ICANN81 | AGM – Joint Meeting: GAC and SSAC
Sunday, November 10, 2024 – 16:30 to 17:30 TRT

JULIA CHARVOLEN: Hello and welcome to the GAC and SSAC meeting. My name is Julia Charvolen from the ICANN GAC support team. Please note that this session is being recorded and is governed by the ICANN's Expected Standards of Behavior and ICANN Community Anti-Harassment Policy.

During this session, questions or comments will be read aloud if submitted in the chat pod. Interpretation for this session will include six UN languages and Portuguese. If you would like to speak during this session, please raise your hand in the Zoom room. Please state your name or the language you will speak, if other than English, and remember to speak at a reasonable pace. I will now hand the floor over to Nigel Hickson. Nigel, please, over to you.

NIGEL HICKSON: Hello, good afternoon. And you've heard quite enough of my voice, haven't you, today? So, you won't be hearing too much more of it in this session. And I promise I'll be quiet tomorrow. So, Nico sends his apologies. He's had to attend a session of the ICANN board. But I haven't really got much to do. As you can see, the sort of ratio of GAC to SSAC is as it should be. And no, this is a session that is SSAC's session.

We're absolutely delighted to have the opportunity for a briefing from them. Over the years, they've done so much work to contribute to the

effective running of ICANN. And I'm sure you're going to find what they have to say really interesting. So, all I'm going to do for now, I mean, I'll moderate the questions and the arguments later. But all I've got to do now is hand over to Ram.

RAM MOHAN: Thank you so much. And thank you for inviting the SSAC to meet with you here at the GAC. It's always a pleasure to be with you. My name is Ram Mohan. I'm the chair of the SSAC. Before I get started with the agenda here, let me also turn to my colleagues who are arrayed here and ask them to take a moment to introduce themselves. They're all members of the SSAC. And, you know, you'll get a chance to see the diversity of knowledge, experience, and expertise here. Let's start to my right.

ROD RASMUSSEN. Rod Rasmussen.

MERIKE KAEO: Merike Kaeo.

GREG AARON: Greg Aaron.

ROBERT GUERRA: Robert Guerra.

WARREN KUMARI: Warren Kumari.

JOHN LEVINE: John Levine.

STEVE CROCKER: Steve Crocker.

TARA WHALEN: Tara Whalen, SSAC Vice Chair.

BARRY LEIBA: Barry Leiba. And I try, but Warren has a better hat.

SUZANNE WOOLF: Suzanne Woolf, who sometimes wears too many hats, SSAC.

RAM MOHAN: Thank you, Suzanne. And there are a couple of members I see also there in the back. You'll see them raising their hands. They are also here in the room to be with us in this session. Najman, thank you for having us here. Gabe, you didn't raise your hand. You got to raise your hand. Come on. Thank you for having us here. We thought we would first, given that not all of you have seen us before, we thought we would

spend a couple of moments introducing ourselves, who we are and what we do, and then go to the rest of the topics.

So, if you look at ICANN's own mission, that's fairly clear. The SSAC is chartered directly under the mission of ICANN. So, we are an Advisory Committee, just like you are an Advisory Committee. And we do not have a kind of formal power, if you will, inside of the ICANN structure. We like it that way because our advice then has to live and die on its own merit rather than on having a vote or not having a vote, right? So, that is who we are.

We are constituted from all around the world, or at least most parts of the world. We are on a path where we're increasing our diversity in the membership in all the ways that you measure diversity. This year alone, we've added nine new members. And of those nine new members, we are so pleased to see that two of them come from Africa, other parts of the world as well. But the fundamental reason why people are in the SSAC, are selected to be in the SSAC, is because they bring specific and, in general, deep expertise in the area that they specialize in. Most of the folks in the SSAC are technical experts.

They have a variety of experience. We have people who touch various areas of the Internet Identifier System. That's mostly who we draw from. But a great deal of knowledge and expertise that stays inside of the SSAC. And the reason for that is because we primarily focus on providing technical advice to the community that we serve, right? So, therefore, we try to have a bunch of technical people with expertise on board. Thank you.

This is the leadership team for the SSAC. You will see, to my left, to your right, you'll see the members who are selected and who have been elected to be inside of the leadership team. What you see is also the Policy Support Staff. And I want to take a moment to mention this. Unlike many other parts of ICANN, where the support staff end up being in a support role, inside of the SSAC, you look at the people who are listed here, Steve Cheng, for example, other people who are here are eminently qualified experts in their own right.

So, they end up participating, contributing to the discussions that we have, and doing more than only being a scribe. They will often provide very helpful guidance and provide helpful input as we work on the various topics that are of interest to us. And if you look at the skills just from this Leadership Team, you will see the collection of them. But if you look at that across all of the SSAC, there is an even larger variety of it.

We have folks who come from academia. We have folks from civil society, from business backgrounds, from government backgrounds, law enforcement backgrounds. And the general way that people end up getting into the SSAC, there's an open application process. They put their applications in. There is a membership committee inside of the SSAC, and that membership committee sorts through the applications, conducts interviews. And once those interviews are done, they recommend people for membership in the SSAC.

The SSAC gets to opine on these folks. And when we get through all of that process, we provide a list of those recommended members to the

board. Every SSAC member is appointed by the board of ICANN. So, I'm going to ask Tara to come in on this topic, because this is at the core of what we do.

TARA WHALEN: Thank you, Ram. So, for those, I guess, who don't know the SSAC, we produce a great deal of technical material and have been doing so for some years. And the topics may vary. They are about Security and Stability of Internet Identifiers over a range of topics. But there are some topics that come back over and over again and are pretty much our evergreen topics. And so, we're finding ways to focus on these and make these materials readily available to the community.

So, as these recurring important topics evolve, you can come to us and get answers to your questions. So, those topics we've outlined here, one of those is DNS Abuse. Of course, the DNS is a significant system, and that makes it a place where significant amounts of online abuse also happen. It's a useful tool for people who want to do a great deal of damage. So, if people are doing phishing attacks, people are distributing malware, then we're looking at how does the DNS play into this, and what might we do for mitigations. So, this is an area where we quite often are putting out advisories and working with the committees to try to mitigate that harm.

A second area, which may be on the minds for many people who are looking forward to the next round, is New gTLDs. So, every time you are going to be adding new names into the system, there are security and Stability issues with those. People may have been following the names

collision analysis project, for example, looking at what will happen when there is an expansion. So, we don't want to have issues with sort of confusion over strings. So, a lot of work goes into anticipating these issues. And this being a very timely issue, we are asked for advice on this topic.

There is also DNSSEC. So, this is one of the core security technologies in the DNS space. We, along with others, have been working in this area to give advice over some time, promoting this technology, trying to make sure that it rolls out well, that it is implemented well. We recognize that it is complex, and people often need some help to try to get this to work the way it was intended. So, we would like to ensure that people have good advice. There may be things like running out better automation, for example, to make it easier for people to put in this security functionality and make it, again, readily available.

There's also the issue of Alternative Namespaces. People may have seen this in the recent years when blockchain was very much in the news. This certainly hasn't gone away. But there were a lot of other naming systems that were not identical to those provided in the DNS. People were doing things for cryptocurrency and allowing you to buy different sorts of domains, which, of course, come up with issues around, then how does this, in what ways does it interact or integrate with the DNS? How will we anticipate the various issues of the coexistence of these systems? So, we continue to look at this because this is very much an evolving space.

And finally, one topic that may be on the minds of many people in this particular audience is the issues of Internet Governance, but particularly those around security and stability, this being the focus of our group, because there are many issues in the internet of which there is an overlap of the technical and the policy space with a lot of very complex questions on both sides. And if you are going to be making decisions in this space, it is very helpful to have clear and useful guidance from technical people to help inform you while making that policy.

And we would like to be in a position to provide that information from our technical perspective. But we also note that our work is stronger when we have input from the people who are needing that advice to try to direct it in the right ways, to be sure that we're answering the right sorts of questions, to be sure that we are landing the message with the right level of communication at the right level of detail.

So, we very much appreciate when we are able to interact with, or for example, speak with, bring in invited experts to consult with people as we develop some of our advice so that in the cases in which they are meant to be useful to an audience in a policy space, then it very much is a collaborative side in order for us to produce the right sort of advice that is helpful to the audience.

So, right now, we have a couple of work parties that are producing some work. Our work often may straddle more than one of these areas, by the way. But two of the initiatives happening right now is a group on free and open-source software in the DNS infrastructure. So, some of

you may know that many of the components that are rolled out in the DNS infrastructure, things that may be in resolvers, for example, a lot of these components are part of open-source initiatives. These can be large or small groups with different amounts of funding who may have different sorts of liabilities, contractual agreements, and relationships with different parties. And this is a piece of critical infrastructure for running the DNS.

So, we thought it would be useful to make it manifest where some of these dependencies are so people can kind of see where are these pieces of open-source software, where you are reliant on them, and also to maybe question some assumptions that people have about those pieces of software, what they can and cannot do, and what you might be thinking about the reliability and the strength of these pieces of software.

Now, we do have at least one of the chairs of the party here. Martin is not here. We have one. Okay, just checking if I have correctly-- Yes, the chair has given me a thumbs up that I have correctly summarized the work parties. So, that work is just beginning. And so, we're hopeful that some of you will be looking for the outcomes when they come out if you're interested in open-source software. Another one that we are working on is sort of DNS blocking and filtering. So, one of the mechanisms for doing content blocking online is DNS is used as one of the approaches for managing content blocking between end users and the resource.

And this has been going on for some time as a technology, and SSAC has looked at this, but the last advisories that we put out are over about a decade old. And since we last wrote about it, the technological landscape has changed, the regulatory landscape has changed. So, we thought it was time to look at these things again.

So, many in the technology aspects, for example, many of the DNS queries are now running over transports that make it less obvious. People can't look at the queries the way that they used to. So, this has perhaps then changed the responses and the information that people get when figuring out how to do content blocking.

So, this is definitely an area where having input, we have been talking with people in the policy space. We were fortunate to just recently being discussing with the policy folks at ICANN, what they've been hearing from what they've been following as they keep abreast of the policy space. And we're very grateful to have that type of input to inform the direction that we can move the documents so that it is again addressing those most pressing questions. And so again, we reiterate, we like this collaborative process.

So, that's the high-level view of our topics. We do have a deeper level, one that I said someone else will take on, on the next slide.

RAM MOHAN: Before we go to the next slide, Nigel, I wonder whether we want to take a moment here and ask if there are any questions or interventions that folks would like to make.

NIGEL HICKSON: Yes, thank you, Ram. I was going to do that because we've had quite a bit of information. It's very interesting how you have stable topics that you come back to because they're all very pertinent. So, any questions or observations before we dig in deeper to AI and blockchain issues? You'll have to shout out if there's any online. Daniel? Oh, our friends. Yes, European Union, please.

GEMMA CAROLILLO: Thank you, Nigel. Gemma Carolillo from the European Commission. Just a brief comment. First of all, it's very good to see that most of what's on your plate, it's on our plate. So, perhaps we should see you very often, more often than we do today. And then the other quick question on, since I understand the work on security of open-sources just started or recently started, and this is a topic of high interest for us, whether we can have a pinpoint, whether a moment to reconnect and have more information on this work. Thank you.

BARRY LEIBA: Okay, I'll take that one. This is Barry Leba. I co-chair the Work Party that's going to be producing that document. Yeah, we'll be happy to present this to you periodically as we progress. We hope that this particular Work Party goes quickly and we should within the next two ICANN meetings be done with it. So, perhaps next in Seattle, we can give you an update on where we are.

GEMMA CAROLILLO: Just to say, that would be great, thank you.

RAM MOHAN: One thing I'd like to add on top of what Barry just said is, there is also an opportunity for the work parties at the discretion of the chairs to invite experts or invite folks who have information to come and provide a briefing that could be informative for what the Work Party is doing. So, there is an opportunity to do that perhaps intersessionally as well, Barry.

NIGEL HICKSON: Any more? Well, there'll be opportunities to come back after the next session. So, Ram, back to you.

RAM MOHAN: Thank you so much. So, let us now move to the next slide. Jeff Bedser was planning to be here to present this, but he's unfortunately not feeling really well. So, I will take this part. We thought it might be useful for you to hear some of our own members' views on AI and DNS Abuse. The SSAC as a committee has not commissioned a Work Party to go look at this topic and provide consensus advice from the SSAC.

So, what you're going to see here in the next few slides are drawn quite a bit from the expertise of some of our own members. So, this is not speaking with the voice of the SSAC, but it is speaking with the technical knowledge and expertise of some of our members in the SSAC. So, just as an early level set, there is machine learning and then there is artificial

intelligence. And machine learning is a subset. And in that subset, algorithms learn from data to make predictions or decisions. While AI encompasses broader technologies that enable machines to mimic human intelligence. So, machine learning is a key method within AI.

Now, DNS Abuse might actually be a pretty good application for AI. It might be exactly the kind of thing that folks who want to be criminals or who are already criminals want to use and leverage. Because AI, especially generative AI, has a pretty good way of creating new text, images, videos, other artifacts. For example, very accurate logos of banks or e-commerce sites. And doing that along with the capabilities of generative AI and the machine learning, the pattern recognition that is there in machine learning, allows for the AI systems to create emails, text messages, other prompts that look almost like it was written by a human or created by a human. And the more authentic you can make it, the more likely it is that the targets are going to fall victim to it.

And again, with generative AI and its own ability, in the past, it used to be, when you got a phishing email, you could almost depend upon some imperfection, something that is crafted incorrectly, grammar that is off, spellings that are off, capitalization that is not right. But now, not only is all of that done well in the base language, but it can be translated automatically into a whole bunch of other languages. And that means that the scale and scope of the problem expands quite dramatically.

So, really, you look at DNS Abuse, fighting DNS Abuse at scale has, until now, used pattern recognition, pattern matching as the primary mechanisms to fight DNS Abuse at scale. So, for instance, you look at

information underlying a domain name or underlying the particular level of fraud that is happening. NS records, the host names, the IP addresses associated with it, who is the name or the resource registered with, which is the registry or the registrar. You find patterns or you analyze the content. You look at the HTML file, you look at the templates, they get reused or you look at file hash values because of humans doing it in the past, there were accessible and repeatable patterns.

With generative AI, each specific domain or URL can be completely randomized. Each phish that goes out, and we're talking about 100,000 phishes that get generated within four hours, often name being added to a zone file. In the past, it would be that you had one phish being sent to 100,000 targets. Now you can have 100,000 individual messages that get sent out, each one of them looking authentic, each one of them looking like it has come from a human, written by a human. So, pretty effective ways to lure targets.

What are some other uses of AI for abuse? So, we're seeing that AI is also, newly it's being used for sock puppeting, creation and use of fake identities, fake accounts, fake reviews. Combine that with the registration of domain names and hosting accounts. It's also being used for non-consensual intimate imagery, as well as CSAM. And fairly straightforward use in falsification, fabrication of data, fabrication of documents, fabrication of pictures. And you can create these identity documents or other documents in some jurisdictions. For example, you have country codes that say, you must provide identity in order to have a domain name.

Well, now that identity can be generated without too much trouble. So, one of the security ways that has been created can be circumvented fairly quickly. You will also note that, perhaps you've noted, but you'll note that the images that are accompanying all of these are generated by AI and they are linked to the content in there. But you'll find that some of the images look realistic, some of them don't, but it's getting much better. The same set of prompts two years ago, the same set of prompts six months ago would have produced images that would not look like they were generated by a graphic designer.

A little hard to read everything here on this slide, but this is some data that comes out from a research report that speaks to the frequency of tactics for misuse that uses generative AI. As you can see, the largest frequency of it is an impersonation, but it's also for scaling and amplification of existing attacks, falsification, and so on. I have spoken to that, pull those out in the previous slide, but this slide takes you all the way to the very end of it. So, it's being used quite extensively.

And as a prior presenter of this presentation is saying, the images generative AI seems to be generating darker and darker images. As we go further into this slide set, we didn't try to do it. That's what it did. So, perhaps there's a signal there. So, even though the capabilities might not always lead to more sophisticated attacks, we do think that generative AI has the potential to increase the scale and the reach of it. And we say here, cyber criminals will progressively integrate. We're wrong. We should have said, have already integrated AI techniques and already use AI systems in their plans. That's what we're seeing in the wild. But it's not all bad news. With the exception of the images, and

you'll see faces now formed. This is what we asked it to, again, we told the engine, with everything that you've seen so far, generate this, that's what you got.

So, as much as AI machine learning can be used to increase the scale and the frequency of these attacks, AI can actually be quite effective at detecting phishing emails. And the fact is that AI-generated phishing emails, at least in its current avatar, in its current generation, they are different from regular emails that humans generate. And they're also different from manually generated phishing scam emails. And if you combine machine learning and natural language processing, that actually helps generative AI tools to understand, process, and then manufacture texts that read and sound human and authentic. So, knowing that that technology exists, you can deploy AI to catch AI. And that's really where it's going.

So, attack vectors and strategies that use AI for abusive purposes, many of you, if not all of you, are already familiar with this. Political disinformation, it's quite easy to have that be generated. You don't need humans to do that nearly as much anymore. Of course, profit-oriented abuse and scaling and speeding up of criminal enterprises. But at the end of the day, cybercrime is directly correlated to the money that cybercrime ends up creating for the perpetrators. And so, folks change strategies whenever necessary to ensure profit.

So, even as AI is deployed to catch these kinds of problems, we will see that evolution will happen. And AI itself is evolving very rapidly. But overall, our view is that this is really a continuation of the same

threatscape that has existed as long as technology has come through. You have actors who decide to use technology and leverage technology for gain in some way, for advantage in some way. And really, the job is to make sure that we stay abreast of what's happening and then deploy measures that can mitigate, if not counter, these kinds of threats.

So, I just spoke about AI and the DNS. I'm not going to spend a great deal of time on blockchain and the DNS. We've spoken about this in other fora here inside of ICANN. There is a report that we have published, SSAC123, that is available. We also hosted a panel at the 2024 SSAC workshop in Washington, DC in September of this year. That is also public. It's recorded. It's available in public. And that was a panel that included experts in the blockchain space today. It included somebody from ICANN's Office of the Chief Technology Officer.

So, there is a great deal of collaboration that's happening between the SSAC and ICANN's OCTO to make sure that we have alignment on the areas of research. We don't coordinate in terms of the exact output of the work that we're doing, but we try and make sure that we're not duplicative in our work.

So, I'll go to the next slide. And this is, at least from my point of view, the most important slide, the biggest ask of you in the GAC. Over time, we found that policymakers, in particular, have a need for capacity building. They would like to be informed on key topics of importance and be informed by people who actually know what they're talking about, but who can talk about it in a way that is accessible to them, not

to just spout jargon at you. We have the ability. We have the opportunity to do that.

We also provide reports. We create reports. But these reports often tend to be dozens of pages long. What we're in the process of doing is distilling those into 500-to-1,000-word summaries, a page or two, and pull that together. But what would really help is if you tell us, as policymakers, if you tell us what are the most important topics for you, because we have 126 papers that we've written, and we don't think it's efficient to just go and compile summaries of those. Tell us what would be valuable for you, and we would love to work alongside you to help provide briefing papers for you and for your audiences.

And finally, we would really like to open up to working with you and your government. You may be having important meetings on topics that speak to Security, Stability, and Resiliency. One of the things, doubtless, that happens for you is you enter into some of these meetings, and you have other colleagues or other policymakers who come in who are not sufficiently informed about the actual facts, but who have no problems providing advice on what should be done about that particular area. And what you find then is a mismatch between a policy solution and actual technical feasibility. And we think that it would be best advised if, as you help create policy, that that policy is based on the hard facts, the actual data that can help inform you as you and your governments help build these policies.

So, we would really like to open that channel with you and offer both the breadth and the depth of the technical expertise that we have beyond just the documents that we provide. Back to you, Nigel.

NIGEL HICKSON: Thank you so much for that detailed overview. And picking up the sentiment at the end, I think it's clear that we, as policymakers, are greatly indebted to the advice we get from the technical community, from the advice we get from other parts of ICANN. I can recall well a few years ago, and going back a bit now, when we were discussing DNS Abuse in terms of the New gTLD round and other issues that your SSAC report, and I can't remember the number of it, but I do remember reading it in detail and the recommendations that you came up with on DNS Abuse were influential in the advice that we came up with in our meetings.

So, I really do think that there is a lot of scope for us to work better together. I also can reflect on the great interest there was on blockchain in particular and DNS Abuse and work on that. And that's no doubt a topic that we will come back to in due course. So, thanks so much for finding us on those issues. I will now take sort of questions and comments from around the floor. And I think, our friends in the Netherlands.

ALISA HEAVER: Thank you. And thank you for the presentation about all the work of the SSAC. And it should be on the top of my knowledge, but I'm actually not

sure if there's a GAC liaison to the SSAC or the other way around. If there isn't, I think that could already help quite a lot.

RAM MOHAN: Thank you for that. I don't believe that we have a formal role like that. We certainly would welcome that if you would like to do that. The one thing that we do inside of the SSAC is that anybody who, even liaisons, incoming liaisons end up going through the same vetting process so that they can be full scale members and participate. But you have plenty of expertise amongst you. So, I think that would be helpful. We do have Gabe, is sitting right in front of you. Gabe is an SSAC member. So, he, in some cases, acts as an informal information transfer that happens, but certainly not in a formal way.

NIGEL HICKSON: Thank you so much for raising that pertinent question. And I think the answer is we don't at the moment. But it's certainly something we can look at, because it does strike me that it's important. I mean, you're a very transparent advisory committee and your papers are well publicized. But even so, having some insight into the work you're doing is probably pertinent. I'm useless with my glasses or without my glasses. But anyone else? Ah, was that you? Ian, or no? Yes, go on. And then in front of you. But Ian first.

IAN SHELDON: Sorry, Nigel, there's a queue forming online. Just wanted to direct your attention there. But I was also at the front of that queue.

NIGEL HICKSON: You go for it then.

IAN SHELDON: Thanks, Ram. GAC Australia, Ian Sheldon here. Thank you for the offer of assistance. I see a great deal of depth and expertise up on the stage. As you'd be aware, GAC members often have quite a large file. We look after a lot of things, both within ICANN as well as outside of ICANN. And so, I was curious to hear your thoughts on the offer of expertise and support. How broad is that remit? Are we talking about just DNS issues, or able to tap into some of that expertise that might sit slightly outside of this forum here?

RAM MOHAN: Thank you, Ian. Great question. So, insofar as SSAC itself is concerned, we will stay within our remit and what we have. But you have access to our members. And should the members be willing to help you on topics that are outside of the ICANN area, more power to both of you.

NIGEL HICKSON: Thank you, Ian. And let me take the US in front of you. And then I'll go to the list on the line list.

LEONARD HAUSE: Yeah, Leonard Hause, US State Department. When the generative AI combination with the DNS Abuse, have they made any best practices of

how this could be, either through the registration process or somewhere along the line, they can dig a little deeper and get to the root of where this stuff begins, whether it's some sort of Turing test or something like that, that is able to go through and nail the generative AI before it gets turned loose, if you will. So, just a question as part of the reports on whether the best practices in that space. Thanks. Thank you for the great work on that.

RAM MOHAN: Thank you. I don't know the answer to that question. But I can ask the experts inside the SSAC who do study this topic and come back to you on that. One thing inside of the ICANN space that at least ought to be part of the consideration is, if it is true that with generative AI, you can have within a few hours of a domain being added to the resolution, you can have such a huge number of abusive messages go out. Are there things that can be done inside of the ICANN space to mitigate that quickly? If the abuse is happening within hours, is it possible to mitigate it within minutes of that being detected? I think that's an open question that we should address here.

NIGEL HICKSON: Thanks very much. And thanks for that answer. I've now got two or three people online. Gemma from the European Commission first.

GEMMA CAROLILLO: Thank you very much, Nigel. Since you were asking about possible topics of interest, I was thinking here in the GAC when discussing DNS

Abuse among the others, we have discussed about the use of predictive tools. And from the European Union, we have some experience in that. It would be really good if there is already material or if there is a space for further work in the potential of predictive tools to prevent DNS Abuse before we get to mitigation. And then I just wanted a small clarification. If I understand correctly, with the use of AI and generative AI, we are not really expanding the threat landscape. It's more, I would say, massive number of attacks that you can get, but they are not getting more sophisticated. We don't have more threats, at least to report at the moment.

RAM MOHAN: Thank you. For the second question, yes, that's true. We don't believe that the threatscape has expanded, but the volume frequency, that scaling has dramatically expanded. For the first question, are there any members here from the SSAC who would like to respond to our colleague?

GABRIEL ANDREWS: I can give just a brief law enforcement perspective. But what we see is very similar threat groups, the same criminal groups that were doing things manually or just adopting the AI tools to do it more efficiently, just as the good guys do. And so, it's not that anything that we're observing is particularly new. It's the same old tricks, just using new tools to accomplish them, is really the general takeaway that we have right now from our visibility at this time.

RAM MOHAN: Thank you, Gabe. I'm just wondering, I think you should restate that first question so that the other members pay attention this time and then can perhaps respond.

GEMMA CAROLILLO: This is very kind. Thank you so much. And I'll try to formulate it as clearly as I can. So, since you asked about potential topics for work from the SSAC and briefings that could be useful to the GAC. In the GAC, when discussing DNS Abuse, we have sometimes referred to the existence of predictive tools to prevent DNS Abuse before we get to the mitigation phase. And hence, I was wondering whether there is material you have at hand or further work that could be conducted in the area. Thank you.

RAM MOHAN: Thank you. Does anyone want to comment on that? Benedict and then Steve.

BENEDICT ADDIS: Hi. Benedict Addis. I failed to get a spot on the rostrum. So, there are some bits of DNS Abuse that lend themselves really well to prediction. So, particularly botnets and malware use very predictable algorithms to generate domains weeks, months, and years into the future. Now, those domains don't exist. They're called DGA domains. We can predict them really accurately. But I would caution you, any tools that claim to

predict badness in a more general way using magic fairy dust AI, I would be very careful of. So, there are some areas that lend themselves well to prediction. But not broadly.

RAM MOHAN: Steve?

STEVE CROCKER: Thank you. In order to operate a predictive process, you have to have access quite quickly and agilely to the registration data and to the registrations themselves. We're in a very frothy period, I would say, with very heavy emphasis on privacy, which is well-intentioned to protect against various forms of harassment, spam, et cetera, et cetera. But at the same time, it's made it difficult, somewhere between difficult and impossible, to get access to the data for legitimate purposes, particularly for some of these purposes, like doing predictive analysis and correlating across domains.

So, there's some tricky, not easy questions that have to be pursued in how do you provide access to the information so that you can do a good job of the kind of predictive analysis you want, and at the same time, still be protective of privacy. So, there's an interplay between these two ideas.

NIGEL HICKSON: Thank you very much. Thank you for the question, which generated some really excellent responses. I think our friend Santosh from India was next.

T. SANTOSH: Thank you, Nigel. Thank you, Ram Mohan, for the detailed presentation about AI and DNS Abuse. So, let us start with the basics. Now, can AI help in working on the accuracy of who is because that is the basic issue which the malicious actors use, because most of the who is not accurate. So, can we have a system in place where the AI tool can say that, okay, this is not WHOIS accurate, so the domain can't be delegated? Thank you.

RAM MOHAN: Thank you. So, the specific response to that is certainly you can take AI or other machine learning algorithms and apply them to a database and compare them to real addresses, people, et cetera, and come to some level of conclusions. But as Steve just said, much of that data is now obfuscated or unavailable. So, even if that technology were present today and accessible, the datasets that would inform those tools, those datasets are just not available.

BARRY LEIBA: And a quick adding to that, Ram. Not only is the data you need to check not available, but the data you need to train your engine is not even available. So, it's a double problem.

GREG AARON: I'd put it a different way. The contact data for domain names is not available to most of us, for example, to security companies, to law enforcement, if it's not available in WHOIS, for example. However, there are parties who do have the data, which is the registrars and the registry operators. And we have registry operators and registrars right now who do accuracy checks using a variety of methods. It's done by .nl in the Netherlands, for example, .uk. So, now we have basically the registrars, especially being the parties who can do checks for accuracy and potential cybercrime.

They have the WHOIS data, they also have the purchase data, such as the financial tools used to register the domain names, source IP addresses and other things. So, the potential to use AI is there, but it's now in the hands of those parties.

NIGEL HICKSON: Thank you very much indeed for that. We've got two or three other questions in the chat, so I'll carry on with those. We've got seven minutes time, or six actually, because we will need to sum up. But I think, I don't really understand the order of these things, but Marco, why don't you come in?

MARCO HOGEWONING: I'll be very quick and brief and echo my colleagues and much appreciate the SSAC for being here and also, you're extending your hand and helping us. You asked a simple but likewise difficult question, what do

we find important? Everything, it's about picking your favorite child I feel, it's a really hard question to answer. I do appreciate SSAC's work, especially in helping us understand the impact of new and emerging technologies on the stability of the DNS system and the internet at large. But on priorities and taking a step back, on one hand, I would love to hear whether SSAC in that sense also looks at some of the global dialogues we have and some of the global processes, for instance, the recent published Global Digital Compact.

And in terms of where you think important work can be done to help us all, but likewise also whether you see an opportunity for SSAC to contribute to some of these ongoing global conversations, for instance, the WSIS review or several WSIS action lines also allude to the security and stability of the system. Thank you.

RAM MOHAN: Thank you so much. Internet Governance and the Security and Stability and Resilience Aspects of it is one of our five areas of constant attention. So, we would definitely want to engage on that. We don't have a structure by which we end up sending a liaison or sending somebody into those areas. But we now have members who pay attention to that, who are directly engaged in that in their day jobs. And that informs quite a bit of what we do. And in fact, it's part of that is what led to the creation of our open-source Work Party was one of our members recognized that there is some focus on this at the governmental level. And so, it might be useful.

BARRY LEIBA: Now, I'll answer that. Basically, three ways that the SSAC decides to work on something. One is that there's one or more SSAC members who are interested in it and propose it. One is that the board asks us to look at something. The other is the community asks us to look at something. And obviously, we can't do everything. But if we get some community members coming in and saying, this is really important to us, would you take a look at it? That's a possibility.

NIGEL HICKSON: Thank you. We've got a couple of other questions. Owen from the US.

OWEN FLETCHER: Hi, Nigel. I think Wang Lang was before me.

NIGEL HICKSON: Oh, right. I do apologize. I'm sorry, Wang Lang. It's my inability to understand the ordering of these things. Go ahead, sir.

WANG LANG: Thank you, Nigel. Thank you, Owen. I want to thank Ram for the fantastic presentation. You just mentioned the blockchain, the DNS, but did not dive in. And we know ICANN accept it unstoppable as the accredited registrar. So, my question is, what's your take of the future of Web3 DNS? Thank you.

RAM MOHAN: Thanks. So, the SSAC has not produced a report specifically about blockchain, but we did produce a report about the evolution of DNS and new technologies. And in general, our approach is technology will evolve. We ought to embrace these new namespaces rather than say that we should be protective only of ours and stop everybody else. However, what is important is, should other Namespaces want to integrate into the DNS Namespace, it has to be done in a responsible way. It has to be done with stability and security in mind. So, at a high level, that's the way we look at it. There are other artifacts and other issues that would exist. Were we to produce a report just on blockchain, I'm sure there'll be other issues that get uncovered. We haven't gotten there yet.

NIGEL HICKSON: Thanks very much indeed, Ram. Over to Owen.

OWEN FLETCHER: Thanks, Nigel. This is Owen Fletcher from the United States. I think this has been a fantastic session and AI and DNS Abuse is a perfect example of a topic where the SSAC's technical expertise can really benefit us in the GAC trying to develop evidence-based, well-informed positions on types of things that the GAC might want to comment on.

So, I think it would be great to have more interactions like this, perhaps including in Capacity Development Sessions that the GAC holds. And I saw another comment to that effect in the chat. Ram, the presentation described some types of abuse, obviously, that are not DNS Abuse as

described or as defined at ICANN, although many of the things could be used by people committing DNS Abuse. But just in terms of DNS Abuse under the ICANN definition, would you anticipate that what I understood from the presentation to be as sort of an accelerating pace of creation of bad domains to lead to any increase in reported abuse cases? Like, should we keep this in mind when we look at statistics and reporting about DNS Abuse in coming months or years? Thanks.

RAM MOHAN: I will just speak personally, because SSAC doesn't have a position on this. But personally, I think it's a logical next step. When the technology enables the complexity and scale of it to become so simple, then you can expect, because there's so much money to be made. I mean, Jeff Bedser, in a comment yesterday, was saying that the value of a good fish is about $20,000. So, if it costs $200, $100, even $1,000 to register a domain name, it's not necessarily enough of a deterrent. So, I think if you take the logic chain, we can expect to see quite a lot more of these kinds of abuses happening and reports happening. That's my personal perspective. Are there other, Merike?

MERIKE KAEO: Yeah, from a personal perspective, I mean, I do security on a day-to-day basis and I basically trust nothing. But it's been really interesting to me. I don't filter my spam because I want to look at campaigns and things that are happening. And what is really interesting, it has to be AI that's causing this, but the type of phishing emails are getting extremely believable. And I believe also that they're actually looking at what

you're posting on Facebook or LinkedIn and actually potentially targeting specific organizations, specific leadership, so that they have the intelligence, what is more believable. And I think that is something where also the quicker that we can act to detect and deter, is something that's really important.

NIGEL HICKSON: Thank you. Thank you so much, Ram. I'm afraid we'll have to leave it there. We've run out of time, but this has been really, really productive. It just shows what an interest there is in the incredible work that you're taking forward. And it's great to see such experts on the table. I'm always proud to sit on the table with Dr. Steve Crocker, just an inspiration that so many of you have contributed to not just ICANN's work, but the Technical Community work on so many issues.

So, thanks coming in again. This won't be the last. Thank you for your kind offers to follow up on various issues. And with that, I think we better close the meeting. Although my esteemed colleagues at the back, could you tell us when's the meeting session in the morning? Could you just remind us when we're?

JULIA CHARVOLEN: One minute. Do you know?

UNKNOWN SPEAKER: Yeah, it's at 1:15. There's still the welcome ceremony, Joiner Political Forum before that, but the GAC will start at 1:15 local time for a discussion on WHOIS Registration Data Issues.

NIGEL HICKSON: Lost the time.

RAM MOHAN: Nigel, thank you so much on behalf of the SSAC for having us here. We hope this is not the last time. We look forward to further engagement.

[END OF TRANSCRIPTION]