Heather Dryden:	Okay, first of all I would like to thank the Security and Stability Advisory Committee for coming to meet with the GAC on this topic. We had an interesting exchange, I think last time around, and I understand you have some work to report on today, and that you have a presentation to provide. So I will turn over to Patrik Fälström, who is the Chair of the SSAC. Patrik? Of course
Patrik Fälström:	Thank you very much, Heather. Patrik Fälström, Chair of SSAC; I'm here to have – I think this is the second meeting that we've had together, and I heard positive input from the previous meeting that we had two ICANN meetings ago, and fortunately having interest from you in GAC to have more meetings with us also; SSAC members have expressed their interest of having more interactions with not only you of course, but also other stakeholder groups, just like they report in San Francisco.
	I would like to just, instead of just – I was thinking of skipping the introduction of every SSAC member, but just because I think it's important to all of you in GAC to be able to reach out in as easy way as possible, not that we have a problem with that now that we're meeting here in Singapore; I would like to ask the SSAC members that are in the room to stand up please.
	Stand up so you can see the ones standing, these are the ones you can reach out to if you have more questions; and the GAC members are standing up so you can see who they are as well, so

you don't have to talk to them, though. So with that as a short introduction of SSAC, let me immediately dive into the document, SAC 50, that we released today.

We got a question a couple of months ago, from GAC, on what indications on the security and stability blocking of DNS would have. Based on that document, we wrote this response. One of the reasons why we didn't say okay, it is bad or it's not bad is something that we tried to outline in the document. In reality, next slide please, any kind of blocking used in DNS is actually involved in altering the responses to the domain name system, and that can happen either when the query is on its way to DNS server or when the response is coming back.

It is quite often done by doing some kind of intercept of the DNS query, not in a hostile way, but the DNS protocol itself is built upon a number of queries and responses being sent where, to start with, a client with a laptop in this room is sending a query to a local DNS cache that is like on the local network or at your ISP or in your home router that you have at home, for example. That intermediary is repeating the query and sending it to various other DNS servers in the world, and when you intercept or alter the response from the DNS server, that is normally happening in one of those boxes.

So it's not interception of the actual DNS sort of queries on the pod, it's actually happening in those cases which have to do with it, which is there by design. This kind of blocking or altering of the DNS response is something that is happening more and more, and

one of the cases where these things happen is, for example, often in the home router or even in the anti-virus software that you have in your laptop itself. These are cases that normal people can think "Well, it's probably good if my anti-virus software is actually doing something." But on the other hand, if it is the case that we are doing blocking globally on the Internet, everyone understands that that might actually have quite a lot of impact.

And the difficulty here is of course to, with blocking your DNS, just like any kind of technical approach to anything you do, there is both benefits and harms, and what they're trying to explain in this document is when talking about the blocking of DNS, there is a balance calculation to make between the benefit and the harm of doing the blocking.

So another thing to point out, apart from the difficulty of making a balanced calculation of the benefit versus the harm, one must know that if it is the case that you prevent some progress resolution into an IP address, that doesn't sort of completely prevent the end user from being able to reference or access the information that is available via some protocol to that IP address, because other domain names other than the one you just used to look up could be used, or the IP address itself can be used.

And this means that if it is the case that you block by preventing the lookout for the translation for domain name's IP address, that will prevent an immediate connection to the main host, but it will not make it impossible to access the information. That means that if it is the case that the goal of the blocking is to prevent access to

information that's referred to using the domain name, using DNS blocking is pretty ineffective, which basically means if you have a problem to solve, using the DNS as a solution to that problem is probably the wrong solution.

If you want to prohibit access, other mechanisms are more effective. So for example, as I just said, if you have a mapping from one domain name to an IP address and that domain name is blocked, it doesn't stop anyone to allocate another domain name referring to the same IP address, and if people use that domain name, access to the information is, of course, doable.

So circumvention is pretty easy. So it's very important, because of this, when doing the calculation of whether you are going to do something, or someone that is in this equation of may be doing something like DNS blocking, it's very important to think about what the potential collateral damage is, and what kind of cost it is compared to the benefit.

And the document talks about, in general terms, that the broader community that some kind of filtering, or in this case blocking DNS has, the higher the risk that there will be secondary effects that can be pretty big, compared to the fact that the broader impact it has, for example, that's blocking, the easier it might be to circumvent. So because on a global level it's much easier to, for example, allocate another domain name in another top-level domain, or whatever; use the IP address for the access to the information.

And to summarize, if you look at the slide on the screen, the bullets, the last bullet says that "to be able to keep the stability of the internet and enable the security that, for example, DNSSEC and other mechanisms are enabling, it is very important that everyone that is in a situation, so they can impose for example, a block on DNS, that everyone together make a concerted effort to do no harm for networks and users outside their policy. And once again, the bigger and broader the implications are, quite often, in most cases, lower effect, higher risk. Next slide please.

So once again, and this comes back to basically, this is a principle that is used in sort of all the time in the technical community, and when we're looking at various things we deal with, the DNS and with the internet, is to consider the possible harm. To some degree, that might make us technical people look very conservative, because we say no to everything, but on the other hand the reason that we're doing that is because before we do any kind of change, regardless of the kind of change we do, we are trying to look, very carefully, at what kind of possible harm some kind of a change is making. Next slide please.

So to conclude, if we look at the DNS blocking, it is the case that all technical approaches to DNS blocking will have an impact on the security and stability of end users and applications, and that do have an impact on the universal stability of the name space. And this is sort of the conclusion of – and this is one of the reasons why anyone that can do blocking will have to be very careful of doing these sort of changes to the view of the name space that the domain

name system creates, within the organization, the inside organization, or within the area where there is responsibility for the potential blocking. Questions?

Heather Dryden: Sweden, please.

Maria Häll: Thank you very much, thank you very much Patrik, for this very good presentation. Just one question; you said that the higher – the lower the effect, the higher the risk. Do you mean the higher the harm? Could you please just explain it a little bit? I interpreted it like the lower the effect, which doesn't really work, because you could access the information via IP address or whatever, but then it's the higher the risk. Could you please explain it once again please?

Patrik Fälström: Sure, the impact of blocking, if it's higher up in the name space – or the higher up you try to do the blocking on the internet as a whole, the higher the risk that it will impact third parties, or the ones, for example, that you didn't intend to impose the blocking on. Let me phrase it that way.

So for example, it might be the case that if you try to do blocking on a big scale on the network itself, for example, outside your own department, if you have like your own home router; if it is the case that you are blocking on an ISP or something, you don't really

know if there is some transit traffic or something, which is also affected by the blocking, etc. So both network topology wise, but also name space wise, the more broad the blocking, the impact of the operation has, the higher risk that you might hit third parties. Let me put it that way.

Heather Dryden: Thank you, Patrik. Italy please.

Stefano Trumpy: Thank you, I think that the main concern why we are discussing this argument is connected to new gTLDs, and of course we would like to know how you see the problem regarding this particular – so we learned that different levels of blockings fit – or whatever are already in place, so they provoke some damages to the global accessibility and internet.

And I wonder if you can talk a little bit – of course in the GAC, it will be involved in the evaluation of new gTLDs and especially those that to our opinion could provoke some negative opinion of different governments, and I wonder if -- you have been talking about the difficulties realized in blocking of a TLD, a successful one, and I wonder if talking too much of this fear of blocking could end up encouraging the governments that do not like a certain new gTLD, to declare that they will block it.

And on the other side, of course, the GAC is preoccupied with the collateral effect of this blocking, possibility of blocking, and these

cases they could recommend the Board just not to approve these kind of registries that could provoke a negative reaction starting from governments. So I would like to have your view looking at these specific cases, and maybe you can elaborate a little bit what has been done in the case of Egypt: when they restricted the registry the access to .eg was blocked.

Patrik Fälström: Let me try to explain a little bit on what might happen when, for example, you picked an example of a top level domain that is blocked. It is correct that there are some cases where top level domain is blocked, and there are various views as to whether that actually has an effect, whether it has an impact on stability and resolvability or not.

And this is why I'm a little bit careful here, because we are in a gray zone, and if you ask a couple of different people, they might say – if you force them to say black or white, yes or no, they might actually say different answers, but I think everyone agrees that if it is the case that blocking is happening, that actually means that certain domain names are not resolvable from certain locations on the network.

That's what's happening. Given that we are moving towards using more and more cloud services and more and more services that we ourselves do not really control, it's harder and harder to know what that actual impact is, and we are more dependant on global resolvability. If I take a very popular service like Twitter, for

example, it's very popular to use a URL shortening service in Twitter which ends in an ly, top level domain for Libya. And that means that even though I am twittering with other friends in Sweden, if it was the case that the Libyan top level domain would be blocked, that would impact the ability for me and my friends to Twitter with each other, even though we're doing it in Sweden; even though we're using a service that is provided by a US organization, etc., etc., etc.

So the number of sort of connections here and there, both regarding the natural topology and the actual domain names used is more and more global, and because of that we want to have more and more global resolvability and global reachability. The other part, the other thing has to do with – you mentioned the interest of blocking a top level domain, and this comes back to what I said about okay, the question is then what is the problem that needs to be solved. Is it access to information that's referred to by domain names in that top level domain, or is it the top level domain itself is a sensitive string that cannot be used.

It is very important to separate those two problems from each other. And as we point out in the report, and I did on one of the slides, the ability to resolve, for example, a domain name to an IP address, just make it harder, not absolutely impossible to access the information that is referred to with the help of that domain name. So if it is the case that the information that potentially is supposed to be used by the domain name is referred to by a certain – domains in a certain top level domain, I can say that from some

point of view, using blocking the top level domain to stop access to that kind of information is not very effective, or different grades of effectiveness. And by the way, I am the only one talking here, but if other SSAC members want to whack me or correct me or come with more proper input, please raise your hands.

Heather Dryden: Thank you, Patrik. New Zealand, and then the Netherlands.

Frank March: Actually, I think Patrik has already dealt with my question extremely well, which was going to be what is the different impact of a top level domains as opposed to blocking at a lower level of the DNS and I think that answer comes very completely. Thank you.

Heather Dryden: Thank you, New Zealand. Netherlands.

Thomas de Haan: Thank you Patrik, and the SSAC for this report. Although it's very short, I think it gives a couple of new insights for me, at least, and I think one of that is that blocking is in itself not bad or good. I think it depends on the purpose; it depends on the way you implement it. So, I think that's a signal which we should take – I mean, we block also in Netherlands.

I mean, it's not only you guys who block but we block also in the Netherlands. One thing which I really cannot grasp yet – and this is for me – it's not sufficient, to be honest… Let's say we go out from the good scenario that SSAC and others recommend this kind of blocking in the way you say it with the right techniques, only affecting own users. Do it in a way that doesn't harm others.

Okay, that's a way of doing good blocking, let's say it like this; and I think if countries are doing this, I think for their citizens it's good because they are protected from something their government or their culture think it's not good for – let's say, it can damage. So, I think that's a positive implementation of this. On the other side, I think I don't get enough grasp to indicate the kind of impact - the volume – of harm which it can cause, because you can have one country blocking, you can have ten countries, and to be honest with you I cannot – as GAC member, say don't.

For example, I can more reject this, because there will be blocking that will lead to – let's say – I don't have any substance yet. So, one of my answers, or maybe a way out, would be- this is more getting into the sensitive strings as Stefano said because basically the reason why we want to know this. What I would say is every application has its own merits, its own risks. What I would say is that as GAC, we are not experts.

We cannot judge the effect of blocking. What I would – maybe it's an idea that I would launch, is that given a certain string which is sensitive, we should ask SSAC for specific advice, what the impact is on the stability and security instead of do it for, in a general

matter without really having real substance on what kind of harm it is. So, that's something which I want to put in the group. I think it's important that we think about this also as GAC.

Heather Dryden: Thank you, Netherlands. Patrik, did you want to comment on that?

Patrik Fälström: Yes, a short comment. It's impossible for SSAC to say what kind of harm it has, as well, a specific string. What we can do, though, is just like we did with this question. If it is the case that you have a specific problem to be solved, we can do a technical evaluation to say whether that problem is solved or not; because there is an underlying problem that is the resolve rate, and without that kind of more specificity in the questions it's very hard for us to answer.

Heather Dryden: Thank you, Patrik. I have the European Commission and the United States.

William Dee: Yes, I'd also like to join those who thank the SSAC actually for thanking the time to produce this report; it's so useful. I have to say, I think it was the Commission who first raised it in June last year at the GAC meeting, actually, and another context, which you'll be familiar with, and I found it very useful. I see the report itself provides some – I think – some very useful principles which

– how you get third parties' respect principles, which is another issue.

That's a challenge for all of us, I think; but it says that when these principles are not applied, blocking using the DNS can cause significantly more collateral damage or unintended consequences with no remedy available to affected parties. I appreciate the explicitness of that advice, actually, because that confirms our view that blocking can cause serious harm and I have been challenged in the last nine months on that, saying there's no evidence actually that blocking could cause harm.

So, I thank you very much for being very explicit in your reply. Just a procedural question – I hope you don't mind me asking this but it's just an issue that we've had to raise – and did the Board at any point ask the SSAC for advice on blocking?

Patrik Fälström: No.

William Dee: Thank you very much.

Heather Dryden: Thank you, European Commission. United States.

Suzanne Sene:	Thank you very much. I, too, would like to – of course – express my appreciation as well for the SSAC for coming in and taking the time and meeting with us, and for your very helpful report; and your responsiveness to our questions.
	I'm going to follow up, I hope, on what Thomas was raising; because I think this is an issue that we are trying to understand better and get our hands around. If we have – you know, it's one thing to understand that certain strings are triggering or may well trigger individual countries to say, "This is offensive to me, I'm going to block it." I think what Thomas was getting at, and I hope I understood him because I agree with you – it's something we are trying to get our hands around.
	How do we best go about trying to understand the cumulative effect of multiple countries seeking to block, whether one string or five strings or fifteen; because that is a challenge we are going to be faced with as we understand the process. We, like everybody else in the community, is going to be looking at whatever lists of proposed strings there is at a given point and time. And so, under the agreement that we have now arrived at with the Board, there is an early warning system.
	We have only 60 days to nationally check this list – you know, consulting capitols – and then we come together as a group. We kind of consult as a GAC. There can be an individual country early warning objection or it can be multiple. So if, for example, one of those early warnings, or two, or five, or ten potentially do not give rise to the next possible step, which is a consensus GAC advice

that suggest strong objection and the string gets approved. So you have one, five, ten countries saying, "I don't like these five, or ten strings. I failed in the early warning process. I failed in consensus. I still don't like it; I'm going to block it."

So I guess – and Thomas, tell me if I'm totally crazy and I'm misunderstanding you. We're trying to understand, ultimately how do you measure – at what point does this kind of incremental blocking – I may be using the wrong words – become like absolutely, fundamentally damaging. Or is that – are we not using the right terminology here? I guess we're trying to understand – is there a trigger point? Thank you. I better stop now because I'm not going to make sense much longer.

Heather Dryden: Thank you, United States. Would anyone like to respond from the SSAC? I can move to the next speaker if you'd like a moment to contemplate that? Okay, so I have Sweden next, please.

Maria Häll: Thank you very much. Well, I think that two aspects – and correct me, Patrik, if I'm wrong - because one problem could be actually the security and stability and harm blocking could make on a technical level.

I mean, for instance the use of DNS second and other aspects. But there are also, which you also mentioned, Patrik, by bring up your example, but .ly TLDs, it's like reaching information and that

might cause problems on the freedom of speech and getting your access to information.

So I think you have two problems and I know that you, or SSAC, is focusing more on the technical things, but on the other hand in your report, you absolutely get the feeling that there might be other, more that kind of problems about reaching information. So, is that correct analyzed from my side? Thank you.

Heather Dryden: Thank you very much, Sweden. Patrik, would you like to --

Patrik Fälström: The first I will answer the question from United States. No, it's impossible to say a number that at, when you pause at nine, that's too much. Okay, it has to do with…. Well, let me take a step back and say one of the first things that this report is saying is that if using a blocking is first of all probably a tool that doesn't solve the problem you have, and anyone that has the interest of blocking probably has some kind of – there is some attempt with the blocking itself.

The second thing is that the effect is different, and you calculate the effect differently depending on whether the problem and the intent is to – as I said – try to prevent access against access-free information this string is referring to or wither the attempt is to block the use of this string itself; which means that when you put

in the effect in this calculation on benefit and harm, you put in different values.

And that's one of the reasons why, for example, it might be hard to say, like, if this specific domain name or something is blocked it has more to do if this domain name is blocked for this purpose, what is the actual effect and what is the benefit and what is the harm, etc. Then, it might be possible to do some kind of estimate – maybe – or something.

The second thing, to answer what Sweden was pointing out; yes, we are referring not only in the document not 100% to technical instability. We are also, just like all of you, following the discussions – for example – in the Human Rights Council and the work in the IGF regarding freedom of speech and openness, and what the special rappateur freedom of expression is saying.

But to what we have been looking at from a technical and stability point of view has more to do with the ability – for example – an individual to always reach their e-mail server and fetch their e-mail regardless of where they are in the world when traveling and the ability for business to get customers all over the world and what kind of potential technical blockings there are. That's where our focus lays on doing that kind of calculations. Thank you.

Heather Dryden: Thank you very much. Norway?

Ørnulf Storm:	Yes, thank you. I also want to give the appreciation of SSAC being here to share this information with us. So, just an observation; so basically what you may be saying is not – of course – the blocking method that would probably cause less harm would then be to block on the protocol level, like on the end-to-end protocol with a deep packet inspection probably and not use the DNS as a blocking tool, and just leave the resolvability and have all the domain names being resolved and then just do this deep packet inspection and block on protocol level regardless of what end-to-end protocol is used. So, that would be sort of one way to do that, of course.
Heather Dryden:	Thank you, Norway. Did you want to respond to that, Patrik?
Patrik Fälström:	What we are saying is that you should try to make sure that you are using as surgical a mechanism as possible to solve the problem that you want to have solved. And what we're saying is that block in DNS is a pretty bad tool to use for most problems that we at SSAC have seen to when we have been writing this report. So, that's as far as we have gone in the works that we are doing at SSAC.
Heather Dryden:	Norway?

Ørnulf Storm: Thank you. As you have pointed out, of course, also the report is about maintaining the universal resolvability for the DNS which is also a point in itself. So, yes, thank you.

Heather Dryden: Thank you, Norway. So, I have a question. I will defer then, if the United States – okay then. My question was more about what happens next with the work of the SSAC. So, if we're ready to move to that question, please? Egypt, would you like to make the comment first?

Manal Ismail: Yes, can I just ask a very quick question before we move to yours? When you say blocking, is this one-to-one with filtering or is filtering something else that comes later, or?

Patrik Fälström: Well, DNS blocking is one kind of filtering, so the term filtering from a technical point of view must be used in a specific context, that you filter traffic, you filter a specific application, you filter a subset of the whatever commands in an application, you filter part of the DNS lookup. So, just filtering is – for us technically – you need to have more context to be able – they are two different terms so it's hard to really answer your question there.

Heather Dryden: Thank you. Egypt? You okay?

William Dee:	Just a quick question. Can they both have the same effect for a top-level domain, filtering and blocking? Could they serve the same purpose, I guess is the question.
Patrik Fälström:	DNS blocking is filtering applied on the DNS protocol. You can have other kind of filtering applied to other protocols, including the IP protocol, the mail protocol, and whatever. So you cannot talk about filtering or DNS blocking, because filtering is - I think what you mean is – with filtering is to block access on an IP level – for example to certain IP address. That might be what you mean when you say filtering. Is that correct?
	Blocking access on the IP level is something that has a different effect, much different effect, then blocking on the DNS level. This is not something that we have been looking into within SSAC, just let me make this clear so I'm just speaking as an individual here, but it is the case that if you block access on the IP level, that of course makes it impossible to send IP packets to that destination where the IP address is. And that has much different impact than make it impossible to resolve a domain name to an IP address.
Heather Dryden:	Thank you, Patrik. In terms of the work that you are carrying out, what are your next steps?

Patrik Fälström:	The next steps. Well, the process that we have in SSAC is that we are triggered by some events and then we might right a document, like within this case. And when the document is written, it's out there and we hope that people pick it up. So, we don't have a need, so the next thing we might do is something else, a follow-up or something.
	But that needs to be triggered by some kind of event, either internally inside SSAC or based on – for example, generate feedback or something like a session like this, or that we get direct questions from GAC or other groups. New questions which then are triggered into other documents. That might be follow-ups that reference to this document. But, for this document as itself, we are done. We are not going to do anything else on this, no.
Heather Dryden:	Thank you, Patrik. I have United States and Sweden.
Suzanne Sene:	Thank you. Perhaps another stupid question, so my apologies because this is all very confusing and challenging for a mere bureaucrat. So, it's – and I take your point that it's impossible to decide that if you have x number of companies blocking x number of TLDs, that's a problem. You know, you can't set that. Is there a way of monitoring reports or announcements or assertions, lets say, that x numbers of TLDs by x number of countries are going to be blocked.

Is there any mechanism that would make sense in that regard, so that – you know, at the end of the day what we're trying to get our hands around is the degree of harm, the scope of the harm, and how you could mitigate it. As you all know, we originally started out way back in 2007 with this idea that one way to mitigate is just don't go there. Don't propose strings that are going to be considered offensive, objectionable, controversial, or sensitive.

So, we lost that battle, so no we're trying to figure out though, how do you establish markers, if you will, so that we can understand when a certain critical point has been arrived at where this is now truly putting resolvability, security, stability at risk.

Heather Dryden: Patrik, please.

Patrik Fälström: First of all, if we look at it from a technical perspective, it's not countries you are blocking, okay? So what is happening, we have to remember there is a chain of events that needs to happen, and the thing you are referring to is the country is imposing a policy on, for example, the service providers in the country, or operating in the country or whatever, under some kind of – whatever kind of tools or licensing mechanism or whatever the country is using or the state is using, that forces whoever is running a resolver to do this kind of blocking in the DNS.

So we just have to know that distinction. One of the reasons why the distinction is important is that is one of the weaknesses with blocking on the top level domain exists, because depending on how that sort of the state is imposing the blocking, for example, let's say it is the main ISPs.

So what about enterprises that run their own DNS resolver? What about the end users that have their own [beacon and tunnel] out of the country? So to a termination point that's outside the jurisdiction of the country. So the distinction there is pretty important. I'm sorry, it's late in the day; I don't remember the last part of your question, actually. I'm sorry, can you repeat that?

Suzanne Sene: Thank you, and this is very challenging for me, so I'm probably not being very clear at all. The idea was is there a way to try to monitor, if so many numbers of countries blocking so many numbers of strings?

Patrik Fälström: Yes, now I remember, thank you very much for reminding me. There are a number – one thing that we saw when we did this report is that there is a lot of talks that you have heard about as well, that blocking exists out there with certain country codes in some parts of the internet. On the other hand, we've found out that it's actually very difficult to get data on that as it is today, because there is today no such monitoring that is covering.

What exists though, is there are a number of initiatives, for example one by RIPE NCC to have something, to have like probes that are in networks here and there, and the RIPE NCC project, which is just one example; there are many out there. I don't even know all of them myself; the RIPE project is called Atlas, where they ask people to put probes out in the network, and those probes are monitoring all the time the quality of the network and resolvability of domain names, etc.

One of the issues that I know RIPE NCC has talked to me about is that deployment of those probes is quite often illegal in those same countries that do the blocking. So to some degree, the monitoring and the blocking, to some degree, is like… And this is one of the reasons why it's hard to get the data. Because it might be that it's difficult to get the data from the areas where you actually would like to have the data.

So to answer your question, I would say no, it is all based on the individuals reporting, which is not bad, because that's how many other things are reported on data collected around the world. The important thing is in whatever ways you got the data, that you know how it was collected so you don't draw the wrong conclusions from it.

Heather Dryden: Thank you for that. I have Sweden and the Netherlands.

Maria Häll: Thank you, Heather. Actually this is not a question, it's a reflection, because I very, very much appreciate of course the

presentation of Patrik, but also the interaction that we have now with the SSAC, with the whole SSAC group and the work that you've been doing. One of the things that I think is very important that I personally think is very important for us, not only for me but for us in the discussions, is actually the interpretation between technical movements or technical actions that have impacted the public policy, because even though you guys are very high level, very good technical persons with a high knowledge, you also in this report and in the discussion, you manage to interpret for us what impact technical actions have on public policy, and that is very important for us. Then we suddenly start to understand, and in discussions today I had many examples of that interpretation that is very valuable for us. Thank you.

Heather Dryden: Thank you, Sweden. Netherlands and then UK.

Thomas de Haan: Yes, thank you Chair. We were thinking about follow up actions, and I think Suzanne made a very good remark, and this connects also to the case of XXX. It's not a fortunate precedent, but it is a precedent; it means that XXX is in the root. We know that many, many countries have problems with XXX, and is there a way in which that specific case can be monitored in the coming half year? I mean, it's in the root, it's available, but there are yet no DNS resolvers to the second level.

So that I would say not only to the SSAC but also to the Board, which could be a signal; watch this very carefully and look whether things are going wrong. Monitor this place, and that's one question. The second one would be maybe that as a follow up action, SSAC could try to elaborate a little bit more on the good ways, the effective ways of implementing blocking, it it's strictly necessary.

It means that you have proof that blocking is not effective, if you do it on a certain root, DNS way, and on the other side it's good to – if you can't avoid it and you need it in a country, then it should be good practices to block. How will you do this? How will you do this so it will only affect your own customers, your own internet users in your own ISPs. Thank you.

Heather Dryden: Thank you, Thomas. I'm sorry, Netherlands. Okay, I have UK and then Italy.

Mark Carvell: Yes, thanks very much. First of all, I appreciate very much the presentation and clarifications and explanations. I just wondered, for a follow up, whether a little bit more comparison of filtering and blocking could help. You expressed a personal point; and I mention it because .xxx has been mentioned, and ICM made several pronouncements that it's not necessary to block .xxx. You know, within a society, if it's desirable to block .xxx they provide all the means for filtering it out to the equivalent degree. So I just

want to float that as a potential area for consideration. I would be interested to hear the view on that and for it to be set out in a short paper. Finally, just a very non-technical point, is the paper available in other languages? Is it English only? Thank you.

Heather Dryden: Please, Patrik.

Patrik Fälström: No, it's only available in English. Do I take that as a request to have it in other languages?

Mark Carvell: Yeah, I think it would be a very good idea for it to be in other languages, because this is of interest to the whole global community. Thank you.

Heather Dryden: Thank you for that, UK. So I have Italy, Egypt, and then I will look to close the speaking order so that we can end the session. Okay, so Italy please.

Stefano Trumpy: Just I want to provoke a little bit, the experience of the SSAC and I am honored to be one of the members such that they could well develop two guidebooks. One guidebook for the information provided that want to avoid blocking of any type, and then try

ways to read secondary servers so whatever is the technology, and as we learn to make a very successful 100% blocking is impossible or difficult, and then they might instead make a guidebook for governments that would like to make some blocking with some success. Because this is the experienced users, normally, they have other needs to avoid and to avoid blocking or just personally with the experience, and on the other side it was mentioned that the case of .xxx; it is certainly not useful to block, because maybe .xxx could spread more directed pornography, but if someone does not want to accept any form of pornography, blocking .xxx has no effect at all.

Heather Dryden: Thank you, Italy. Egypt, please.

Manal Ismail: I was going to ask a question along what UK has already posed, and I understand that blocking, you said, is one way of filtering, but you also mentioned that IP filtering is very different from blocking and has very different effects. So can we say it effects more internally more than its negative effect on the external world, or not necessarily?

Heather Dryden: Egypt is last in the speaking order, so if you want to respond. Patrik, to some of the questions that have been posed?

Patrik Fälström: Thank you very much for very good questions, and regarding first of all the translation, we will take that question back, we have translated some of our reports to other languages, for financial reasons we don't have budget to do all of them, but this is just two pages, so if there is a request we will take this back and see what we can do about that.

Regarding blocking and filtering, we have been looking very specifically at blocking on using the DNS, and both blocking and filtering, as terms by themselves, are very, very broad, and that's why we talk about DNS blocking. So every time in the discussion have used the term blocking, we actually mean DNS blocking.

If you look at it technically, what is the difference between blocking and filtering, well it's two different terms, with like what's really the difference. But now, what you all hear is is there any difference between doing impact on the DNS protocol and then the IP protocol? And your answer is that depending on what you want to do, the two mechanisms might have different effects, first of all. So you once again have to start with what is your goal?

If it is the case that you want to do blocking, because just saying "I want to block" is not enough; there must be reason why you want to block. If you want to take it as an example, a couple of times is it the use of the string itself, is it the string that is sensitive, or is it the data that you can access with the help of the domain name, that you don't want parties to access? Those are two very different things, and depending on which one of the problems, for example,

these two problems, and there are more, you want to resolve, there are different ways of solving that problem.

Okay, so if you look at for example the IP address, then blocking compared to DNS blocking, DNS blocking stops the ability of using that domain name. The IP address blocking stops the ability to use things using the IP address. But I think there have been and probably will be quite a number of sessions, for example at the IGF, that talk about various ways of doing this, or for example, in discussion with law enforcement agencies, if it is the case that you want to block access to information or prohibit people from accessing information, as we heard Italy saying as well, to be able to do that 100% is not possible. You need to go there, literally you need to go to the host web information and turn it off. That's the only effective way of doing the things.

Heather Dryden: Egypt?

Manal Ismail: Just a very quick response. Actually I was not looking how successful would it be to address the purpose of the DNS blocking order, I was asking it the other way round. Which would be less harmful to the outside world? But again, it's from one side, how successful it would be, but this was not really my question.

Patrik Fälström:	Now I understand, and that's a really good question. I think, just from the top of my head directly, this is the type of thing that there could be long investigations to try to answer that question, but I would say, I'm looking carefully at Danny, that will probably whack me now afterwards if I say the wrong thing here, but I would say that most people say that lower down in the protocol stack, it would be the impact on the communication, the more surgical it would be. The more precise it will be.

Notice that I am not using the term less harm here, more precise. Because if you do impact on the IP address level, if you're unlucky, you might have impact like, for example, YouTube accident when a routing announcement mistake in Pakistan made YouTube inaccessible in large parts of the world. Well, the domain name look up actually worked, so what harm it might make is also very difficult to draw conclusions on.

So yes, I am ducking; I am not renouncing your question, but is exactly why we cannot answer a regional question yes or no. We have to produce and present to you the algorithm that has to be used when you do the calculation of checks and balances. And by the way, one more thing, Jim, our last Chair of SSAC pointed out to me that both the term blocking and filtering are very generic, and both of them are actually used as equivalents of each other, so to some degree, because you need to have a context what is it you're doing?

You're filtering on the DNS protocol, you're filtering the IP address, you're blocking the IP address, you're blocking access to

certain IP addresses, you're blocking access to certain domain names. So please, whenever you are using these terms, be a little more precise, like when we are saying DNS blocking, for example. Thank you.

Heather Dryden:

Thank you for that, Patrik. So with that I think we can move to close this discussion, and again, I will thank you. This has been very informative for us, and I think has raised a few questions as well around related issues beyond just DNS blocking. So thank you very much.

For GAC members, if you could remain seated, we will ask New Zealand to take us through the work plan for the framework of interpretation country code working group, before we have our break. Is that okay, New Zealand?

Frank March:

Yes, thank you Heather. I hope this can be dealt with expeditiously, because I know we all need to take a break. Basically, the framework of interpretation working group came out of the work done by the – let me get the name of it right – the Redelegation and Retirement working group, which gave a series of reports, I think to the Cartagena meeting or the one before that. And made specific recommendations about follow up studies and the framework of interpretation working group was the first step in terms of working through those recommendations.

The recommendation was that as a first step, the ccNSO Council will undertake the development of a framework of interpretation for the delegation and redelegation of ccTLDs. This framework should provide a clear guide to IANA and the ICANN Board on the interpretations of the current policies, guidelines and procedures relating to the delegation and redelegation of ccTLDs. So that's where it came from.

Although it's being run by the ccNSO, it is in fact a multi-constituency working group, and we, the GAC, provided observers for the original delegation, redelegation, retirement working group process. The San Francisco meeting agreed that the GAC would take full participation in the framework of interpretation working group.

Now I understand that three members of the GAC put up their hands to actually take part. I was one, I think Bill Dee did on behalf of .au, and Suzanne for the US. I don't think any of us have actually managed to partake of any of the discussions that so far have taken place in terms of that working group.

Suzanne Sene: Not true.

Frank March: Not true? Have you?

Susanne Sene:	I was on a call.

| Frank March: | Oh, my apologies. I certainly wasn't able to; there have been two calls so far. The working method is basically that no decisions are made until at least two calls have been taken, and as they move around the clock so that people that are caught in the middle of the night can take part in another meeting before decision is taking place. So it takes time to work their way through. |

Now, this particular document, which was circulated and is available for inspection; I circulated to the GAC along with a document which was the actual set of terms that were going to be discussed. So it was circulated some time ago. I don't believe it is contentious; it is simply a layout of the work plan and the timings, which are going to run through to the middle of 2013.

The process is prolonged and the steps are detailed. I undertook to get endorsement of the GAC to the document; while the working group was seated with its work, so that these things could go on in parallel, and I believe that will be a possibility as we go forward. We don't want to impede the progress of the working group, but there will be plenty of time for the GAC to comment and for respective changes to be made if necessary.

That is the case here, there is an invitation for us to add or change the document, even though the working group itself has agreed to it, and is progressing with it. I think that's probably enough for me to say at the moment. I'm very happy to answer any questions; at

least questions I can answer at this point. I would point out that we can also discuss it when the ccNSO meets with us tomorrow, and there is an open meeting of the working group on Thursday afternoon, I think 3:00 to 5:00. So I'll leave it there, Heather, and I'm happy to answer any questions.

Heather Dryden: Thank you, New Zealand.   Are there any questions about next steps for this working group? European Commission?

William Dee: Thank you, and I apologize; I was also unable to participate in two calls. Frank, I think you have, however, been able to follow a bit more closely than me. I didn't read this paper, but you used the expression 'you undertook to get GAC endorsement' for the document, and I wonder if you have a feeling for the timing on that, given that we haven't discussed it yet? I guess it's going to be more than one page, this document.

Frank March: Unfortunately, the document is quite substantial. There are copies available; it was circulated about – I think I circulated it about two weeks ago. It is very long, it is very detailed. It actually requires quite careful reading, but it is, in the end, simply a time table of outlining the work plan. It explicitly says the working group itself will not look at policies but will simply be concerned with interpretation. And there's no policy outline within the document itself, so I don't know. In answer to Bill's point about how to proceed, I was rather hoping that this meeting would simply give

the tip to the document so we could report on Thursday that the GAC was happy with the document and for the work to proceed as outlined.

Heather Dryden: Thank you, New Zealand. Did you want to come back on that, European Commission? Okay, and then I have the United States.

William Dee: Yes, no, that's fine. I think, you know, I think I have looked at it actually, and it's mostly a time table of work and I wouldn't envisage anyone having problems with that. I just – endorsement always sounds very formal to me, actually, like we're signing up or something, so I think the absence of any concerns at this stage actually, and encouragement for the working group to go forward would be fine, if that's what's being – if that's what they're looking for. I think we're not that stage yet, but issues of delegation, redelegation, retirement are potentially extremely politically delicate matters, so we should probably avoid at any point endorsing anything without time for proper discussion and a careful consideration in the GAC. It sounds to me as though we're probably not going to have an opportunity at this stage to do that, but it also sounds as if we don't need to endorse anything much, just encourage the working group to keep going. Thank you.

Heather Dryden: Thank you for that, European Commission. United States?

Suzanne Sene:	Thank you, and I appreciate Frank's overview and Bill's comments as well as you giving us time, because I know we do need to take a quick break. But just as a quick FYI, I participated in one of the two calls as one of your liaisons, so in now commentary from me regarding the GAC perspective at all, just being there to understand what their intentions were. It was their very first call, and they were reviewing the work plan, just to get agreement, and it takes the two calls to do that.

As Frank points out, it's quite detailed, but it's got a timeline that scopes out how they will tackle all of the different issues. There was an interesting sentence in there that I would draw your attention to. I don't have it in front of me, my apologies; I don't know what page it's on, but I think they're trying to be very, very clear about the scope of the work. But there was a sentence that gave me pause, because it seemed to suggest that they would not – the intention is not to revisit or rewrite existing policy, but to interpret or reinterpret, to help interpret what the policy means.

The existing policy documents are RFC5091 and the GAC principles. So I raised what you hope will think was a very logical question, which is does that mean you would not – you are not looking to the GAC to revise its principles, or you would not have a problem should the GAC decide it needs to? Because it strikes me that that would be – and they were very careful to say, to back off immediately, they hadn't intended to suggest that they were dictating to the GAC.

It is our decision to take, should we wish to revisit our 2005 GAC principles and guidelines for ccTLD delegation and redelegation. I'm just, in personal observation, I'm guessing we may want to, because there are certain issues, as you go through the timeline, they devote work to specific categories of issues. There are certain issues, like how do we want to define the interest of the local internet community? Which I believe our 2005 principles do not address; but that is something that we may want to speak to.

So I just wanted to add a little bit more flavor behind that, so that we know as we go ahead, and I don't think we have to decide anything when we meet with them tomorrow, and I think Bill and Frank are both correct. I don't know that we need to endorse their base document, but just concur that we strongly support this work, and intend to work collaboratively with them.

Heather Dryden: Thank you, United States. New Zealand, and then UK, and then I think we can conclude this discussion. Norway, and then we will conclude. Okay, please New Zealand.

Frank March: Thanks, and thanks Suzanne, for building out. I was abbreviating my comments, and I was going to highlight just exactly what the scope is. The working group is tasked with interpretations of policy statements, and as Suzanne has said, the two policy statements that are being picked on are RC5019 and the GAC principles, is the two documents they used for this. The other

source material is the decisions that have been taken by IANA over the existing sale of redelegations that are taking place. Those are the source materials for the terms that need to be interpreted, and the scope specifically states "any proposal to amend, update, or change the policy statements is outside the scope of this working group." So there's no intention of doing that, it's a matter of providing initially, a set of definitions for the various terms that have arisen. I did circulate a second document, which did outline what those terms were. That's the initial part of the work plan. Thank you.

Heather Dryden: Thank you for that. United Kindgom?

Mark Carvell: Thanks very much, and obviously there's a lot of work involved here by the FOIWG, I must admit I really haven't focused too much on this at all, because of new gTLDs primarily. I think what- I hope to enable me and perhaps colleagues who find themselves in a similar position to enable me to get a handle on this, in a document like this, it highlights we will need GAC advice on this issue, this element or something, within a time frame and so on. So I can quickly and then I can quickly assess I've got to do some work here, this is to do with a country code, maybe I have to consult a registry or whatever.

And then I know I can start planning ahead to sort of engage with this and contribute where – as the GAC rep, I need to contribute,

and then contribute to a GAC response or input and so on. So that's just my kind of plea, as a way to get a handle on this. I mean, it – there's a lot of detail in this particular paper within the work plan and so on. If there's some sort of highlighting, "we will need GAC inputs on these", that will, I think, be a great help to me and maybe others too. Thanks.

Heather Dryden: Thank you UK. Norway?

Ørnulf Storm: Thank you, and US touched upon this, and of course it would probably be most helpful to have a working group like this interpret the GAC's ccTLD policies, but of course the authority to interpret would be GAC, of course. But of course then you could have how the community interprets the policies, the principles, and then of course the GAC may then have to revisit and make it clear, or do more definitions, or whatever. So I think it could be useful, but of course at the end, of course, GAC would be the authority to be interpreter of our own principles. So but that could be, of course, helpful for us to make it more clear, if it's unclear. So, thank you.

Heather Dryden: Thank you, Norway. With that, I think we can take a break. So you are aware, we've asked the Board to come later to meet with us, so we will meet with them starting at 5:30, so between 5:30 and

6:30, so if we can be back in the room in 20 minutes, this means we will have an hour to prepare in a closed session, for our meeting with the Board. Okay? 20 minutes, thank you.

[End of Transcript]