ICANN83 | PF – GAC Session on Security and Stability
Wednesday, June 11, 2025 – 09:00 to 10:15 CEST

DAN GLUCK

Welcome to ICANN83 GAC Session on Security and Stability on Wednesday, June 11th at 0700 UTC. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior and ICANN Community Anti-Harassment Policy. During this session, questions or comments will only be read aloud if submitted in the proper form in the Zoom chat pod. Interpretation for this session will include all six UN languages and Portuguese.

If you would like to speak during this session, please raise your hand in the Zoom room. When called upon, participants will be given permission to unmute in Zoom. Please state your name for the record and the language you will be speaking when speaking a language other than English, and please speak at a reasonable pace to allow for accurate interpretation. I will now hand the floor over to GAC Vice Chair, Marco Hogewoning. Thank you and over to you.

MARCO HOGEWONING

Thank you, Dan. Good morning, everybody. Indeed, I'll be chairing the session and I hope our esteemed chair, Nico, is somewhere in the back enjoying a nice cup of coffee. As you can see, we have split this session in two. First, SSAC will take us through some of the

projects they'll be doing, and then I asked Cristian Hesselman from SDNLabs to guide us a bit further on how quantum interacts with DNSSEC as a follow-up to the session we had in Seattle at ICANN82.

Before we kick off, maybe a quick run of introductions of who is behind the table. Dan already introduced me. I'm Marco Hogewoning, GAC representative for the Netherlands. And maybe, Maarten, you want to take it first?

MAARTEN AERTSEN: Good morning. My name is Maarten Aertsen and I'm a member of SSAC.

WARREN KUMARI: Hi, I'm Warren Kumari, also a member of SSAC.

GREG AARON: I'm Greg Aaron from SSAC.

RAM MOHAN: I'm Ram Mohan. I'm also from SSAC and the chair of SSAC.

CRISTIAN HESSELMAN: Cristian Hesselman. I'm with SIDN, the registry for .NL, the top-level domain of the Netherlands.

MARCO HOGEWONING Well, thank you. Then, without further ado, I think I can hand the floor to you, Ram, for our first topic, domain registration.

RAM MOHAN Thank you, Marco. If you could please go to the next slide. We wanted to share some comments with you on Domain Registration Data Access. Next slide, please. What we wanted to make sure that we share with the GAC is what our goal is. We want to make sure that any policies for gTLD registration data access is well-defined, is robust, and that it serves the needs of the global Internet community in protecting against security threats. That's what we're solving for.

The way we think that should be done is by creating an access system that follows a structured and expedited mechanism, so that legitimate requests, especially urgent requests, are handled in a prioritized and expedited manner. That the policies for the response times, policies for the how and the what and the when, those pieces are clearly defined and accepted inside of the community. And we believe also that ICANN, the organization, should continue to share metrics on data requests that come in for domain registration data.

And we think that access to registration data is important. It's a foundational part of security and stability. And we've provided feedback to the EPDP on this, but we want to say that this is not an area that is in conflict with privacy needs. You have to have the privacy needs addressed in an appropriate way, but there is a clear

security and stability concern. And so, we want to make sure that the process by which these changes are done in the community take into account the principles that we have listed here on the screen. That's really what we wanted to say. Open for any questions or comments.

MARCO HOGEWONING: Thank you, Ram. And of course, yes, I think the GAC aligns with your points about access to registration data. Do we have any questions? No, it's still early. I'm seeing none in the Zoom. I see none in the team. Well, maybe near the end of the session we can come back. But then the next topic, I believe, is talking about open-source software. Maarten?

MAARTEN AERTSEN: Yeah. So, we're working on a topic that may be familiar to some of you, which is free and open-source software, which is software that can be freely used, shared, modified even, or studied. And we're examining specifically the role of this type of software within the global DNS. So, we had thought that this is heavily relied on, but there was no extensive study for this community available.

And free and open-source software has quite unique characteristics in terms of development and governance. And while around the world people are discussing infrastructure, reliability, software, etc., we found it to be valuable to make visible the role of this type of software, its characteristics, to make sure

that when there's a policy discussion that this is taken into account. So, this work has two objectives. We want to make visible this critical reliance. And we would like to make visible the characteristics of this software and maybe inform some of the assumptions that would be logical to make about software in general, but may not hold true for this particular type of software. So, this is a bit of a teaser presentation.

Next slide, please. The areas we're looking at are basically four. We're doing a survey where we describe the state of the land. We look at the domain registration side of things. And we look at the DNS side of things, where people publish and retrieve mappings, which gives you state of the world. We analyze the characteristics of this software, including its development model, which is not the same as you would assume to be true for physical goods or for other software. And then we contrast within this area of free and open-source software how these general characteristics hold for the software that's popular in DNS, the software we care about in this context.

The third portion is then to clarify assumptions, assumptions that we've seen made in practice that do not hold, and clarify where there's misconceptions. And finally, we try and list relevant risk factors to be considered in policy making or regulation. They pertain to development, but also to operations of this software. So, that's basically the areas we cover.

Next slide. And in Muscat, we hope to perhaps tell you more about this, because we hope to publish this report in the months following this event today. As a slight teaser, we believe the use of free and open-source software in DNS and domain name registration is a strength, but there are risks to consider. And we feel we can offer some guidelines in this regard concerning the use of free and open-source software. That's it for today. I'm happy to take questions.

MARCO HOGEWONING: It truly is a short and brief teaser. Are there any questions for Maarten about this work? I'm looking around. I see India has his hand up again.

SAJID: Thank you, Chair. Sajid from India. My question is actually to Mr. Ram Mohan. You missed out because of the shortage of the time. We have a shared objective of that the registration data should be provided within 24 hours, but it's been more than 24 months that we are still trying to get the ICANN come to an agreement on the timeline, forget about 24 hours. I mean, whatever timeline. As of now, we don't have any timeline for that matter.

So, although the urgency has been made multiple times, both from the GAC and from SSAC, but because of the prolonged process, I think now it has gone into dual track, one for authentication and the other for the policy track. What would you think as a chair of

the SSAC and maybe to the GAC vice chair also, I think, should a joint statement from SSAC and GAC would be useful to impress upon the ICANN Board to come to this timeline, have a decision on the timeline as soon as possible?

RAM MOHAN

Thank you for the intervention. We agree that for urgent requests, the process should be made very clear. And I believe there are some discussions that are already underway with the parties who have to implement those changes. I cannot speak for all of the SSAC yet. I'll have to consult with the members. But we have been fairly clear that if something is termed and deemed urgent, it ought to be treated as urgent and the responses ought to be very expeditious. It shouldn't be something that takes a long amount of time. If it helps to do something together with the GAC, we'd be open to it, to underline the importance of this issue. We believe it is an important issue. Part of it is that we have to have clarity that urgent means urgent, urgent doesn't mean normal course of business.

MARCO HOGEWONING

Thank you for that, Ram, and I do agree. Obviously, as you know, the GAC has mentioned urgent requests, I think, in the last five Communiques, at least that I can recall, including some advice. We are active, or at least some of our colleagues are active in the small teams looking at this. In my perspective, it is progressing. I do agree with your observation that for an urgent request, it's not

progressing with the urgency it might need. And I think I can happily align with Ram, so let's keep this in mind and think about if we think that a joint effort could help move things along, I'm happy to entertain that thought, so let's come back to that at some point. Are there any further questions? I see somebody pointing at me. Russell, yes, sorry.

RUSSELL WORUBA Thank you, Chair, and thank you, our esteemed colleagues from SSAC. You guys are doing a great job. I'm a big fan of SSAC, and thank you for the work on force. I just have some reactions. I think many of the countries in the underserved region are heavily relying on open source, mainly BIND to run our DNS at the ccTLD level, and then, of course, now with the landscape that is shifting, we really look forward to what the outcome of this study will be. Would you have some baseline at this time on what it is at the moment, especially on across the regions, just for our appreciation? Thank you.

MAARTEN AERTSEN Thank you for this question. So, I'll give a little teaser. So, on the landscape survey, where we tried to get hard data on who uses what, I think we plan to say, or the current draft, which is not subject to publication, says something like the global DNS runs on open-source software. So, it's not just you, and we have some statistics to back that up. So, for example, in the ccTLD space, 20 out of 25 top operators use this software. If you add the gTLD

space, it's 9 out of 10. And if you look at the root server system, it's 9 out of 12 that exclusively use FOSS.

And I think this is one of the values that this report can bring is to surface to a larger audience what maybe some of the people in doing the technology knew that this stuff is everywhere, and we hope to surface the information because we saw in some regions software being regulated and FOSS being an afterthought. And because the characteristics are so different in terms of development and in terms of funding, in terms of who uses them, that might not be the winning strategy. Yeah.

MARCO HOGEWONING Thank you. I've heard Germany in the queue as well. Rudy.

RUDY NOLDE Thank you. Rudy Nolde from Germany. Originally, I wanted to ask what advice you have for policymakers. Then I saw your last slide that you will offer guidelines to policymakers, and I think you just gave a little teaser. Since I'm so impatient, maybe could you maybe preliminary say in which directions these guidelines or advice to us policymakers would go?

MARCO HOGEWONING So, I don't want to steal time from my colleagues, but I'll keep it brief. So, the way we're currently thinking is to make visible some of the misconceptions. So, for example, one misconception that is

quite natural is that you can use contractual relationships as a mechanism in policy. So, you say something like we regulate critical infrastructure operators in our region, and then they impose requirements on whoever their suppliers are, and their suppliers will impose requirements on whoever their suppliers are, etc.

So, this may work for physical materials and sometimes in software. It doesn't work when software is basically downloaded from the internet, because then there is no chain. So, this is a misconception that this type of instrument would work, and in practice it doesn't, because there's a lot of software that is developed and maintained by a dedicated group, but where the use goes way beyond the existence of support contracts or such instruments.

So, in terms of advice, I think we might offer some thoughts on that particular space, like how to deal with developers in this regard or how to think, but also if you put requirements on operators that would restrict their ability to choose best-in-class software, which might well be this type of software, then you may not achieve the policy you hope to achieve. So, I guess that's the area where we would be, but I'm speaking out of turn. We first need to publish the report, and then I'll be gladly back to talk to you about this.

MARCO HOGEWONING I think we're happy to have you back once the report is published and then follow up on this discussion. I see my queue is empty and

conscious of time, I suggest we move to the last SSAC topic, one that I'm personally also very interested in, and that is DNS Blocking Revisited. I guess, Greg?

GREG AARON

Okay. Thank you. This is a paper that's an update of two papers that SSAC wrote about 12 years ago. So, DNS blocking is not something new, but we thought it was time to update it because there have been many new examples out in the world of DNS blocking taking place, and we've seen what's happened as a result of those actions. There's also some new technology that's been developed in that time that affects DNS blocking and how people are able to get to resources on the internet. So, this group involved about 20 SSAC members. Warren and I were the co-chairs of the group.

So, what is DNS blocking? So, when you are at your computer and you want to visit, say, a website, you type in the address, the domain name, and then your query goes up to a DNS resolver. We call these recursive resolvers. It's often run by your ISP. And then the recursive resolver helps figure out the IP address of your destination, translates your domain name into an IP address, and eventually the DNS figures out where your destination is and allows you to then talk to that website you want to visit.

And normally that process happens instantaneously almost. You get to where you want to go. However, the recursive resolver can block a domain name. And what that means is that the resolver will

tell you something different than is expected. Basically, this is done two ways. The first time, in that first instance, the recursive resolver might tell you that the domain name you want doesn't exist, when in fact it does. So, you try to go to Wikipedia, for example, and you don't get the answer. You don't get connected to Wikipedia. The alternate means is, instead of being taken to the website you want to go to, you're taken and redirected to another destination. So, one way to put this is that the recursive resolver is telling you something unexpected, or some people would even say it's lying to you. It's not giving you the answer that exists in the DNS.

So, DNS blocking is a technique. It is a tool. Like any tool or technique, it can be used for various purposes. It can be used expertly. It can be used clumsily, just like a hammer. You can use a hammer to build a house. That's great. You could also use a hammer to hit somebody over the head, which is not a good thing or a good use. So, it's designed to prevent people from getting to content, basically, or to be able to use a service. This affects not only visits to websites, but any use of the DNS. So, it also will affect email, network management, all the other things that rely on DNS.

Next slide, please. So, if a DNS resolver was Gandalf—we always have to have a pop culture reference here at SSAC—that's what it would say. Next slide. So, DNS blocking is used for a lot of different purposes. So, motivation is important. Now, one of the ways it's used is for security. So, a resolver might not take people-- Oh, how dramatic. The electricity has been blocked. A DNS resolver might

be set up so it will not take people to a site with malware or phishing or something like that. So, that is set up to be a beneficial service.

And probably all of us in this room are protected by DNS blocking in some way. For example, all the web browsers pretty much have a system that will pop up a warning page and not allow you to go to a known phishing site, for example, until you decide you really want to go there. So, that is something that is endemic across a lot of systems and it's pretty much ubiquitous and generally designed to help people and protect people. And that is done at usually a local level. So, you choose a provider you want at a company to help you do security within your network.

Some people use it for content control. So, for example, your local public library may not allow patrons to go to certain kinds of sites that the community deems shouldn't be accessible from the library. For example, gambling or pornography sites because there are children at the library. Some companies use DNS blocking within their companies because they don't want their employees doing certain activities like visiting social media or gambling sites while they're at work on the network. So, again, that's a kind of a local setup where the company decides a policy for its workplace.

What's most controversial are the uses of DNS blocking to prevent people from going to content, especially if the blocking is done at a national level. In other words, preventing the citizens from an entire country from visiting a particular location, seeing particular

content. And this is one of the reasons why we want to present this information to policymakers and GAC members and the like because those decisions affect a lot of people.

Sometimes the blocking is done based on a law. For example, some countries do not allow citizens to visit known sites that distribute child sexual abuse images. That's done for the protection of the children and the protection of the citizens. Countries will have lists of these domain names that they distribute to their ISPs. Most controversially, DNS blocking is done in some places to prevent access to content that expresses political opinions. So, it's used for censorship.

Next slide. We want to make a distinction between DNS blocking and the suspension of domain names. They both have the same purpose, to prevent some content. But DNS blocking does not remove content from the internet. If some people are blocked, other people can still get to the content. Domain suspension tries to prevent access to the content by taking down the domain name, to prevent it from working. Now, thousands of domain names are suspended every day for security and abuse problems, like phishing sites.

Occasionally, sites are taken down by court orders, so they stop working for everyone. Law enforcement, for example, on this graphic, will take down a website as a result of a court order to prevent criminal activity. And they may either take it down completely, or redirect it and take over and put it on new name

servers. These are two separate things, but they're often used for similar purposes, to prevent access.

Next slide. This is a note from the paper. SSAC is talking in this paper about the techniques that are used for DNS blocking, some of the motivations. Of course, people can disagree, however, about particular cases. What is illegal in one country may not be illegal in another country. People can disagree about the merit of a court decision to block something. We're not making judgments about any of those particular cases. Next slide.

WARREN KUMARI

Thanks. So, as Greg said, DNS blocking is a tool. And as with any tool, it has some strengths and weaknesses. It's also important to understand how the tool works, so that you can best understand how to use it, and not accidentally cut yourself while doing so.

So, DNS blocking works by putting lists on the recursive resolver of what should be allowed to be resolved and what shouldn't. One of the implications of this is it only applies to users who are actually using that recursive resolver. This means that if a user decides to use a different recursive resolver, they will be able to bypass or circumvent the blocking.

So, in this diagram at the bottom, the user is sending their queries to a sort of one of their standard resolvers from their ISP. If the name that they're trying to look up is okay, it just resolves normally. But if it is on one of the DNS block lists, something else will happen.

Either you'll get back a response that the name does not exist, or possibly the recursive resolver will try and redirect you somewhere else. But if the user's not querying that recursive resolver, that the DNS queries go to a different resolver, and there isn't blocking there, the user will be able to just access the internet normally.

Next slide. So, how is it that users might be able to use a different resolver? So, one of the obvious ways is there are a substantial number of so-called public resolvers, and they're used by a large number of users. Geoff Houston's APNIC research shows that around 21% of users are currently using one of the well-known worldwide public resolvers. Some examples of these, Google Public DNS, Cloudflare runs an open public resolver, Quad9 does as well, but there are also government-provided versions of these. The obvious and well-known example of this is DNS4EU is a government-sponsored public resolver service. And so, it's relatively easy for even non-technical users to update their recursive resolver settings and decide to point at one of these alternative DNS servers.

Next slide. If you've watched any streaming service in the last many years, you will no doubt have seen a bunch of ads for different VPN services. Common ones are NordVPN and Surfshark, but there are a huge number of these. And they provide a couple of good benefits to users. They enhance their user privacy, and they provide more anonymization, but they also have made it fairly clear

in their ads that these are designed to bypass geographical restrictions.

So, for example, if you're traveling, and you would like to watch a streaming service in your home country, or content that's available in your home country, you can just start up a VPN, and now it looks to the internet as though you're in that country. The other obvious thing for this is if you're in a country and you want to watch content that's not available in your country, you can just fire up a VPN, choose an endpoint in whatever country you wish to appear in, and suddenly it looks to the internet as though you're there.

One of the things that that means is you're using a different set of recursive resolvers, and to the internet, you look as though you're not in the country that you're actually in. This means that if there is blocking in a set of recursive resolvers, you can easily bypass this by just turning on a VPN. Next slide. I think it's back to you.

MAARTEN AERTSEN

Next slide. So, what can go wrong, or not go well, at least? So over-blocking is when a block is too broad. For example, you can block a third-level domain, which is more precise than blocking a second-level domain or blocking at the TLD level. If your blocking is too broad, you may cut off access to more than one destination or more than one website, and that would inconvenience the visitors to those sites that don't present problems.

So, that often happens when you block the wrong place. There are many, many case examples, by the way, in the paper of all of these things, and so if you want to get into the details, we do suggest you look at the case studies. In one case of over-blocking, for example, Italy has a system where it distributes some domain names to its ISPs, and accidentally, they listed a domain that was used for infrastructure, and it was over-blocking, and it actually blocked Google Docs, for example, for users in Italy for a brief time until someone realized the mistake. So, that mistake inconvenienced people and prevented them from getting to all kinds of content that was not problematic at all. So, this is a kind of collateral damage. You do it poorly, you start to affect people you didn't mean to affect.

Next slide. So, as Warren described, people can get around blocking. So, whenever blocking happens, you should probably assume that some users are going to get around it, especially if they're very motivated to do so. They can use their VPNs. They can use their alternate resolvers. In fact, there are other technologies that help people keep content available or allow users to get to content. So, the effectiveness of DNS blocking is often a matter of degree. If someone assumes that if we block a domain and we send an order to our ISPs in our country, that the problem will be solved. It will be solved for some number of users, but probably not for all of them. Next slide, please.

WARREN KUMARI

So, when a domain is blocked, the recursive resolver can reply with two general answers. One of them is just the domain name does not exist. But another thing that we see being required is that the recursive resolver redirect the user somewhere else. There seems to be an increase in this type of blocking. And we think that this is really quite dangerous.

The reason for this is if the user is trying to reach a site, for example, foo.bar.com, and they are redirected somewhere else, their web browser is going to pop up a warning saying you tried to reach foo.bar.com, but the web server you're connecting to isn't foo.bar.com. And users will be trained to just click through these warning messages, and that has some serious security implications. Primarily, they will just learn to ignore the warning pop-ups. And while this might be happening for a DNS-blocked site, the next time it happens, it's likely to be their bank or something similar. So basically, one of the things Druckmann says is, please do not do redirection if you're going to do DNS blocking.

And this leads into the next set of things, which I believe is recommendations. That's me again. As we've said a number of times, DNS blocking is a tool, and just like any tool, especially powerful ones, they can be used to do good things, but if you don't understand exactly how it works, and if you haven't read the warning instructions, you can end up hurting yourself badly. So, if you're going to implement or mandate DNS blocking, make sure

that you actually understand how it works, and also what the collateral damage and side effects are.

MAARTEN AERTSEN

Next slide, please. So, the second recommendation that the SSAC makes is that if one is going to mandate some blocking, that could be within a company, it could be at an individual ISP, it could be at the national level, you should follow these guidelines. Some of these guidelines are basically based on the medical advice of do no harm.

So, first, you should understand whether DNS blocking will fulfill your objectives. There might be alternate ways of solving your problem. Again, for example, if you're going to block, you may have some users who will get around the blocking. Is that going to help you, or is that not enough? Second, you should have a clear policy about what you're going to block and how you're going to do it. And you should have well-defined procedures to review what goes on a block list, and you should minimize risk. You should, for example, understand how to correct an error. We don't recommend specific policies and procedures because they should vary depending on what your goals and your tasks are, but this is an important principle.

Third, implement in a way that minimizes over-blocking or the collateral damage that could affect your users, so the people that you have administrative responsibility for. Again, for example, in a company, your employees. And finally, you should not affect

people outside of your administrative responsibility. Here in Europe, for example, there are lots of countries. Some of the ISPs in Europe serve customers in more than one country. So, if you're in country A, and the ISP serves people in country A and country B, what happens if the ISP gets an order from country A to block? Because that's the jurisdiction that the company is in.

How does the ISP block but not affect perhaps people in country B, which are outside the jurisdiction? We must remember that when we look at the globe, we see the lines that are our national borders, but the internet doesn't quite correspond to those lines. So, we're basically saying, be careful not to affect people you don't have a right to affect. Last slide, please.

WARREN KUMARI And I'll go really quickly because we're out of time. The last recommendation is aimed at resolver operators, and the SSAC recommends that they use this new RFC to annotate error messages, including blocking, with why it happened. Moving on. Actually, I think we're out of time for questions, too.

MARCO HOGEWONING Well, yeah, we're very strapped for time, but thank you. It's a very elaborate piece of work. As part of your target audience, I really appreciate this. It gives you a lot to think about. We're strapped for time, but I do think I can take in one short question. And I saw

Papua New Guinea on chat already. Russell, you want to come in and ask your question?

RUSSEL WORUBA Thank you, Marco. We have been, as a country, invited to participate in trials on protective DNS. And I wanted to just make sure if this is actually this one, in a sense, protective DNS.

MAARTEN AERTSEN Yes, so protective DNS can be accomplished through DNS blocking. For example, the public resolvers that we mentioned are in the business of providing protective DNS. They do block phishing and malware, for example, to protect their users. So, that is one technique that can be used to protect people. We also want to mention that this paper has already been used to inform some policy decisions currently under discussion in Japan, where they're considering blocking a very specific kind of content within the country.

WARREN KUMARI And a very short update to that. Cloudflare is one of the organizations which offers public resolvers. And they offer three different addresses, or at least three of them. One of them is their standard 1.1.1.1, where they don't really do any blocking at all. Then they have 1.1.1.2, which blocks malware. Then they also have

1.1.1.3, which is a more protective DNS thing, where it blocks malware and adult content.

I think what the SSAC, or at least maybe this is just my view, if there's going to be a protective DNS service offered to a large group, the user should be able to choose what level of protection they would like. If you are a parent, you might want to block access to adult content. So, you might want to choose the protective DNS service that does that. But if you're an adult, you might want to be able to see that content. So, I think it's an opt-in versus opt-out thing. And that goes back to something earlier, which we had said that there's different types of blocking and different sets of people who are affected. If it's something you have chosen to do, or you have opted in to have that protection, it's probably more tenable than if it is protection which is imposed upon you by someone else.

MARCO HOGEWONING All right. Thank you, Warren. I have three people in the queue. I close it here. Please all be brief. If we can take one minute for each question and answer, we should be back on track timewise. First one I think is DRC, Blaise.

BLAISE AZITEMINA FUNDJI Yes, thank you very much. Blaise Azitemina from the Democratic Republic of Congo for the record. I have a concern with VPN. While I'm very thankful about the security and safety that VPN tools or facility can provide, but at the same time, on a public policy

perspective, I have a concern about the de-location. Well, mostly in so-called developing countries, people are using VPN not really for the safety and security criteria, but mainly to have just to hide to another address, mainly a country, just to show that I'm in another country. And that sometimes is a safety or public policy breach for some of our countries.

We've seen some streaming platforms which have found a kind of solution. When you're connecting through VPN or proxy, definitely it will tell you that you do not qualify or you do not have access. So, what may be the balance between safety, security, at the same time, the accuracy of your geographic position? Thank you.

MAARTEN AERTSEN I don't think the SSAC has considered all the implications. The truth is that VPNs are widely available and like a lot of tools, they're, again, used for good purposes and bad purposes. Criminals use VPNs to hide where they are. A VPN takes advantage of the way the internet works, and so they're here to stay. Some companies maintain lists of known VPN IPs. They use that, for example, to rate the risk of traffic coming from those addresses. So, there are some tools to detect and understand VPN traffic.

WARREN KUMARI And a very short follow-on from that. VPNs are designed to look like regular internet traffic. And so, there have been some places which have tried to ban their use, either in a company or in a country. And

what seemed to end up happening with that is they're able to block the large VPN services, but users want to be able to access the content they want to be able to access. And so, users will go to a less well-known, less tracked VPN, which might end up being a lot riskier to them. So, I think there's always a negative consequence that one needs to take in mind if you try to block a technique that users are trying to access content that they want to access. They will find a way to reach it, potentially in a more risky way.

MARCO HOGEWONING Thank you, Warren. Maybe allow me to take the first two questions and then you can briefly respond to them. So, the first hand up is India. Should we brief?

SUSHIL PAL Thank you. This is Sushil from India. Do you think the government-backed DNS, like what you said, DNS for EU, it offers any significant benefit over other public DNS? And the second question is, yeah, I think VPNs, they have the relevance. Yes, of course, provided they're known VPNs. Does security agencies, they're looking at any way of monitoring the unknown VPNs?

MARCO HOGEWONING Ashwin? Yes.

MAARTEN AERTSEN: What I can tell you about DNS for EU is what they say on their website. They said that they set it up as an effort in sovereignty, basically. Rather than sending traffic to large commercial, the public resolvers, Europe now offers DNS for EU, so the traffic is in Europe. So, take that for what it says. Do security agencies look for ways to monitor unknown VPNs? I don't know.

SUSHIL PAL: Is that a concern for security agencies?

MARCO HOGEWONING: Indonesia, last one.

ASHWIN SASONGKO SASTROSUBROTO: Yes, thank you. I just want to get your comment about blocking, because you mentioned about the negative impact of blocking and so on. What if the approach is not allowing all DNS to enter our cyberspace, but we only allow what we want? So, for example, .go.id, okay, you are all allowed. Okay, this one is .com. I will find, okay, this one is allowed, this one is allowed, and the other are not allowed. So instead of blocking, we actually block everything and only allow DNS which we approve. Thank you.

WARREN KUMARI: I don't really know if that's feasible to do. There is millions of sites on the internet, and so building the list of what is allowed to be seen would be very difficult. But even if you were able to do that,

it's not really technically possible these days to block all DNS access. There is a number of new technologies, DNS over TLS, DNS over HTTPS, DNS over QUIC, where it's not actually visible that the query is a DNS query at all. It looks like any other internet traffic. And so, the only real thing you would be able to do is just block all internet access in your country, disconnect the country from the internet, and ban Starlink and other satellite providers. So, if you connect to the internet at all, some set of DNS traffic is going to get out and people are going to be able to reach stuff.

MAARTEN AERTSEN And the technologies that Warren mentioned are basically encryption-related technologies designed to protect the identities of the end person who's making a query. And so, these technologies are attempts to provide greater privacy on the internet. Thank you.

MARCO HOGEWONING And apologies, this is a really interesting topic and I see a lot of engaging debate, so I think it warrants a follow-up. Meanwhile, behind us is the QR code for the full report. So please, of course, read it. It has been out for a while. With that, can I thank you, Ram, Greg, Warren, Maarten. Please feel free to stay around. But without further ado, I'd like to swap over to what I said was a follow-up on the discussion we had about quantum computing and some of the risks during this session in Seattle. And I'd like to hand the floor to Cristian Hesselman from SIDNLabs to talk us through how this

impacts the DNSSEC and especially what we as government representatives can do in helping to mitigate some of the problems. Cristian, the floor is yours.

RAM MOHAN

Marco, just before that, I wanted to thank the GAC on behalf of the SSAC. We really value our continued interaction and collaboration and look forward to much more of the same. Thank you.

MARCO HOGEWONING

Thank you. Sorry, Ram. Now then, Cristian.

CRISTIAN HESSELMAN

Thank you, Marco. Okay. So, this presentation is, as Marco said, on quantum computers and DNSSEC and what the impact of these future machines might be. At the end of this talk, I included a few suggested actions for the GAC from a government perspective. The slides are gone. Anyway. I'll just keep talking. So, the picture you saw is a picture I got from the Leibniz Computing Center, which is in Germany, where they are working on these quantum computers. But they're still, I wouldn't say science fiction, but they're still very much in an experimental phase. So, we're talking long-term research here. Okay, we're back. Okay, thank you.

Next slide, please. Okay. So, first of all, what are the expectations of quantum computers? And I should add that I'm not an expert on quantum computers. I'm an expert on distributed systems. So, I

think quantum computers or expertise on quantum computers is mostly in the realm of physicists, and I'm not one of these persons. So, this is what I read in the literature. So, the expectations of quantum computers are new applications like new drug discovery methods, improved machine learning, or the development of revolutionary materials.

But as Greg already mentioned, you can use technologies in different ways. So, this is the hammer that Greg talked about, so that you can use it in a positive way, but it also has certain risks. So, the downside of quantum computers is that they might break the current cryptographic algorithms that we're using. So, one of them could be the algorithms for DNSSEC, which are being used to authenticate DNS messages and check the integrity of these messages.

The slides are gone again. Do you want me to continue or just wait for the slides to come back on? Okay. We have returned. Okay. So, the risk of quantum computers for DNSSEC is that they could potentially break your cryptographic algorithms that DNSSEC is using to verify the authenticity and integrity of DNS responses. So potentially, an adversary could re-sign DNS messages with a compromised key and then pretend that the message was real and coming from an authentic source. And as a result, people would end up at a wrong site, or software components would end up at a wrong site.

This, I should add, is something what we're assuming here is that we're already living in the post-quantum era. So, that's not now, but in the future. And this is not the store now decrypt later types of attack, but really an attack where you can almost in real time decrypt or compromise the keys in DNSSEC. But experts think that this won't happen for another 10 to 15 years. So, the question you might ask is why should we work on this topic now?

Next slide, please. And that's because adding new or replacing cryptographic algorithms in DNSSEC takes a very long time. So, this is a graph that comes from a paper where you see the development of a cryptographic algorithm in DNSSEC. So, from first initial draft in the IETF to a substantial level of deployment on the right. And as you can see, this takes roughly 10 years. And I think this is characteristic of infrastructure updates. And the same goes for introducing new DNSSEC algorithms. So, if quantum computers are going to become a reality in 10 to 15 years, we better think about what to do about that for the DNS now, today.

Okay. So, next slide, please. So, in addition to the time aspect, there is also significant deployment currently for DNSSEC. So, on the left, you can see which countries have signed their ccTLD with DNSSEC. The green countries are the ones that actually have it in operations, green and blue. So, that's roughly 48% of the world. And as you can see on the right, that's a validation. That's a map that looks a bit more red and amber. And that's because validation of these signatures has a lower adoption level. So, there's things to be improved there still. But as you can see, there is a significant

deployment of DNSSEC currently. So, this is kind of a thing in combination with quantum computers, especially if you assume that the validation will increase in the future, and also the signing on the left will increase in the future as well.

Next slide, please. So, if you want to protect the DNS against quantum computers, then we identify three strategies to do that. So, one is to what we call, we call them replace, redesign, and retire. Replace means, well, replacing the existing crypto algorithms in the DNS with new ones, the ones that are post-quantum safe. Redesign means completely redesigning the DNSSEC system, which is the second option in the table. And the third one would be Retire, which means getting rid of DNSSEC at all.

And all these three approaches have different pros and cons. So, for example, the Replace strategy is relatively easy to implement. It's standardized, but it has operational risks. And I'll be talking about that a little bit later on. Redesign is actually a clean slate kind of approach to DNSSEC, where you would use new technologies such as Merkle trees. It would reduce the operational risk, but you have to basically overhaul the entire DNSSEC system and protocols. So, that will take a long time.

And then Retire, well, that may sound easy, but it will also have an impact because if you get rid of the DNS, you open the DNS up to all types of attacks, which the DNSSEC attempts to protect against. And you might also affect protocols that depend on DNSSEC. So, in

our work at SIDN, we opted for the first option, which is Replace. So, that's why the first row is in green.

Next slide, please. And I'll be talking about that particular approach from now on. So, I'm not going to explain this figure, so don't be afraid. But what you can see here, what you see here is the interactions that take place between resolvers and authoritative name servers with the DNSSEC messages shown. And the messages with the red and yellow badges are the ones that have key material in there, so either signatures or public keys, and these are the ones that need to be updated.

Next slide, please. And to also give you a flavor of what these signatures look like, these are two examples. So, at the top, there's two current, there's a public key on the left. So, in gray on the left, there is a public key signed with a current, sorry, a current key that we're using in the DNSSEC. And on the right in gray is a signature generated by that key. And in blue, you see a public key and a signature that is created by a post-quantum algorithm, so an algorithm that is strong enough to protect against quantum computers. And as you can see, they're quite a bit longer. Okay. so, that's just to give you an indication or a flavor of what it looks like from a technical perspective.

Next slide, please. So, there are various quantum safe algorithms that are currently being developed, typically in the realm of the NIST PQC contest. So, this is the National Institute for Standards and Technology in the United States. And they have set up a

contest for cryptographers to come up with algorithms that can withstand quantum computers. We've been experimenting with a few of them. And as you can see in this table, so examples are MAYO Falcon, and SQSign.

So, the names are kind of funky, and there's more of them. But what we've been doing is we've been experimenting with these algorithms and validated there the time it takes to sign a zone file. So, for example, the .nl zone to validate DNS records. And we also looked at the signature sizes and the key sizes that were involved, because on the previous slide, you saw that they differ quite a bit, or they can differ quite a bit. And as you can see from this table, it's kind of a trade off, because if you do, let's say, small signature sizes, you get-- if you get small key sizes, then the signing speed might go up and the other way around.

Next, next slide, please. Here we go. So, this is the first experiment that we ran for the .nl zone. We tried signing the zone with, or we didn't try, we actually signed it with two post quantum crypto algorithms. So, that's Falcon and MAYO. You can see them on the right in the figure. I'm not going to talk about the details, but what you can see here is that it roughly takes twice as long to sign the zone with these PQC algorithms. So, usually, it's about 10 minutes it takes to sign the .nl zone, and with these PQC algorithms, it's 20 minutes. So, that's still quite okay. So, these are results that are okay from an operational perspective.

Next slide, please. So, this is where we currently stand at SIDN. And we identified a few additional work items that we would like to look into in the future, which mostly have to do with the size of these signatures and public keys. And we'd also like to study the validation time at resolvers in more detail, for instance, in combination with the role of caching. Yeah, I saw that. Thank you.

So, my last slide is a few suggested actions for the GAC. So perhaps you could work with the NIST, which is a US government agency, to explore how we could align the PQC algorithms that they are developing with the requirements of the DNS. And I know that these people are interested in this particular use case for them. Another potential action could be to incentivize the development of open-source software that would integrate PQC algorithms into DNS infrastructure. So perhaps this could be done through funds like NLnet or the Sovereign Tech Fund. At least these are the two I'm aware of that would sponsor such work.

Perhaps also stimulate deployment. That could be done, for instance, through a site like internet.nl, where you can check the properties of domain names or the properties of your internet connection. And it could be possible to also add checks for PQC readiness of your domain name. And finally, expanding on the previous slide a little bit, is that we also need to do more research on the operational impact of these new PQC algorithms if we follow the Replace strategy and what that means for the DNS and its operators, such as for the root zone.

Okay. Next slide, please. So, the software that we developed, so the experiments that we conducted we carried them out on a testbed and the testbed is open source. So, the software, you can download from our site. This is the QR code. And if you have further questions, you can reach out to me. And that was my final slide.

MARCO HOGEWONING

Thank you, Cristian. So, we can all just download some quantum software and play around, or quantum safe software. Nice. Yeah, no, thank you. My key takeaway is that we do have actions. Taking a view from our government's perspective in the Netherlands, what we're starting to do is asset management, as you briefly showed. DNS is, and it also came through from Warren's presentation, the DNS is everywhere. And that means DNSSEC is everywhere. And that means that this crypto basically sits in everything. So, we're very much already internally at work to try to build a list on where is it in case we need to replace it. And I can tell you from experience, that's easier said than done. With that, I have two questions. I have Barry here, and I have Peter online. I'll take Barry first.

BARRY LEIBA

Thank you. This is Barry Leiba from SSAC. Just one clarification that I want to make that I find whenever we talk about post-quantum cryptography, that this needs to be stressed, that there's a misconception that quantum computers put all of our encryption at risk. And I wanted to make it clear that as Cristian was talking

about signing and signatures, that that's a particular kind of encryption that is put at risk by quantum computers. The general encryption that we use to encrypt traffic on the internet is not at risk. It's specifically the types of encryption that are used for digital signatures and key exchange. And that's why we always stress those issues when we're talking about this.

CRISTIAN HESSELMAN Yeah. In particular, the DNS has specific requirements because everything needs to fit into a UDP packet, for example. And these are use cases that are not being considered by the folks at NIST. So, that would be an interesting way forward to reach out to them and take this, well, critical use case, I would say, into account.

MARCO HOGEWONING Thank you. And I've got Peter online, I think. Peter Thomassen?

PETER THOMASSEN Well, actually, I'm here. Hi. This is Peter Thomassen. I'm an SSAC member. So, I'd just like to add one aspect. The relative numbers of DNSSEC signing are actually low, like 5% in .com, for example. But if you consider the absolute numbers, it's still more than 10 million domains. And so, that's a significant number. And it is still unclear, of course, what the future signing method will be when DNSSSEC has to transition to post-quantum methods. But obviously, there will be some sort of transition. And now with more than 10 million domains that are signed today, or maybe by the

time the transition is needed, it might be more, it will be difficult to do such a transition in a way that is not well coordinated. So, what's important is to have this supported by automation.

And in the map that you showed, you don't have to go there, but the map had a few blue countries. And the blue countries have ccTLDs that support automation for such changes. So, one thing to consider is whether your country, I mean your specifically, but anyone's country wants to add support for such automatic transitions. And the SSAC, I suppose, will be happy to interact further about any such aspect. So just reach out to me or any other SSAC member if you're interested in that.

CRISTIAN HESSELMAN That's an excellent point. Thank you.

MARCO HOGEWONING Thank you. We still have a bit of time left. So, if there are any other questions. Nico, Mr. Chairman, go ahead.

NICOLAS CABALLERO Thank you. Thank you so much. And thank you for the wonderful presentation, Ram, and your team. Always a pleasure to have you here. So, two things very quickly. One is if we can arrange, Ram, Cristian, if we can arrange and taking advantage of the fact that I have my very esteemed colleague Jim Galvin in the room, if we can arrange a presentation for the Board for Muscat, for Oman, that's

in October. We might need to give a sort of like a vanilla version maybe, except for three or four Board members who are very strong in terms of technical background. That's on the one hand.

And on the other hand, and again, taking advantage of the fact that I'm sitting right next to my esteemed colleagues from Brazil, and we're organizing a regional capacity building session for Latin American countries in Sao Paulo or Brasilia, we still need to define that. But before or after Oman, would you be able to help us with that? We would basically be talking about DNSSEC implementation, and a short review on cryptography, symmetric and asymmetric, and the fact that the RSA, and I stand to be corrected, but about two or three weeks ago, apparently, I don't know if it's for sure, but apparently RSA was broken. I don't know if that is in fact the case, but I heard some stories.

Anyways, that's on the one hand. And on the other hand, the many advantages of open-source software for governments. I'm a big user, a heavy, fast user, but I struggle to explain in simple words to people without technical background about the advantages from a technical point of view, but also from an economic point of view, and many other things about the beauties of GPL-2, GPL-3, and licenses in general, and why it is a good thing. So, with your help and your expertise, we might be a little bit more successful. So, those two things, a presentation for the Board on the one hand, and help with our capacity building session, regional capacity building

session for South American countries, in this case, that might be happening in Sao Paolo or Brasilia.

RAM MOHAN Nico, thank you for that. We are strongly aligned with both of these ideas, and we'll be happy to contribute directly for both of them. Please come back to me, and I'll be happy to facilitate that.

CRISTIAN HESSELMAN Yeah, same here.

NICOLAS CABALLERO Now, sorry, but on the RSA breaking, could you please?

WARREN KUMARI Yes, I suspect what you're talking about is a paper which was published by Google fairly recently, and it's an academic paper which says that the bar has been lowered to crack RSA. It's nothing that's happened yet. It's just the amount of post-quantum crypto that you need, sorry, the complexity of the quantum machine that you need has been in doubt. How many quantum bits do you actually need in order to build a reliable system?

And what this paper said is you don't need quite as many as we had initially thought, but it's still very unclear how long in the future we need to be worrying about this. If you talk to a bunch of different experts, you'll get very different numbers, but it's not that RSA has

been broken. It's that it looks as though in the future, in some number of years, this is likely to be broken. But the actual estimates vary wildly. There is a page somewhere which I was looking for, where they've basically taken the average of a whole bunch of quantum scientists' estimations, and that number moves back and forth. But it could be tomorrow. It could be 50 years from now. It could be 500 years from now. It's very hard to actually predict. It's likely to be much closer to the few years, but again one of those hard predictions.

It's kind of like fusion. Sometime fusion energy is going to be coming in the next 20 years, but that's been true for the last however many years. It's definitely worth preparing now, though, because if it actually happens and RSA is easily broken, or any other crypto algorithms are easily broken, we need to have start preparing for that way before it happens.

NOCILAS CABALLERO You fix the roof when it's not raining, right?

MARCO HOGEWONING Okay. Thank you. We're two minutes away from coffee. I have one hand up from Australia. I suggest we quickly take that. Ingram?

INGRAM NIBLOCK Hi, there. Thanks for that. I was just wondering about the table on a previous slide, which had the different trade-offs. It's key sizes

and signing speeds and all that kind of thing. Key sizes, I definitely understand, because of, yeah, the UDP packet size limitation. I was just wondering, what's the practical effect of higher signing times? If it goes from, I can't remember what you said it was for .nl, from 2 minutes to 10 minutes. Is that a problem? Are you having to do that that often that it becomes an issue in the DNS?

CRISTIAN HESSELMAN Well, so we have 6.2 million domain names in our zone, and about 60% of them have been signed, and we have a publication window of about 30 minutes. So, we need to re-sign every 30 minutes. If the, let's say, the signing time would take a really long time, we might run out of time, basically. Yeah. So, that's why we wanted to know that.

MAARTEN AERTSEN So, this also depends on the deployment model. So, Cristian is describing a certain deployment model where they do the whole zone every-- But there's also deployment models where there's incremental signing or even live signing for each query. So, it's kind of a hard question to answer in general, but the speed matters.

PETER THOMASSEN Maybe the main point is, the longer the signing time, the more other changes you need to the deployment model.

MARCO HOGEWONING

Thank you. I hope this answers your question. We're out of time. Happy to see that the first appointments for a follow-up are already made. I suggest you go find our colleagues in the coffee break if you want to know more information. I believe there's quite a few people from SIDN here, and of course the SSAC is also here with almost full force. So, thank you once again, Ram, Warren, Greg, Maarten, and Cristian for all your wonderful information and taking us on this sometimes very technical journey and trying to help us understand what's going on.

Before I send you off to coffee, after the coffee in half an hour, we'll return for the WHOIS and Data Accuracy Session here in the GAC room. So, for the GAC colleagues, I hope to see you all back there. For everybody else, I hope this was informative. Thank you for attending and enjoy your coffee. Thank you.

[END OF TRANSCRIPTION]