HYDERABAD – ITHI Workshop
Monday, November 07, 2016 – 17:00 to 18:00 IST
ICANN57 | Hyderabad, India

ALAIN DURAND: Well, good afternoon. This is the ITHI Session. ITHI stands for Identify Technology Health Indicator. We have a Latin name for this session today, which is DNS Sanitas: Sine Morbus. We will see we will use a little bit of Latin during the rest of the session. My Latin was a little bit rusty so I translated it to English.

There was another session this morning on health by GDD. This is a different effort. Both were started roughly at the same time but they're focusing on very different things. In this particular effort, we're focusing on technology metrics and not so much on business related metrics.

Next slide please.

The agenda for today, we will have an introduction by definition of health that I'm going to propose, and then we'll have a panel of discussions. We'll have Denise Michelle here, Laureen Kapin here, Lars-Johan Liman, and Jeff Bedsar, then we'll have an open microphone. We will finish that session at 5:55 sharp so we'll try to make the best use of our time.

Next slide please.

This project falls into the ICANN Strategic Plan from 2016 to 2020. This is a slide I took from kickoff meeting we had at the ICANN55 in Marrakech.

Point 2.1 in the Strategic Plan talks about foster and coordinate a healthy, secure, stable and resilient identifier ecosystem. That gave us a mission here on health and also the scope, which is the Identifier Ecosystem that ICANN helps coordinate. So we're not only gong to talk about DNS names but we will talk about any of the global identifier that ICANN helps coordinate.

Next slide please.

We started this project, we had a kickoff as I said in March in the ICAN55 in Marrakech and the number of community decided to join us but demanded to drive your own components so today we will focus fully on the name related side of it and we will have a statement from the NRO from a number of community at the end of my presentation.

In September this year, we had a workshop in our ICANN office in Washington DC. It was very interesting and a lot of really good discussion that went late into the evening so I'm glad to see the engagement of the community around these issues.

We had another workshop at M3AAWG meeting—or [Marg] depending on how you pronounce this thing—in Paris a week or two ago where we went into some of the details about this proposal on health and now we have the session here.

Next slide, please? Oh, just go back once.

I wanted to point that we have the website, icann.org/ithi in the associated mailing list so you can find information on how to subscribe to the mailing list on the website. The slides that I'm displaying here are also on the website so if you want a copy of the slides for later if you want to go and look at the details, you can find those slides there on the website.

Next slide.

The methodology for this project, we have decided to follow that recommendation that SSAC made in the document SAC077. When we look at this type of project with data, there's always a tussle there of some folks saying you first need to step back and define the problem, which is essentially what SSAC did and then try to compute metrics, or you can look at this for I have tons of data and it's like big data and we can use all kinds of new technology to go [inaudible] big data.

We've decided to follow the first approach as recommended by SSAC. In the first step, we will define health. That's what we're

trying to do today. Next step, we will go and figure out what can be measured within this definition of health and next we will go and get some data to compute those metrics. I do not underestimate the challenges to go and define #2 specifically #3, but first we are now at step 1.

The goal is to get a community consensus on this definition of health. Following this session and we will have some feedback, we may update this slide deck and then we will turn this into maybe a report, and we want to start public review comments probably sometimes toward the end of the month and maybe we run this till early January to really collect all input from the community.

So we will see there are lots of slides, there are lots of definitions, there are a lot of definitions, there are a lot of texts very specific. I don't expect you to discuss all the different bullet points today but this will be available for review.

The goal after that is by the next ICANN meeting, ICANN58 in Copenhagen, we will be able to move on to really defining those metrics according to some of the points we have here. And if we are successful, that we can start getting some data and track this over time, because at the end of the day the objective is not to say if something is healthy or not but to have this data that

characterizes health as we have defined it and to look at the trend over time.

If something has a number of 79 today, it doesn't matter much but if it goes to 81, 85, 92, this trend is an interesting observation. That's really where we'd like to go to.

Next slide, please?

So when you talk about defining health, I've had conversation with many people from the community, and if you talk to 10 people about health and defining health, you will get about 11 definitions. That doesn't really help us much. So I decided to go to the dictionary and I found a really nice and simple definition that I would like to propose today, which is health is a state of being free from illness or injury.

It has a couple of good aspects to it. The first one is very simple. The second one is we can make this evolve over time. We can define some of those illnesses or some of those diseases today and maybe a couple of years from now we can say this disease doesn't exist any more. It has been eradicated, great. Or this new disease now is showing up so we can start redefining a new disease and then go for this process again. So what we decide here doesn't have to be a static picture but it could be a dynamic picture that we will build over time. That's why I think personally Webster, it's quite interesting definition.

Next slide please.

So when we talk about health and disease, specifically disease, in the medical field, they have some specific way to look at this so I went to the Mayo Clinic—for those of you who are not from the U.S, it's one of the most well-known sites and actual clinic where they look at the complex disease and they have a lot of experience in that—and I looked at the way they describe disease.

This is a random example of Polio. I just stumbled on this one and for each of those diseases, they look at the definition of a disease, it's a short definition. When they look at symptoms, they look at the cause, they look at the risk factor, they look at the complications, at potential treatments, and a couple of other things. And I thought, "Wow, we can really use some of this and take the same approach, have a systematic approach to this and try for each of the disease that you're going to look at, describe them this way.

Next slide, please.

A couple of definitions to really wrap our minds about what this is. So what are the different categories that we are going to use in our taxonomy? A definition that's kind of obvious so it's a statement of the exact meaning. The symptoms are the sign of existence of something, something that can be observed. In

particular when we are going to look at metrics later on, that certainly will be a place where we can look at to go and define metrics.

The causes are the personal thing that gives rise to an action, a phenomenon of condition. Again, all the symptoms right inside I just picked up from the dictionary, I didn't make it up. So it's what creates a problem. Again, put the answer for finding something to measure.

Risk factors, that's an interesting one. The risk factor is something like a characteristic on exposure that increases the likelihood of developing the disease. This is not what creates the disease, it's not causing the disease but in fact increases the likelihood that you will have it.

So for example, you could say that smoking is a risk factor for some of the diseases like some lung complication and others. It's not the only cause but that's something that is certainly going to increase the risk.

Complications are a secondary disease or condition that is aggravating something that's already there. So you have one disease and if you don't treat it, you are going to develop another one that is more severe.

The impact is the effect of the influence of this thing and why we care about that, it's because that tells us why we are looking at those diseases. Why have we picked that disease? Is it that this is something that is going to create a serious problem in a particular part of the ecosystem, is it going to cost a lot of money, is it going to require people to build huge infrastructure, is it creating a criminality? So for each of the disease some other test for us, do we care about it or not.

And potential treatment is kind of obvious is the care that can be provided to the patient. What's important here is the keyword potential, not claiming here that it will work. It's something that could be tried and things get to be really important in some of this discussion that there is no claim that this will work.

All right, our next slide, please?

As I mentioned, we're going to do Greek and Latin because when you deal about disease, well, disease names are Greeks and Latin. The way it works is very, very simple, it's like Lego bricks. You just put together some root and some prefix and some suffix.

So sanitas means health, morbus is a disease, cine means without, so data cine morbus means data without disease. Malus means bad, nefar or nefārius is crime or criminality, magnitudo is magnitude or quantity. Perfluo is a leak or leakage,

Fallax means lying. What I found really interesting is when you have a name of a disease, by putting a suffix it gives it a category like is it an infection, is it a disorder, is it a condition or pain, so we can have a lot of fun with that.

Next slide please.

When we had this workshop in Paris, the first question that people asked me is who is our patient? Well, I want to be very clear here, the patient here is the system of unique internet identifier that ICANN helps coordinate. So that's the patient. The patient is not a particular root server or particular website. This is the unique identifier of systems – the systems of unique identifier.

Next slide, please.

There are a lot of slides in the deck. For those of you have downloaded it, we're not going to go through all of them. We have five diseases that we have identified, two of them that I want to go into more details before going to the panel discussion and two that we will simply scheme through.

The first one is datamalgia which means in Latin pain for bad data. Data means data, malus means bad and algia means it's a pain.

Next slide please.

We will define this as registration content server incomplete, inaccurate or fraudulent data. We're going to follow the same process or same taxonomy as we had on this Mayo website so symptoms, causes, etc. Next?

On this one I'll go real quick. I will focus on the next ones. So some of the symptoms will be contact information points to a whole new so none existing location of persons.

Cause – next slide.

Well, we don't have data. Some of the registrants don't have data. Something that's out of scope for this particular one is the use of privacy of proxy services.

Next one, risk factors. For example, one of the risk factors is there's not an agreed upon definition of what accurate means. Different people have different definitions for that, so that is a risk factor because that makes our task much more difficult. So we can go in all of our different bullets but for the sake of time let's skip to the next one.

Next slide.

Complication, that can escalate to abuse of the system which is the disease. We are going to go more into details so next?

Impact, why are we looking at this? Well, we're looking at bad data because public safety, technical or business communities have difficulties identifying people that are responsible for domain names. That's the impact to the society to our ecosystem that we have and that's why we're looking at diseases. The next one is potential treatment but I will not go into the details.

So that's how we're going to look at those disease. So let's look at the next one which is probably one of the most important for us here that we call abusitis which is abuse infection.

Next, definition of that.

Domain name abuse is the registration or use of a domain name with the capability to cause spam, phishing, malware, malware distribution or common and control of botnets. The very simple definition is something that creates things like that.

Symptoms? Symptoms that can [inaudible] just from that is the domain names are involved in phishing campaigns or spamming campaign and are critical to control botnets or to distribute malware. So it's a case where the symptoms and the definitions are more or less the same thing.

Next slide.

Cause of abusitis. All those bullets [have came] really from a discussion with the M3AAWG last week in Paris where we really fine-tuned all those bullets.

The cause of this is abusive and harmful activities are facilitated by the registration and use of domain names. There are some contractual and operational weaknesses, poor contractual enforcement in domain name registration process and life cycle. That's what recreates the root cause of this problem.

So risk factors, next slide.

Sometimes registrants cannot or are not able to or just simply don't discover at the time of registration the nefārius symptoms of the registration. So they look at something and it looks nice but actually it's not. They only discover that later so that's a risk here.

The use of privacy and proxy services has been identified by the M3AAWG Community as a risk factor. This is something that is authorized within the ICANN framework but that creates some risk. Similarly, incompetent complacent or complicit behavior of some of the actors like registries or registrar could be a risk factor. That does not mean that all registrars and registries are either incompetent complacent or complicit, it means that if some of them are then that will increase the likelihood of this disease.

Another one that was mentioned at M3AAWG was if the ICANN Compliance departments were to become ineffective, for example, because they don't have enough funding to do activities or the staff gets reduced or something like that, then that will be an additional risk factor for this particular problem.

Next slide please.

Complications. That leads to the other problem that we know well like phishing, botnet, spam, etc., so that's fairly straightforward.

Impact, we see those domains in anti-abuse list. There's a very large economical impact for merchants and there's consumer and damage to some brands, there's some erosion in consumer confidence, there's erosion in confidence in the DNS system.

The first one is more erosion into the confidence into a brand and the second one is more erosion of confidence into the overall DNS technology, and the last one is could lead up to some kind of fragmentation of a DNS if people decide, "Okay, we really don't want to talk to that part of the world because they have too many problems over there."

Potential treatment, again I want to stress this is potential. It doesn't mean that this will work. It could be some tools for screening automatically registration before it's actually put in

the system. It could be also more automatic responses after the abuse has been discovered. They could be accelerated procedure to take down names. They could be having in the Registrar Agreement or Registry Agreement some common language on anti-abuse because now some are governed by different types of contracts depending on when they have been created and that has been seen by the M3AAWG community as an issue.

Another point that was proposed by the M3AAWG community was setting up some universal minimum price. Again, none of this is guaranteed to work, we can certainly add to that. The idea is not yet to go later on and measure this but to give some perspective of what could be done potentially. Next?

The next issue I want to dive into is magnitudalgia. Again from Latin, magnitudo means quantity, algia is pain. So it's pain when you have too much traffic and typically that will be a DDoS attack, for example, but it does not have to be a DDoS attack.

When we had those workshops, especially the first one in DC, we realized that there are two parts of a community that is interested in these health things. One part is what we call the registration part. We have the names and we're going to put them into the DNS and it may have problems and may have to be taken down.

The other part is the people operate the network. For example, operating root servers or operating TLDs and things like that. And those people may be in the same company but they have a very, very different perspective. So what is important here is to try to get people from very, very different perspectives to talk together and try jointly to define these disease.

Next slide, please.

Pain from quantity. The definition is that you are seeing a higher volume of traffic than should be observed in an ideal world. In that case we are specifically talking about DNS servers but we could [in that] over servers too. Ideal means no more than a few queries per name for the duration of a TTL.

What has been observed is that on some of the root name servers and some of the top-level domain servers, there are a lot of resolvers that do not respect the TTL and send very, very rapidly sometimes multiple times per second or once every minute different ranges. They send the same query over and over again to the point that the number of really useful query is in the few persons. It doesn't mean that the others should not be answered to but it just means there are way too many than should be there. So that's not DDoS attack because it's always constant but that's a concern. So that's basically the definition of this.

Next.

So how do we see that? What are the symptoms of this? The symptoms is when we check the monitoring systems on all the servers and they detect higher than normal traffic. And other symptoms could be further down the road when there's even more traffic and the servers cannot handle this traffic, they start dropping traffic unable to sustain the load because?

Next slide.

As I mentioned earlier, many queries often sent at rapid interval asking the same question, ignoring the TTL. Sometimes it's hard to know if it is a DDoS attack or if it's something that's mis-configured. The last number of queries that are sent to non existent domain names, and of course when there's DDoS attack, well you just get lot and lot of traffic. But the point here is not just about DDoS attack. There's a constant level of noise that has been talked about and that is a problem.

The risk factors, next slide.

Things that have been identified in conversations, the prevalence of poorly managed open resolvers that just send queries and don't respect TTLs. Violation of this is misconfigured or buggy DNS resolvers so it could be a bug, it could be

misconfigured, it could be badly managed, different ways to somehow create the same problem.

BCP38 could be an issue. It's funny I wrote a sentence compromised IoT device maybe a week before we had the well publicized incident on DDoS attacks so created by IoT devices which was kind of interesting. But always are not a root cause of disease but it was a thing that increased the likelihood of a disease to appear that's why we call them risk factors.

Next.

Complications or what can go bad from this is when some names have may become unreachable and in some extreme case, if all the name server for specific names are unreachable and the TTLs have expired, then the name will not resolve.

Impact, next? Thank you.

Impact of this is the DNS operators have to build an infrastructure with larger capacity than otherwise. First off, they have to build a capacity that can handle all those extra queries that we see every day but they also has to build that extra capacity to handle DDoS attacks.

Treatment, DDoS mitigation techniques, excessive queries suppression, capacity adaption, all of these are really suggestions that have been made on how this could be handled.

I'm not sure if this will work or I'm not sure if this is the best way to do that. Maybe some work is needed here.

Next please?

I'm going to very quick on all the other two disease. That's the category of DNS transmittable disease. It's a disease that is not really a DNS disease but somehow it's there because DNS is play. The first one is perfluoism which means leakage.

Next.

This is when you have private names that leaks into the public name space.

Next.

This is, for example, when we have .corp, .mail, .home that are leaking out into the DNS.

Let's go straight to impact. Thank you. Why do we care about this one? Well, that's because those strings like corp mail become problematic and it cannot really be used now without medication in the global DNS.

Next disease.

That's my favorite name, datafallaxopathy which means lying disorder about data.

Next.

This is when responses from DNS resolvers to queries contain unauthorized, forged or tampered data. We have seen that in a number of places where the resolver points to the wrong place. So we're not talking about parental control here where parents may say, "No, we're going to block this device, this site." We're talking about modifiers usage where some example a resolver will point to website to one of his competitors.

Go to the impact, please? Thank you.

The impact of that is loss of business, again financial losses, loss of confidence in the DNS systems. So this is fairly serious and that's why we're looking at those disease.

Next.

So those are what we have looked at in the name space, the DNA name space. In the number space, our colleagues from the IRR have been starting some project on this and they have decided to run their own project regarding this.

Next slide.

We got a statement from Oscar Robles, the CEO of LACNIC and he's the current Chair of the NRO and now being the Number

Resource Organization which is essentially the CEO of the five IRRs together.

I'm just going to read the statement. "Currently the NRO through the Registration Service Coordination Group is working on the analysis stage of this project" – so essentially what we're doing here – "and have identified several steps to complete this work and join the RSCGs of the Registration Service Coordination Group face-to-face meeting that will be held late November in the AfriNIC meeting, which will in two weeks from now. They will review this project definition and work on risk identification steps and they will share any relevant finding after that meeting." So they have started the project and will come back to us.

Next slide.

So that's it for my rather long introduction but I wanted to really go through the methodology that we had and now I will turn over to the panel.

So next slide, please.

We have four panelists. We have Denise Michel from Facebook – former Domain name Systems, Strategy and Management at Facebook. On my left we have Laureen Kapin who's an attorney practicing consumer protection law at the U.S FTC and a

member of the GAC Public Safety Working Group. We have Lars-Johan Liman over here, Senior Systems Specialist at Netnod and a long term member of RSSAC. And we have Jeff Bedsar, CEO at iThreat Cyber Group and a long-time member of RSSAC. I'm very happy to have somebody from SSAC, RSSAC and PSWG to come to this panel today and give us their impression of this work and where should we take this. We will start with Jeff on my left.

JEFF BEDSAR: Thank you, Alain and thank you very much for putting this together. This is really creative framework that I really—it's nice to be able to put a framework around terminology because there is a lot of cross termination confusion. It really does put it in a nice framework to help.

The topic I just wanted to hit on is that there's one really important aspect to make this work and it's data and it's data from a bunch of different sources. The only way this going to be successful if we can get the data from numerous sources or if we can get the data from the providers of services that basically we can say that inaccurate, WHOIS and other things that would demonstrate some lack of health somewhere.

We're going to be able to define things to your terms from injury to illness and injury might be something that's done purposefully. So if someone is registering domains to commit a

fraud or abuse, first as someone who has compromised a domain for fraud abuse so that's more of an illness. You've been infected by somebody else.

So we need to be able to have sources where we can get authoritative abuse and badness data so that we can effectively measure where the problems are, where the illness and injuries are so we can look to measuring them in a way that gives us an ability to fix, to solve, to cure.

I think this is a really good step toward a framework where you can start understanding [inaudible] the illness. You can start solving by understanding problems that affect TLDs directly and registry operators. You can understand the problems as they affect the registrars and you can understand the problems as they affect regions and you can start to measure. But every type of data source is going to be coming from different places and they have to have a set standard of authoritative agreement that yes this is a source of data on spam that is agreed upon to be the authority that they are right most of the time, and I guess we may have to determine how much right at the time – most of the time means.

Like for example, if it's a provider that measures spam and says, "This domain was spammed today and will be spammed tomorrow," was not hosting spam tomorrow, then we can say

that, “Well, on that day temporarily it was and on that day temporarily there was an issue and if we can measure up temporarily with incidents of traffic issues with DDoS, with use and registration and volume and bulk, there’s a lot of different factors here but a framework that lets you understand how they impact each other temporarily and you break it down by different types of stakeholders – registries, registrars, ISPs, etc., you can really start tackling this problem nicely by having an understanding of the problem, which goes back to your SSAC007 which is basically defining the problem.

Now we understand the problems both in terminology. Hopefully, we can adapt this, actually I kind of like this health version. We can adopt a common definition of the problems so we can do a common definition of how they’re impacting where the data comes from and that gives us the ability to try and work out yours.

ALAIN DURAND: Thank you, Jeff. Denise, provide us some feedback on this. What do you think?

DENISE MICHEL: Thanks, Alain. I thought it was a very comprehensive proposal and it dovetails with stated priorities of not only Facebook but

business constituency and the three commercial constituencies. We've had the need for data and analysis has arisen several times this week in discussions with the commercial constituencies for a range of reasons, so we're really pleased that this project is getting underway.

I think our only concern is the pace. We're quite anxious to have this data and this effort in the public sphere as soon as possible so we would want to make sure that it has the priority attention and resources that it deserves to stay on track and we're hoping to see the initial results early next year.

I think the one thing in that vein that I would want to ask a question about and raise a concern about is it wasn't clear to me that you would actually have access to the number data. I wasn't quite clear what the correspondence from the NRO Chair actually meant and if it indicates perhaps that they're still considering whether they want to cooperate and provide IP address related data. I think that's something that should be addressed. Well, I think it's something that should be addressed at the Board level. Since the IRRs have an MoU with ICANN, they have a joint responsibility to address global policy in the IP address space and the IRRs have a responsibility to provide advice to the Board on a Number of Resource Allocation Policy.

I think this project and the provision of data in their space to support this project is quite critical so I would suggest that this be elevated to the Board level and that the Board communicate with the IRRs and through the NRO and ensure that there is the appropriate amount of cooperation for this critical project, thanks.

ALAIN DURAND: Thank you, Denise. Laureen?

LAUREEN KAPIN: Thank you. Thanks for inviting me here. Can we go back to slide 20 please? One of the things that I was happy to see was the scope of the DNS abuse definition here, particularly the inclusion of spam because studies have shown that spam is the delivery mechanism for a lot of malware, phishing attempts and abuse in general. And I know sometimes that there are different perspectives about what is within or outside of ICANN's remit but in terms of including this data, I think you must include spam and I was gratified to see it there.

And also I wanted to emphasize at least from my perspective why I think it's within ICANN's remit and that really flows from the base Registry Agreement, which has a provision on

mitigating abusive activity and I'll just read from that portion of the Registry Agreement.

"There's a mandatory requirement for registry operators to include in their registration a Registry/Registrar Agreement, a provision requiring registrars to include in their registration agreements with prohibited registered name holders" – so this is a downstream agreement – "registry to registrar, registrar to name holder provision that prohibits distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices counterfeiting or otherwise engaging in activity contrary to applicable law."

So that's a really broad definition that covers a broad range of abuses so my view is that spam fits squarely within that particularly when we know that spam is often the delivery mechanism for a lot of abusive conduct including phishing and malware. So that's my first reaction, which is a good one. And also I would urge as this project evolves that the information that's obtained be available to the public. That there is transparency here so that all this helpful information about abuse levels is collected, that the public has access to that information so they can use that as a tool to decide where they're going to travel on the Internet, how they're going to conduct their transactions and behaviors.

So thanks for including me and I'm really looking forward to seeing how this evolves.

ALAIN DURAND: Thank you very much, Laureen. Liman, and after that we will take some questions.

LARS-JOHAN LIMAN: Thank you. So I'm Lars-Johan Liman, I work for Netnod a small company in Sweden and we are on the operational side of this Internet. We're operating for the structure services so we are actually—I wouldn't say one of the targets but we are collateral damage in much of what happens here. We see—I won't say daily but frequent attacks where our systems are involved, not necessarily on the receiving end but often on the reflecting end. I think this is a good effort. I welcome any effort to try to mitigate the abuse problems that we have of different kinds of Internet.

I think there are a couple of things. I see the patient not as being the identifiers only. The patient is the Internet ecosystem for me and if you have a limited remit, which ICANN does, you are a specialist doctor of a certain part of the body and doing your work on that part is a very good effort but you have to realize that there are things beyond that as well. But do what you can with what you have at hand is absolutely commendable.

I am very much a proponent for looking at – when it comes to health issues to look at the underlying causes. If you have a pain in your back and you go to the doctor and he just gives you a pill that kills the pain, you haven't solved the problem. But if you go to someone that says, "Oh, you're carrying a shoulder strap bag. That would kind of turn your back askew." So if you go out to carry a backpack instead, you can solve the problem long term. Maybe you're going to have the pain a bit but eventually in the long run you would actually solve the problem. So I would very much urge you to look for that type of factor underneath when you start to dive deeper into these problems.

And one thing I think we have to work with is to understand how money flows with these abuse systems. If we don't understand where the money is, we have no chance of fighting the systems. So the real challenge is to understand the black market money and also to understand at the other end how can ICANN via policy and contracts help mitigating that and prevent the bad operators of various types of systems and [inaudible] from actually earning money on the Internet.

One aspect of that is that with excessive traffic volumes, the players that provide services at different levels on the Internet have to overprovision. We just learned this morning – and then this is numbers that are easy to confirm for me back home – that virtually 75% of the queries that hit root name servers are crap.

They are queries that should never have appeared at a root name server. That means that only for normal traffic levels, we overprovision by four times over what we should have do and that's even before looking at various types of focused attacks.

And that's actually a financial problem in the far end. We have to pay more money to make these services work and that money that always comes from a single source, the end user. There's no other entity that pays, that you can always trace the money back to the end user.

And we also from one angle—I want to stress this very carefully. From one angle, actually this abuse drives even wide business because we have to buy more hardware in order to provision for this so the hardware producers actually earn money from the fact that we are the target for abuse in a way.

That is one angle of it and I want to stress that. I also think it's very important if we are going to succeed well in any way, we also need to maintain cooperation with others. No doctor that has a narrow focus on the body can succeed to heal the entire patient when you have a problem that permeates the entire body, so it's very important to maintain an open attitude towards other players that try to work and approach these problems. Thanks.

ALAIN DURAND: Thank you very much, Liman. Now I would like to [inaudible] our panelist to have spent time to look at the slides and come up today and provide the feedback. We have a few minutes. Five minutes about and so I would like to open the floor for questions and we had questions or maybe a comment from Alan.

ALAN BARRETT: This is Alan Barrett from AFRINIC and I'd like to comment about the NRO. Firstly, the ICANN Board has absolutely no jurisdiction over what the NRO chooses to do. We have an MoU with ICANN. We intend to comply with the terms of that MoU. We have agreed to work on listing some aspects of IP number health that might be useful to this project. We don't yet have that list but we are working on it.

UNIDENTIFIED FEMALE: Thank you. What does it mean providing a list? Is that a list of the data that we'll be providing to this project and are you so satisfied that this will be advanced through the IRRs?

ALAN BARRETT: We're still thinking about that. We'd like ICANN to do things that it's asked to do by its community and perhaps the DNS community has asked ICANN to work on these DNS health things. The IRR community has not asked ICANN to work on IP

address health things but nevertheless, we're willing to cooperate.

UNIDENTIFIED FEMALE: Great.

ALAIN DURAND: Thank you. We have another question here.

UNIDENTIFIED MALE: We've had Warren [inaudible].

ALAN BARRETT: Okay, can we get back to slide 20? I wasn't originally going to mention this but seeing that someone else brought up slide 20, I'm assuming that on it you actually mean intent not capability, because I'm not quite sure what you mean by a registration of domain without the capability to do that so I just wanted to make sure it is intent which is very hard to figure out.

ALAIN DURAND: That's an interesting question. There was a really long discussion which we had in M3AAWG in Paris about the word intent or not. When you talk about criminality, you have to – from what they have told me – demonstrate two things: One, the

actual arm, which is relatively easy to do. The second one is proving the intent. And from what I understand from people around me is this is really, really, really hard to prove the intent. That is the reason why we have tried to refrain from using the word intent in this definition here.

ALAN BARRETT: But don't all domain names have the capability to send spam? You can't create a name which doesn't have the ability to send spam so capability also isn't what you're aiming for here.

ALAIN DURAND: So I think that we will welcome some suggested texts here. Next comment?

JAY DALEY: Thank you. I really like this as well. I am not sure if you are a genius or crazy but I really liked it. Sorry, my name is Jay Daley from .nz. I just wanted to echo Liman's point. There are two of your conditions that I think are too broad – the pain from the data and the pain from the volume. I think that with more thought we can get more specific issues there and possibly more rather two actually split out to more than that and that would be more useful for us.

ALAIN DURAND: Could you elaborate a little bit what you mean by being more specific.

JAY DALEY: If we could go to the one for the data one, the dataitis or whatever it was, I'm sorry. I did actually do Latin and ancient Greek for many years but I have forgotten it all now. Yeah, the pain from bad data, datamalalgia. Incomplete data is an irritation but it is very, very different from fraudulent data and I don't' think putting the two together is helpful at all.

I think that this data needs to be split out. In fact incomplete data is a minor irritation in comparison to deliberate fraudulent data.

ALAIN DURAND: We had a number of presentations from the public safety law enforcement community. I remember in some of the IRR meetings recently you came and explained that sometimes the data is incomplete in fact makes our life really difficult and that's somehow why it was put in there. But I get your point, maybe we need to separate this into different variations of the same disease, maybe different gradation.

JIM DALEY: They may actually be very different diseases. I think if you take out incomplete data and work through the rest of your model based on incomplete data then it may look quite different. I don't know. I'm sorry I haven't done the work but just in terms of the way that I manage things within my registry, those are very, very different things.

ALAIN DURAND: Very good feedback. Thank you very much. We have time for one last comment.

[DANIEL MIGO]: I was just wondering if we had a complete view of all the different symptoms.

ALAIN DURAND: Would you mind introducing yourself please?

[DANIEL AMIGO]: [Daniel Amigo] from [Erickson]. My question was I'm not sure that we have a complete view of all the different symptoms. And for example, the one that I was thinking of is when we talk about the quantity of traffic. To me for the Global Identifier Ecosystem if we have names with no data and no traffic, it might be also an

issue because they are just taking some space within the names. So the thing is that I was wondering if we know the passion but we have kind descriptions of all the symptoms that can be observed?

ALAIN DURAND: I think it goes to a point I mentioned earlier. We're not going to have an exclusive list of disease. That's the starting point and we may have to add more disease and to your point we may have to split some disease into different sub-disease because they're actually different in the way people are handling them. But I don't think we will ever come to the point where we have a completely exhaustive list of disease.

[DANIEL AMIGO]: Okay.

ALAIN DURAND: Well, thank you all very much. This is will be the end for this meeting. Again, we have this ITHI mailing list that you can subscribe from the website. I will encourage you to do so. The slides are published over there and we will soon have public comment period on this and I will certainly encourage you to participate and provide feedback. Thank you again for participating today.

**[END OF TRANSCRIPTION]**