues that we've addressed over the last few years and have continued to do so ranging from internet fraud where brick and mortar scams like business opportunities, work at home scams are marketed via the internet.

There's spyware, several different spyware cases where we've seen time and time again people falsely advertise antivirus software when it's really infecting consumer's computers.

We've got cases related to P2P file sharing and digital rights management and also increasingly social networking, there was a very successful social networking case that involved a COPPA violation and obviously spam as I mentioned before, there's been a lot of enforcement of the canned spam act where international cooperation has really been a key component.

Next slide, today however I'd like to highlight one case to illustrate the FTCs work in this area, it's a fairly recent case, it's filed in June of 2009, FTTB Pricewert.

And this was a case against a rogue internet service provider that had hundreds of servers in the United States although we believe the operator of this company were actually living abroad.

The case is significant for many reasons but especially because it was the first time the FTC had used this authority to take down an ISP.

Next slide, the complaint that was filed against Pricewert was filed against Pricewert which was a shell corporation that operated under various aliases including 3FN as an ISP.

And the FCC alleged in this case that Pricewert normally hosted a maximum amount of illegal content including child pornography, online pharmacies, botnet command and control servers, pirated music and software, spamming tools, etcetera, basically anything bad, they had it.

And in addition the FTC alleged that price port actually collaborated with spot herders to configure deploy or operate the botnet comprised of literally thousands of compromised computers.

Next slide, the case was really an excellent example of collaboration among government academia and the private sector.

And today I just would like to give you an overview of some of the different types of evidence that we obtained from all the different sources including National Office of the Inspector General, the University of Alabama, the National Center for Missing and Exploited Children, Spamhaus, Shadowserver foundations, Symantec, the SEC's own investigative team.

It really was a very useful collaboration among a lot of intricate stakeholders, an example of how when we all collaborate we can really sort of achieve good results.

Next slide, so let's just start with the discovery of 3FN and how this all started. NASA first learned of 3FN as a result of computer intrusions at NASA that were traced to MoColo and ultimately 3FN.

And MoColo was another sort of notorious ISP that was ultimately shut down. Pursuant to a federal search warrant, NASA copied contents of MoColo servers related to these intrusions and by analyzing the data, a special agent at NASA was able to determine several different things that ultimately proved immensely helpful in the SEC's case.

But one of the things that they identify with the location of 3FN data centers, where the servers were housed which ultimately ended up being in San Jose California.

But significantly the agent also obtained 3FN ICQ logs which were transcripts of instant message conversations between various parties that were relayed through the MoColo servers.

And as I mentioned this evidence as you'll see in the next slide was really pretty critical. Next slide, so this is an excerpt from 3FN's ICQ chat log.

These messages were originally in Russian and NASA was actually able to link the cat participants to 3FN, at least two of them through their unique ICQ identifiers. And so here they're just listed as the various names that they were going by.

And this particular slide I think you're looking at the senior project manager slide, yes, a senior project manager for 3FN is approached by a customer seeking to work with 3FN on a botnet and clicker, the use of a botnet to commit click fraud.

The senior project manager enquires about the size of the botnet and asks 3FN will need to rewrite the software to control it. The senior project manager assures the customer that we can manage it, then the proceeds to explain to the customer that 20,000 active bots are needed in order to generate $500 a day through click fraud.

Next slide, in this slide, another one of the ICQ chats, the 3FN's head of programming engages in a conversation with the customer regarding the number of compromised computers the customer controls.

The customer informs 3FN that he controls a total of 200,000 compromised computers with 20,000 online and available for use at the time of the chat.

The customer then offers his massive network of bots to 3FN, the head of 3FN programming department agrees to work with the customer but complains upon learning the size of the botnet that it will require a lot of effort.

And so as you can see it's kind of direct evidence that 3FN not only hosted malicious content that was created by third parties, but it was also directly involved in colluding with criminals who were deploying botnets to further these illegal activities.

Next slide.

Margie Milam: Shaundra, can you speak a little slower for our transcribers if that's okay.

Shaundra Watson: Oh sure. So moving on as I mentioned we had a number of different really important evidentiary sources, and so another was from a research director for computer forensics at the University of Alabama.

And the research director analyzed content of domains hosted by 3FN and was actually able to confirm just the malicious content included as we've already mentioned, child pornography, spam generation software, pirated music software, online pharmacies.

In addition he also was able to confirm that 3FN was advertising in a forum called crutop.nu which was really a forum that spammers - that was a discussion forum for how to make money using spam.

And that was also a Russian language forum. The research director actually studied malicious code downloaded from 3NF domains and figured out how to access 3NF hosted Websites associated with the malicious code and was actually able to view tracking statistics made by the individuals who were controlling the botnet.

And that's how he was able to determine that there were literally thousands of infected computers in the botnet.

Next slide, another source was the National Center for Missing and Exploited Children. The National Center for Missing and Exploited Children maintained a cyber tip line and through this cyber tip line they enabled members of the public service providers and law enforcement to report images containing child pornography on line.

The organization analyzed IP ranges that were controlled by 3FN to see if they match any of the reports they received and as this slide indicates they were able to determine from their databaser that they had 700 reports of child pornography.

And they were actually able to confirm 500 of those that 500 of those reports actually did result in child pornography by looking at the content.

Next slide, another really helpful source in this investigation was Spamhaus and as many people know, Spamhaus is a very active anti-spam organization that creates bots, lock (with), it does its own research and if they discover that IP addresses are associated with some sort of malicious activity they typically contact the ISP which in turn may take action.

So Spamhaus followed this practice with respect to 3FN after determining that some IP addresses were not only connected to malicious activity but also 17 different IP addresses controlled by 3FN were related to botnet command and control servers.

However when they contacted 3FN representatives, according to Spamhaus 3FN was in compliance but then they would just shift the sites to other IP addresses owned by 3FN for example.

And so the sites would be back up. And so a representative from Spamhaus was able to file a declaration in our case to this effect, they discussed the massive number of botnet command and control servers.

As I mentioned they indicated that there were 17 during a specific period on one network which they believed was actually a very significant number to have on any one network.

And as a result compared 3FN to MoColo and Intercage which were other sort of notorious ISPs that were ultimately shut down.

Next slide, we also received assistance from the Shadowserver Foundation which is a group of security researchers that gather information on malicious software, botnet activity and compromised servers.

After reviewing 3FN IP ranges the Shadowserver Foundation concluded that 311 3FN IP addresses participated in or facilitated malicious activity.

As you can see it also concluded that 4576 unique malware virus specimens used 3FN server for control and command functions.

An analysis of the malware showed various programs that were capable of key stroke logging, password stealing, data stealing, programs involved in the distribution of spam so a number of different types of malicious activity.

Next slide, Symantec also reviewed a number of 3FN IP ranges and searched their own database for cyber intrusions or attacks originating from these IP addresses that belong to 3FN.

And they also confirmed that these IP addresses were connected to bot attacks, bot command and control activity, spam and phishing attacks.

And last - next slide, last but not least, the FTC used its own investigative team to collect a variety of information.

Our FTC investigator was able to connect various aliases that Pricewert used actually based on its WHOIS information and domain name registrations which were all actually listed to Pricewert as a registrant.

So although all of these different aliases kept coming up they were actually registered under Pricewert.

The FTC investigator also followed up on several other evidentiary leads including confirming that the operators were foreign, securing translations of the ICQ chat logs, reviewing various complaints on line.

The FTC investigator also visited sites hosted by 3FN and that actually resulted in eight computer infections and so the computers were infected with programs that ranged from - that redirect consumers to Websites, to programs that would steal passwords for bank accounts or other Websites.

Next slide, the impact assessment. Now what was the impact of this 3FN shut down? Well that's difficult to measure precisely. There was a significant drop in spam levels. One estimate was actually 30% but unfortunately that drop was temporary.

It also had the 3FN takedown also had a significant impact on what was called the cut wheel botnet.

Next slide, unfortunately the bad news of the impact assessment is that criminals are reacting to these take downs by decentralizing their operations even more and continuing to take advantage of the ability to operate anonymously on the internet.

And are simply rebuilding their operations despite efforts by law enforcement and security communities to take them down and stop the malicious activities.

So we definitely need to still explore other solutions, and I think we'll take questions during the discussion. Thank you.

Alice Munyua: Thank you very much Shaundra. Our next speaker is Debra Hughes who shared the experience of Red Cross in responding to DNS abuse in the wake of the Haiti earthquake.

Debra Hughes: Good afternoon, it's such a pleasure to be able to speak with you this afternoon about some of the unique challenges that non-profit organizations like the American Red Cross face when using the DNS to execute it's important mission.

I think most of us would agree that non-profit organizations perform some of the most important work on the DNS and I'm humbled to be here with you today to talk to you a little bit about some of those challenges.

The American Red Cross is one of more than 180 countries that are part of the Red Crescent and Red Cross movement. Next slide. And for those of you who aren't familiar with the movement, the Red Cross and Red Crescent movement provides humanitarian aid without discrimination to the world.

And we are proud to be able to do that. But what we want to talk to you today about are about how we use the internet to execute that mission and some of the challenges we have doing so.

Next slide. Some of you may be familiar with some of what we do but wanted to let you know that the American Red Cross of course provides disaster relief assistance, next slide. That we also provide assistance to wounded soldiers in - who are injured in the performance of their duties.

We also provide information to the world about importance of collecting blood. Next slide. We offer training, life saving skill set via the internet and opportunities for the public to purchase those.

Next slide, and working in association with our wonderful national societies we provide international relief aid. Next slide. Wanted to talk to you a little bit more specifically about some of the challenges we have in how we use the DNS to execute this mission.

And for example we do offer international humanitarian law courses that provide information to communities about the importance of international humanitarian law.

That information is on a Website, that information is shared with the world. We also use the internet to talk about the importance of getting engaged and volunteering and all that information is also used on Websites that are owned and operated by the American Red Cross.

Next slide, some of you may not be aware that we also use social media to engage and empower the communities that are affected by disaster or who are impacted by the work that we do and we're fortunate that we have the ability to use social media to get the word out.

I was talking to a couple people while I was here in ICANN explaining that for organizations like the American Red Cross the internet is a wonderful opportunity for us to spread the message, to get information that's very, very important out to the communities we serve in a very cost effective way.

Next slide. In times of disaster, Websites like FamilyLinks allow those who have been impacted by disaster to connect with their family. And you can imagine in disasters like Haiti and what has recently happened in Chile, Websites like this are vitally important.

And what a shame it would be when DNS abuse happens and sites like these are impacted. Next slide. And finally I guess most importantly in order to execute this fine work, we also use the internet to collect donations.

It is a opportunity for fraud sadly but it is an obligation that we take very seriously and is vitally important to the work that I particularly do for the Red Cross and I think all who are members of the Red Cross and Red Crescent society want to say that we really appreciate the generosity of those who donate to non-profit organizations.

And we value that trust, and sadly there are those out there who would take advantage of Websites where we're collecting funds to do nefarious things.

Next slide. So because the world is an imperfect place, we must have a strong enforcement program to protect the communities that we serve and to protect those who donate funds to the American Red Cross using our Website.

It's a large part of what I do for the American Red Cross and to those of us in non-profit organizations sadly we must use resources to address this type of DNS abuse.

One thing that I'll mention is that the American Red Cross is fortunate enough to have the protection of the Geneva Convention to prevent the abuse and misuse of the name Red Cross in internet domain names.

However what I want the community in ICANN to think about, what about those organizations that come from small and developing countries that may not have the protections of international treaties?

That may not have the benefit of a statute to protect them from abuse. What about small organizations that are trying to do the best they can but don't have the resources or don't have an in house team to prevent DNS abuse.

And so I'm also speaking I hope in a way to bring to ICANN's attention that although organizations like the American Red Cross and the ICRC have the protection of the Geneva convention and can - the resources thankfully to reach out and to get and partner with local law enforcement, there are many organizations who don't.

Next slide, so I have to play cop and I don't have the time or resources to do that and I want to just send a special acknowledgement to my team back at the American Red Cross who I hope is watching.

We - when I say my team, it's me and my great friend (Rick), and that's not all that we do. I don't spend all of my time doing internet enforcement and managing the DNS.

There's a lot of very important work that those of us who work for the American Red Cross and non-profit organizations are forced to do.

We have to multi-task, but we must do what we must do. Next slide. So what do we do? We monitor the internet, fine. Fraudulent Websites, we send cease and desist letters.

We investigate complaints that we receive via call centers, but I can tell you guys something. Sadly most of the responses in the matters that come into the American Red Cross don't come from any offensive acts that I'm doing, any monitoring or proactive work that I'm doing.

It comes from calls that come in from our volunteers and our corporate partners who are concerned about the abuse that's occurring out there. Calls from victims who have been duped by nefarious people.

Next slide, so what type of abuse are we seeing? It's what you might see in the corporate sector. We see people register domain names that contain Red

Cross in them, that have misspellings of Red Cross and sadly we are forced to deal with the same type of abuse that our non-profit partners - that our for profit partners also must deal with.

But keep in mind, we don't have the resources that these commercial users have. We also see people setting up Websites in organizations, setting up Websites to try to distract the public away from our official Website to theirs, to try to create an affiliation which creates good will or some sort of boon that will help them do whatever their particular need is.

And sadly that's another type of abuse that we have to deal with at the American Red Cross. Next slide. So wanted to just talk a little bit about some specific examples of you know when you're talking about DNS abuse Debbie, what are you talking about?

What types of abuse? I mean are you telling me that really, it's occurring? And it is. And I think my predecessor spoke to ICANN in 2005 about some of the problems that we had after the Hurricane Katrina but I just wanted to talk a little bit about what I've experienced since I've been at the Red Cross for about a year and a half.

And I just want you to sit in the day in the life of Debbie Hughes for a moment. So I'm sitting at my computer, it's about 4 o'clock in the afternoon in January. And I'm trying to help a team pull together some information about a project that we're working on.

And lo and behold I start to receive an influx of emails about a horrible disaster that's occurred in Haiti. And so while I start now talking to the teams about what our disaster response is going to be, how we're going to help these teams respond, at the same time we start to receive a flood of emails and calls about offensive domain names that have been registered.

And all sorts of DNS abuse that's occurring on the internet. So my team of half a person, because I'm not doing this all the time and neither is my dear friend (Rick), we now have to resort to take all of our resources that we could have used to help effectuate the other important tasks that the American Red Cross.

And now we have to put on our enforcement cop hats again and now go figure out how are we going to combat this DNS abuse?

And so we have people who registered domain names that have Haiti and Red Cross in them, and in first example the person who set up this Website actually had set up a PayPal account to encourage people to donate to the Red Cross and they were certainly not affiliated with us.

And the list goes on and on and on. I can tell you some people might wonder well what kind of traffic are we talking about at the Red Cross? On an average week before the Haiti impact, just to kind of give you some idea about what we're talking about for traffic and how many people really own Red Cross Websites.

The week prior to Haiti and I got these stats from my IT team there were about two million page views of redcross.org. During the week of Haiti around that period the page views increased to 14.7 million.

So we're talking about a lot of volume. And when you add to that the wonderful advertising and promotional efforts that happen around what we're trying to accomplish to help the people in the community in Haiti, you can imagine the abuse that spikes around that time.

There was a lot of interest in how we were trying to help the community and sadly at the same time we also saw a spike in the number of matters that we had to deal with.

I can also just mention too in Chile when that disaster struck, that base line of about two million spiked to about 3.1 million and we're not sure if that's totally due to the efforts in Chile still spilling over.

But there was a spike in activity on redcross.org around that period of time as well. But just wanted to kind of give you another stat that you might find interesting. Within the first two weeks after the Haiti response, I had the pleasure of having to deal and investigate with approximately 90 instance of abuse.

Ninety, in a two week period. Keep in mind that's not all I do. Keep in mind I'm also trying to help fund raise for the American Red Cross to support those efforts.

And I just want to stress when we talk about is this a real thing? Oh it's real, I live it. I live it every day and so does the American Red Cross.

But we're committed to it and I didn't mind that I didn't get a lot of sleep during that period but that's okay. But you do what you have to do when you believe in something that's important.

I can also mention that just generally after Hurricane Gustav there were about 172 domains that were registered within the first 24 hours and then also in Hurricane Katrina hundreds and hundreds.

Next slide. We also have spam email problems just like everybody else Next slide. And so our challenge is how do you prioritize all of this work with limited resources, trying to identify who is the registrant of these domain names.

Next slide, when you find a registrant that is using a proxy or privacy service, then taking the extra step to go through those hoops to find that person and while we're willing to do and play by the rules, keep in mind when we're talking about DNS abuse related to the American Red Cross there's time that

is of the essence because we're talking about people's donated dollars that are at issue.

And we're not just talking about you know your run of the mill type of abuse, we're talking about abuse where people have donated funds or there's a threat that they may donate funds to an improper Website.

So that's our main challenge and that's really the message that we wanted to bring. If ICANN things that non-profit organizations do important work then we hope that you'll think about non-profit organizations when you create policies and best practices surrounding the use of the internet and DNS abuse.

Thank you.

Alice Munyua: Thank you very much Debra. Our last speaker is Richard Boscovich, I hope I have pronounced that correctly and he will detail Microsoft's legal assault to take down the Waledac botnet network effective of spreading spam and harmful computer bots. You have the mic Richard.

Richard Boscovich: Thank you. I just want to make sure that you can hear me. I wanted to first thank ICANN for giving me the opportunity of presenting today.

Alice Munyua: Richard we have an echo, perhaps you - are you on a speaker phone?

Richard Boscovich: No, I'm not. What happened was the computer was on as well and I just muted that, I'm sorry.

Alice Munyua: Okay, thanks.

Richard Boscovich: First off, thank you for giving me the opportunity to present today. We at Microsoft are very grateful for ICANN on giving us this opportunity.

Before I go ahead and begin the presentation I just want to give you some background on the group where I work at Microsoft and it's called the GEO crimes unit.

And to put these in context, we are part of the legal and corporate affairs of the company. However we are not located in legal and corporate affairs but rather we are embedded with trustworthy computing at Microsoft.

Microsoft's malware protection center which is our antivirus solution as well as the Microsoft research center. So we are closely linked with a lot of the researchers and engineers at the company which look at security on a daily basis.

And we're basically comprised of attorneys, the majority of which are former prosecutors from either state or the federal government as well as program managers and forensic examiners.

Next slide please. We decided to take some unique action against bots and during the course of our analysis as to how we're going to address taking a different approach on addressing the bot issue we first had arrived at a particular target which we believed would be a good first candidate for a novel civil action or legal action.

As well as a novel technical counter measures. We worked closely with industry partners and academic partners on this.

On the academic front we worked closely with the University of Washington and also with the University of Mannheim, Bonn and Vienna as well as a Shadowserver, Foundation, Symantec and several other industry partners which helped us tremendously but requested that their participation be kept confidential.

We ultimately settled on the Waledac bot due to its unique structure in the sense that it was both an HTTP and peer to peer based bot.

It has a four tiered structure with a fast flux component to it. And we thought this was interesting since we would be able to test both of our theories, the first being have you addressed the controller command server which is domain name based.

At the same time utilizing technical counter measures while simultaneously to address a peer to peer architecture.

Moreover from the legal side we had to find a bot whose damages were clearly identified and would be readily understood by a civil court in that we wanted to make sure that there was at least in the US a specific violation which a court would feel comfortable with and quickly recognize.

Since we were going to ask for an extraordinary relief, in essence we were going to ask that the court go ahead and issue a temporary restraining order directed not at the registrars but rather at a registry.

Sever the domains associated with the Waledac botnet. That was extraordinary and very difficult to obtain such a TRO as we call it in the states and in most countries who's laws are based on common law.

In that for it to be effective it had to be ex parte, ex parte meaning that the other side that is the registrants, the owners of the domains would not be present and would not have an opportunity to be heard at the hearing.

As a general matter courts do not like to do that since in essence you are taking someone's property so to speak away from them temporarily at least without giving them an initial opportunity to be heard.

So the damages issue was important since we had to prove clearly and unequivocally that Microsoft was being damaged and that such damage is ongoing, irreparable, and it would continue to go on if the court did not issue that temporary restraining order which would direct the registry to sever the connections to those domains.

Waledac fit the bill in the sense that it was easy to identify spam as a problem, we were able to document to the court in our pleadings that we had blocked in an 18 day period approximately 650 million IP's associated with Waledac as it tried to send spam to our users on hotmail.

We were also able to identify and present to the court that an additional 24 million spam emails had actually made it through and reached our users, thereby conclusively showing that we in fact had suffered harm.

As a result we were able to present copies for examples of the spam issued by Waledac showing trademark and copyright infringements not only against Microsoft but a host of other companies which were not necessarily party to the suit.

But were clearly victims as well, companies such as Pfizer, Rolex, and other well known companies worldwide.

And of course the victims themselves were also the computer users who's computers were infected with the virus. We were able to convince a court to give us a temporary restraining order and the order was directed to the registry.

In this case it was VeriSign since the Waledac botnet was primarily if not exclusively in the dot com domain. Next slide please. The law gave us 14 days to be able to go ahead and now provide notice to the domain owners.

And this was basically the major point and the reason why we had to proceed ex parte with a TRO. And why we argued to the court that this was the only procedure that would work in this case.

We told the court and explained to the court that as opposed to standard trademark cases or copyright cases in which you would go directly to the registrar and request a take down that the very nature of the bot itself and those behind the bot, the bot herders would if given any indication at all or any notice at all that we were trying to take down those domains would move.

And that movement would be virtually immediate and thereby continuing to harm against Microsoft and putting us back into square one.

That is why we had to develop the strategy that we did and that is why we asked of course the TRO. After we get the TRO and that was in fact granted and it was the first TRO specifically tailored ex parte TRO specifically tailored to combat a bot.

We had 14 days to provide notice to those individuals who owned the domains. Again courts are very hesitant to take people's property and rights away without giving that individual or entity the right to be heard and that makes sense.

Another hurdle that we had to overcome was to provide the court sufficient explanation as to how we were going to go out and advise or reach or provide notice to those domain owners, the registrants.

Part of our strategy was to go ahead and utilize the system already in place in providing notice. We would go to the registries and ask for the registrant information and we told the court that that's what we were going to do.

That that was the process in place and that we would reach out both by mail and email to the registrants in an effort to locate them and provide them notice.

Moreover in order to provide the court a higher comfort level we also indicated that we would proceed via the Hague convention with the understanding that this may take four to five months for the process to run through nonetheless it was a process that was recognized and familiar for the court.

Now the court understood that our position was that a lot of the information if not all of the information that the registrants provided the registrar would more likely than not be fictitious or inaccurate.

And at the conclusion of the 14 days, the court held a hearing and at that hearing we advised the court with the exception of two domain name holders, both of which were able to contact, both of which at that point were located in the United States and were not aware that their domains had been compromised, the remaining 275 of the 277 never responded.

And the reasons are obvious. Next slide please and I'm just using the slide as a background as to the extent of the problem we were looking at, and this last slide which is up now indicates from the US perspectives the number of IPs that we were associated with Waledac during that time period.

And also on a global basis. Once the hearing took place, the court went ahead and modified temporary restraining order for a preliminary injunction. And legally what that means is doing dependency of our case, we would now have those domains severed.

And the bot herders will not have the ability to utilize those domains for their CNC. Now in addition to that as I mentioned in the beginning this was a unique bot in the sense that it was HTTP and peer to peer, our technical

counter measures with our industry partners and academic partners were able to address the peer to peer components.

In such a way that we have seen a drastic reduction in the bot's ability to communicate and therefore send out spam and potentially infect other consumers as well.

From a legal perspective the next step at this point and all of this is available on our Website which I provided to ICANN where all of our legal pleadings are located.

And incidentally the pleadings are both in English and in Chinese, since these domains were primarily registered with the exception of two or three with Chinese registrars, would be to request discovery for purposes of better estimating the damage involved with the Waledac botnet.

We anticipate that within the next several days the federal court in the District of Virginia would provide us a new order in which we will be able to request that VeriSign now direct traffic information to Microsoft pursuant to the court order for a period of a week or two.

And at that particular time we'll be able to report to the court with much more specificity. The exact number of infected computers as well as be able to geo located the computers as to where they are located and what type of harm we are seeing on those computers.

That would allow us to go back and better articulate to the court our next steps as to what we're going to do with that information and the conclusion of our case.

To just go over one last point in terms of the complexity of the operation, both legally and technically I cannot go without mentioning the support we did receive literally at the eleventh hour from China CERT.

While we were preparing our documentation to file, in the eastern District of Virginia our academic partners identified additional domains which had just been added and which we had no time to immediately include in some of our papers.

With the cooperation of China CERT we were able to address those domains effectively and also take them out of the control of the bot herders so that the operation for all intensive purposes on the legal side was a success.

And on the technical side our latest reports from our partners indicated a drastic reduction in the number of new IPs infected with the known Waledac malware.

In terms of our internal review of spam, we've seen a 50% reduction of spam directed at hotmail from IP associated with Waledac. We believe that the other 50% which are also associated with Waledac are more likely than not, not being sent by Waledac but rather that the same computers originating from these IP addresses are more likely than not infected with other malware.

And thereby are continuing to send spam due to multiple infection on those boxes. All in all I think that the operation proves that working together in a community based operation both with industry and academic partners on the technical side and searching for novel legal solutions or the implementation of traditional legal solutions to a novel problem definitely has its merits.

And we at Microsoft considered this a small step forward and one more mechanism by which we could address the botnet threat and hopefully learn a little bit more as to why the DNS system is being abused by bot herders and working closely with the community to come up with alternatives to hopefully minimize this threat in the future. Thank you.

Alice Munyua: I thank you very much Richard and all our other panelists. I think we'll open for questions now.

Margie Milam: (Michael).

(Paul Horton): (Paul Horton), Serious Organised Crime Agency. I think I'm the only law enforcement officer in the room. Can I just thank everybody who stayed for this session? It's a very important area and I think we're preaching to the converted, to the people who are actually here.

I think the percent is - the percent - especially Debbie who's put a very humanitarian aspect on what's seen sometimes as a white collar victimless crime which it's not. Can I just ask each of the presenters if they could give us maybe one or two bullet points which would give tangible advice on how to enhance cooperation between industry and law enforcement as per the title of the workshop? Thank you.

Alice Munyua: Thank you. Okay Debra you could start.

Debra Hughes: I could say the first thing would be education and providing ways to get information to non-profit organizations. I feel blessed that I'm at an organization that supports my activity in ICANN. And so I have access.

But there's tons of non-profit organizations don't - that are victims of this type of abuse but they don't know the shortcut. They don't know the ways to work through these complicated issues when you get attacked by spam, when your Web site is compromised, when a phished email or phished Web site appears and you're trying to figure out what's going on when you get customer complaints.

Best practices I think is an exciting idea that I think I heard one of the workgroups talking about. I'm not talking about mandatory requirements or mandatory things that registrars and registries should do, but registrar

partners like Nominet and others that reach out to the non-profit organizations or others in the ICANN community that could provide assistance and guidance and information, I think that's one thing.

And then I think the other thing is when we're thinking about policies that affect users of the Internet, can we also remember that a lot of the users of the Internet are non-commercial and they have limited resources.

So when we talk about oh if you've got DNS abuse, go file a UDRP, keep in mind that it's personally offensive to me to have to spend my organization's resources to go file a lawsuit or to go seek protection in a UDRP.

So if the community could be creative and think about ways and options for those - the least of these who are out there doing their best but also want to do great work within the DNS. Thank you.

Alice Munyua: Thank you Debra. Lesley go on.

Lesley Cowley: I guess my comment...

Woman: ...argument of the mike.

Lesley Cowley: Thank you so much. I would suggest cooperation in developing an understanding of how people work, how the systems work, what policies there are, if there are policies in place and understanding how best to work with those policies.

As I have talked to you, I don't think legislation is an answer, but developing policies that are able to be responsive and reactive and responsible, not rash, is a good way forward.

I would also just speak up against some of the direction I've traveled in this area to make sure that we protect the genuine registrants who are not

malicious actors but may well have activities are acted out then the kind of try to take advantage of any fast roots that are developed through policy.

So I think, you know, there's a real balancing act here of being responsive to deal with criminal activity but also helping to protect genuine registrants who maybe might have that kind of policy used to their disadvantage.

Alice Munyua: Thank you Lesley. Shaundra do you have any comments to make on that? You have the mike?

Shaundra Watson: Yes. Can you hear me?

Alice Munyua: Yes we can.

Shaundra Watson: I guess in response to the question, I would say I think it's important for both the private sector the secured community to engage with law enforcement, and particularly internationally in the development of global solutions to address these problems.

There are a number of public private initiatives that are international. For example, the London Action Plan, the FCC in conjunction with the UK's Office of Fair Trading and Industry Canada operate the secretariat for the London Action Plan which is a global organization that's devoted to addressing spam, spyware and related Internet threats. And it's comprised of law enforcement agencies and industry representatives from over 20 countries.

And so those are the types of initiatives that I think could really fuel some of the cooperation between law enforcement and industry. And so investing in those types of partnerships, particularly those that are global because it really is a global problem, I think will go a long way towards addressing this problem.

And the other sort of key thing I think that's important, which is sort of one of the goals or objectives of global organizations like that is information sharing. So and for example the case that I highlighted today, you know, there were about five or six sources of key, I mean critical information that did not come from our agency. It came from academia. It came from industry representatives, and so that information is actually going to be very important when it comes to actually filing an enforcement action not only for our agency but for all of these foreign agencies that are trying to tackle these problems.

And so actual sharing of information and developing these contacts within these networks I think is really key.

Alice Munyua: Thank you Shaundra. Richard you have the mike.

Richard Boscovich: Oh thank you. Wow that's a real good question. I mean, at the Digital Crime Unit at Microsoft, we have a long history of really working closely with law enforcement in terms of criminal referrals, assisting forensically and trying to do the right thing whenever possible.

The major point that I want to bring up is that one of - it's very - well let me put it this way. It's very hard at times to share information as a result of privacy concerns.

From the private sector's perspective, we have to be very careful in how we go about sharing that information. We at one point have to guarantee the privacy rights of our users while at the same time we have to protect them.

I think that we at Microsoft reached a very good balance between the two in that we aggressively do our internal research and investigations. And due to certain legal issues in the United States, we do not bring in law enforcement until we are ready to refer the matter to law enforcement.

And it's that, you know, approach that I believe has been very helpful and useful to Microsoft in which we respect our user's privacy. Yet we go out and investigate and protect their rights and engage law enforcement once that investigation internally is completed so that they could go ahead and engage and do what they do best.

I think the Waledac experience for me at least really highlighted the effectiveness of industry cooperation and academic cooperation. It was clear to me that especially on the technical countermeasure side, that the wealth of knowledge and expertise from researchers outside of Microsoft was invaluable in our operation.

And their willingness to cooperate, to address a (sethinick) threat in the ecosystem where we all either do our research or do our business, and for the consumers where they transact business or communicate with family members every day was really the underlying motivator for the vast group of those assisting us in that operation.

So, cooperation is the key. And I think that the DNS issue is one that in my opinion can be addressed from an industry perspective at this point. And I really encourage the community to look at what the weak spots are and come up with creative ideas to address those.

Alice Munyua: Thank you very much. We have a question from a remote participant.

Margie Milam: This question is from Eric Brunner-Williams and he has a question for Debbie. His question is would a hold down timer for domains that contain a present moment disaster identifiers substantially change the problem?

Debra Hughes: I'm sorry but I don't think I quite understand the question. Oh yes. So sure, I mean that would certainly solve part of the problem but the issue really is the ongoing abuse. I mean if it's - I'm not - so part of my challenge is monitoring

the domains that pop up and then they go away, right? That's part of my prioritization process.

The second is what about the domains that pop up, go away, pop back again. It's like playing Whack-A-Mole. So if you can help me fix that Whack-A-Mole problem - so I spend a bunch of time in resources on one particular domain name and registrant and then whoop, Whack-A-Mole is now no longer active.

Let's say maybe I didn't request to have that domain name transferred into our portfolio because it didn't make sense maybe financially or just didn't make sense for me to hold onto that domain. And then it pops back up again and then Whack - I mean my resources aren't such that I'm going to probably litigate every bad actor.

So the problem is, maybe I'm dealing with that one incident and that one bad actor, but what happens when that bad actor is a little bit smarter and has a little bit more resources than me as a non-profit and is counting on the fact that maybe he'll be able to jump around.

So it may - that may be a great solution for that one incident, but what we've seen is that people who are nefarious and want to do wrong are really good at it. And what we need to do as a non-profit organization is to learn to get as smart as they are.

Woman: Excellent. (Unintelligible).

Lesley Cowley: One practical suggestion that we've shared with another - other registries within the ICANN community, we introduced the phishing locks and timed back specifically for phishing activity where registrars could place a lock on a name. And that has recently been extended to include criminal activity for example. And that may well achieve the desired effects.

Alice Munyua: So we have one last question please.

Evan Leibovitch: Hi there. My name is Evan Leibovitch. I'm the Chair of ICANN At-Large North American region. And the session that was just previously on before this in this room was about development of a high security certification program of sorts that a registry or top labeled domain could ask for.

I want to ask the people and the speakers, would you work with something like that or do you think this is a matter that ICANN's core regulations should be strengthened sufficiently?

And if you do think the idea of the high security certification is a good idea, I'd invite you to get involved with it because right now there's not an awful lot of participation from the end users that would benefit from it.

Debra Hughes: It certainly sounds promising. And I've been following a little bit of it. What I can say is from my own organization's perspective, the idea that there would be such a zone is good news for us if it's going to mean that I'm spending less and less time dealing with these types of abuse, the phishing, the scams, the malicious code being inserted into emails and that sort of thing.

I guess what my concern is how universally it's going to be accepted. And, you know, so before I think we can really make an assessment, I think isn't that really part of it? Isn't it really how is that going to be embraced by the ICANN community? And I would hope that it's a conversation that many of you in this room will continue to have.

Lesley Cowley: I have an easy answer. The Nominet in the UK are already involved in the initiative and we're looking to play and be informed by those discussions. I didn't see that any change to ICANN's agreement might be necessary result but of course it depends what comes out of those discussions.

Alice Munyua: I'd like to ask if our remote speaker Debra, Shaundra and Richard would like to respond as well. Shaundra you have the mike.

Shaundra Watson: Yes. I guess I would say personally I would support sort of any measures that are aimed towards providing more security for users.

Alice Munyua: Richard you have the mike.

Richard Boscovich: Well obviously any - I agree with that. Any measures that would increase security is obviously something that Microsoft would welcome. Unfortunately I'm not familiar enough with what the gentleman was describing to actually provide a good assessment. And maybe that answers the question as to I should in fact learn a little bit more about that particular measure that ICANN is planning on taking.

But like the prior speaker, if it enhances security, obviously I think it's - all ideas should be looked at.

Alice Munyua: Okay thank you. One more question, the last one please.

(Paul Horton): Sorry, at the risk of being boring can I just give a couple of perspectives from law enforcement, very simple ones. When being approached by law enforcement, please bear in mind that every minute is preventing and disrupting crime the safer incident and protecting the public which should be your drivers as well.

What I would also say is please bear in mind that you will have a lot more technical expertise and skills than the officer who is coming to you with any kind of request. So whether it be law enforcement or NGOs or anybody else, if you're going to say no, please explain why you're going to say no because they may be able to work through it and come through some of your processes.

And my final point really, with the - and if it's something you can remember, just try and find a reason to say yes rather than looking for a reason to say no. That would be my last point. Thank you.

Alice Munyua: Thank you very much. I'm going to ask the speakers if the - any one of them has any closing remarks? Debra?

Debra Hughes: I just want to thank all of you who have stayed. And thanks so much for the great questions. And I just hope that this conversation continues and would encourage anybody who wanted to speak further about any of the issues we had to kind of rush through, I had plenty more to say but I can give you more examples if there's more examples and people feel the need to discuss. Thank you.

Alice Munyua: Lesley?

Lesley Cowley: I'd say yes to a safer Internet. And I'm sure many other people will which if I go back to where I started, which is why some of the statements made in a more negative way were not very helpful this week. Many of the people in this community are very committed to safe, secure, stable Internets, absolutely.

Alice Munyua: Shaundra you have the mike.

Shaundra Watson: Hi. I'd just like to thank Margie for coordinating the panel. And, you know, I'm just very excited that you're having this DNS abuse forum and that we were discussing these issues. And I just look forward to reaching some cooperative solutions.

Alice Munyua: Richard you have the mike.

Richard Boscovich: Likewise, you know, thank you for giving me the opportunity to present today. On behalf of Microsoft we are excited about the fact that everybody's looking at the DNS issue very closely. And I just want to say we are as well.

And within the next several weeks, we will be taking even a more aggressive and unique action in this space with additional partners both in academia and in the industry to continue our work that we've began in Waledac and we see this going on for the foreseeable future.

Alice Munyua: Thank you very much. I'd like to thank all the speakers and specifically to Margie for having organized this session, to ICANN for having organized it and but beyond that for having presented an opportunity to (read capacity) awareness around this issue in our region through the workshop and this session, and to invite everybody for the same session in this - during the next cycle meeting in Brussels in June.

Thank you so much for your participation as well.

END