ICANN73 | Virtual Community Forum – GNSO: BC Membership Meeting
Tuesday, March 8, 2022 – 14:30 to 16:00 AST

BRENDA BREWER: Good morning, good afternoon, good evening. Welcome to the Business Constituency membership session at ICANN73 on Tuesday, the 8th of March, 2022, at 18:30 UTC. My name is Brenda, and I am the remote participation manager for this session. This meeting is recorded.

To ensure transparency of participation in ICANN's multi-stakeholder model, we ask that you sign into Zoon sessions using your full name—for example, a first name and last name or surname. You may be removed from the session if you do not sign in using your full name. Please note that this session is being recorded and follows the ICANN expected standards of behavior.

If you would like to ask a question or make a comment verbally, please raise your hand from the reactions icon on the toolbar menu. When called upon, kindly unmute your microphone and take the floor. State your first and last name clearly and at a reasonable pace and mute your microphone when you are done speaking.

And now I am pleased to introduce the Chair of the BC, Mason Cole. Thank you.

MASON COLE: Thank you very much, Brenda. Good afternoon, good evening, good morning to everyone. Welcome to the BC call on the 8th of March, 2022.

And further welcome to ICANN73. So it's a pleasure to have you all here. A special welcome to our guests who are not BC members. This is an open meeting and you're more than welcome to participate in our call. So it's pleasure to have you with us. You see the agenda is front of you. We have 90 minutes today, so it should more than enough to cover our agenda.

But before we begin and before I introduce our guest, are there any changes or updates to the agenda as you see it on the screen?

Okay, I see no hands. All right, let's go ahead and dive in then. We're very lucky today to have Marciej Korczynski with us from the University of Grenoble, who, as I'm sure you already know, is the author of a study on behalf of the European Union on domain name system abuse. Marciej's study was published recently. It's been under consideration by many of us in the community. And I know I know we're looking forward to hearing his remarks. Marciej is going to present to us a bit about his findings for the next 15 minutes, and then we'll have 15 minutes of Q&A. So I encourage you to get your questions ready for Marciej.

So I believe that's everything. Marciej, may I turn the floor over to you, please?

MARCIEJ KORCZYNSKI: Thank you very much, Mason, for the invitation and for the introduction. So today I am going to discuss in particular the technical part of the study that we produced in Grenoble Alps University, which

was part of the bigger study on DNS system abuse that was commissioned by the European Commission.

Next one, please. So here is a brief agenda for today's talk.

Next one, please. And here are the objectives of the study. So the main objective was to assess the DNS abuse phenomenon, starting from the definition, categories, roles of actors, and magnitude of DNS abuse. Also, in the main document, in the main study, policies, laws, and industry practices were reviewed and we also provided recommendation for improvements.

Next one, please. So the methodology consists of primary and secondary research. And in this presentation, I'm going to concentrate on the real-time measurements and analysis of 2.7 million incidents and 1.68 million abuse domain names using reputed domain and URL backlists in the second quarter of 2021.

Next one, please. So the start of this study—the objective—was to go through the technologies and terminologies used so far by the industry. And we concluded that there is no clear distinction between so-called technical- and content-related abuse. Just to mention: with phishing, we cannot really blame or expect registrars to take down the domain name when actually the website is compromised and used in phishing attacks.

So our definition is quite broad. Domain name system abuse is any activity that makes use of domain names or the DNS protocol to carry out harmful or illegal activity. So we can discuss this definition perhaps

during the Q&A session, but here I would like to highlight two important things. First is that we explicitly distinguish the definition from the fact which intermediaries should react and mitigate and also prevent DNS abuse because, for example, registrars, as mentioned before, are not always in the best place to mitigate certain types of abuse, such as malware distribution. And the second thing that I would like to highlight is that, contrary to the existing definitions, we propose a bottom-to-top approach and analysis of each individual case to actually verify who should react on such an abuse type. And in particular, we make the distinction between compromised and maliciously registered domain names.

Next one, please. So how we define DNS abuse? We define three types. Type #1 is abuse related to maliciously registered domain names. Type 2: Abuse related to the operation of the DNS and other infrastructures. And Type 3 is abuse related to the domain name distributing malicious content. And one more important thing here is that the attackers may take advantage of compromised or maliciously registered domain names.

Next one, please. So just to give you a couple of examples of our bottom-to-top approach, here is a URL that was used in a phishing attack. Below you can see the screenshot of the malicious webpage.

Next one, please. And the next step is to analyze the content of the registered domain name. And we see no content on the domain name. We also see some deceptive keyword, like “update,” in the fully

qualified domain name. And we concluded that the domain name was registered only two days before the URL was blacklisted.

So what are the implications? Next one, please. So this is Type 1 (maliciously registered domain name) but it's also Type 3; it is used to distribute and illegal and abusive content and, in this particular case, for phishing of credentials, trademark, and copyright infringement. So what are the implications? What intermediary should mitigate? And it should be a DNS service operator, registrar, or perhaps a TLD registry, but also a hosting provider. And this is another thing that we can discuss during Q&A if you'd like.

Next one, please. So here is another example of a malicious URL, serving, again, malicious content. Below you see the screenshot of the Bank of American phishing website.

Next one, please. And once more, we need to investigate this case a little bit more. So here on the registry webpage we see legitimate content. And also, when analyzing the WHOIS information, the domain name was registered back in 2015. So most probably the domain name itself is completely legitimate. When we take a look at the malicious URL, we see wp-includes indicating that, actually, the website was compromised and a vulnerable WordPress plugin.

Next one, please. So we concluded that this is a legitimate domain name. So it's Abuse Type 3. And the domain name is legitimate, but there's abuse to distribute to illegal and abusive content—in this case, phishing of credentials once more, trademark, and copyright infringement. So what intermediary should mitigate? Generally, it

should not be mitigated at the DNS level because it might cause collateral damage to the owner of the domain name, perhaps the business behind it, and also legitimate visitors of that website. So it should be mitigated at the hosting level.

Next one, please. So here is another example, a typical DDoS attack, where compromised machines send, from botnets, packets with spoofed source IP addresses of the victim's webserver, and they send it towards open DNS misconfigured resolvers that amplify and reflect the attack towards the victim. So this is Type 2: abuse related to the operation of the DNS and other infrastructures. And what are the implications? What intermediary should prevent these types of attacks in the first place in the DNS perspective? It should be operators of misconfigured, open resolvers.

Next one, please. So here briefly I summarize the role of intermediaries in abuse handling, once more highlighting that, in the case of malicious content distributed using compromised websites, when it comes to this particular type (3) of domain name abuse, remediation should be at the hosting level rather than at the DNS level because the registrars do not control the content of the websites.

Next one, please. So here we present the magnitude of DNS and overall health of the TLDs. So here on the left, on the pie chart, you see that estimated market share of different TLDs. And here on the right, you see the distribution of abuse domains for different TLDs, like legacy gTLDs, European Union ccTLDs, new gTLDs, and so on.

And here what we can conclude is that, in relative terms, new gTLDs with an estimated market share of 6.6%, are the most abused group of TLDs. The percentage of the abuse domains is 20%. 20% of all abuse domains were registered with new gTLDs.

However, I want to highlight here that not all new gTLDs suffer from DNS to the same extent. And actually, a lot of them did not experience a single abuse incident in the second quarter of 2021. And the two most abused new gTLD combined account for 41% of all abuse of new gTLD domains. And also, for the EU ccTLDs, EU ccTLDs are by far the least abused in absolute terms. Only 0.8% of all abuse domains were registered with new gTLDs and, in relative terms, [inaudible] overall market share.

Next one, please. So let's take a look at compromised versus maliciously registered domains. So, in red, we marked maliciously registered domain names and, in blue, compromised websites. And for spam and botnet command-and-control, the attackers generally need to control the DNS infrastructure. So the great majority of those domain names are maliciously registered. And this is not the case for malware and phishing attacks because here the attackers might maliciously register a domain name just compromise website to distribute this type of content. So about 25% of phishing domain names and 41% of malware distribution domain names are registered by legitimate users but are compromised at the hosting level and generally should not be blocked by the DNS service operators.

Next one, please. So here we present similar statistics but by different TLDs. So here on the right, we see that almost 98% of abused new gTLD domain names were labeled as maliciously registered. When we take a look at EU ccTLDs at the left, we see that almost 42% of them are actually compromised. And this is another thing we could discuss eventually, afterwards.

Next one, please. So we also estimated market share of registrars for 251 million domain names that we collected and for which we managed to get the WHOIS information.

And why are the sizes of registrars so important? Next one, please. Because we wanted to normalize the number of abuse domains per registrar sites. And to the best of my knowledge, this is the first study that, when calculating registrar reputation, takes into account only maliciously registered domain names and not all blacklisted domain names. So here, for example, we see that Namecheap suffered from 132,000 malicious registrations in the second part of 2021. And the top five most abused registrars account for 48% of all maliciously registered domain names.

Next one, please. The study also reveals some registrars with very high abuse rates.

Next one, please. And also, within the study we measured uptimes. And we can see here that, for Namecheap, Namecheap cleans quite fast, at least in the second quarter of 2021, based on our blacklists, where we measured uptimes, and the median was six hours. So they cleaned quite fast.

Next one, please. We calculated similar metrics also for hosting providers, and we concluded that there are hosting providers with disproportionate concentrations of spam domains, reaching 3,000 abuse domains per 10,000 registrations.

Next one, please. We also analyzed free services—so, for example, free hosting and subdomain providers—and concluded that they're extensively abused, especially in phishing attacks.

Next one, please. But what is interesting is those services—the providers—also clean very fast. Here on the y axis you can see the counts/numbers. And on the x axis, you see the time analysis. And we conclude here that, within one hour, [NGRow.io]—it's just an example here—cleans the great, great majority of abuse incidents.

Next one, please. So, within the study, we also measured the adoption of different DNS security practices like DNSSEC, DMARC, and SPF. The overall adoption remains unfortunately low, apart from a couple of TLD registries when it comes to DSSEC to that provide incentives. We also analyzed RFC-compliant e-mail addresses. So, for example, .com., there should be [alias]abuse@webmaster@. And this is especially important after the introduction of GDPR. We enumerated 2.5 million open resolvers that can be effectively used as amplifiers in DDoS attacks and also discussed the problem of the deployment of inbound [inaudible] validation. That potentially exposed DNS infrastructure to similar attacks.

Next one, please. And we propose a set of 22 recommendations—in the main study proposal, a set of 27 recommendation[—]in six areas. And

some of them also come from the technical part that I just discussed. And some of them I could also discuss.

Next one, please. So very briefly, acknowledgements to all the intermediaries and data providers that helped in this study.

Next one, please. And I would like to thank you very much. And you can download the main report and, in particular, the technical report that I just discussed. So thank you very much.

MASON COLE: Maciej, thank you very much for that presentation. Very informative. I know there are members who've been following the study in the context of our interest in DNS abuse now for some time. And I know we have a couple of—oh, and Brenda has very helpfully put the link to the report in the chat if you're interested in downloading it there as well.

So I know we have a couple of questions already queued up, and then I'll take a regular queue from anybody wants to ask Maciej a question. But first let me go to Steve DelBianco, and then we'll go to Marie. Steve, over to you.

STEVE DELBIANCO: Thank you, Mason. With so many actually potential recommendations—there's 27 recommendations which start at Page 15—I love them all but I'm going to ask you to help us prioritize. And a prioritization should look at, say, criteria for priority. And one might be,

will it have an immediate impact? So think about items that have most impact (and the most quickly) on the ills of DNS abuse.

And we also look at them through the lens of implementabilty of the recommendations, as well as whether the actors who implement them are at ICANN Org or among the ICANN community. Not every recommendation is incumbent on ICANN to do it.

So I know it's a big ask, but could you share your thoughts on how you might prioritize for having the most impact and which actors would be the ones to implement? Thank you.

MARCIEJ KORCZYNSKI: Thank you very much for a great question. So I believe that security in general is not only about the technology but I would say it's 50/50 with economic incentives. So I would say that perhaps one of the most effective incentives would be price incentives. So perhaps, as a community, I will go through intermediaries that could implement these types of recommendations. I would say that, first, we would need to have very reliable reputation metrics for registrars, for example, or for TLD registries. And those with these proportionately lower abuse rates could be incentivized by lowering their registration price. And this is not a new recommendation. This is the recommendation that we also discussed extensively as the output of the [inaudible] study. Perhaps you remember it. This was the study commissioned by the CCT Review Team and ICANN a couple of years ago, where we also made a technical part of the study.

And I think that first thing would be having very reliable reputation metrics and, second, having price incentives. Why those price incentives? Because, for example, in the study, we see that all the TLD registries that incentive their registrars with price incentives reduce the domain price by euro cent, for example. If the domain name is secured with DNSSEC, that works. And we see the deployments of DNSSEC over 50% in comparison to 1 or 2% in other TLDs.

So I believe that that would be one of the main recommendations.

Another recommendation may be sanctions also, meaning, if we see those security metrics and if we see some, for example, registrars that suffer from really high abuse rates, then perhaps ICANN could consider taking their accreditation. So the previous study revealed, for example, [inaudible] with 80/90% abuse rates with a massive number of maliciously registered domain names. I don't think that their accreditation was taken by ICANN because of the abuse rates. So I would say that this is another thing.

And now the questions of intermediaries: what intermediaries could implement such price incentives, let's say? It could be registry operators locally. That could incentivize their registrars. I could be ICANN incentivizing, for example, registry operators. This is a little bit outside of the scope of the discussion, but similar incentives could be applied also for the hosting market.

Another thing that could potentially help—but this purely anecdotal—is perhaps KYC also. As mentioned, this purely anecdotal because, in our study, we analyzed the DK TLD registry that implements Know Your

Customer and really deep verification of their registrant information. And we do not see a lot of maliciously registered domain names. But this is, I would say, purely speculative because we did not measure this.

STEVE DELBIANCO: Thank you very much.

MARCIEJ KORCZYNSKI: Thank you so much.

MASON COLE: Thank you, Steve, for the question. Marie, over to you, please.

MARIE PATTULLO: Thank you so much. DK Hostmaster just jumped into my head. I can't imagine why.

I've got a two-part question, if I can—one policy, one practical. You may know that we just came out of a meeting with the ICANN Board. During that, the CEO of ICANN showed us a very beautiful graph, making it very clear that, according to the data that ICANN has, DNS abuse is going down.

Now, according to the conversations I have with the people that I work with, including many people here with us today, that's not what they see. There's a lot of different data sets out. We know that.

MARCIEJ KORCZYNSKI: Absolutely.

MARIE PATTULLO: You can always read data as many ways as there are hours in the day. But based on your study, based on your work, is it going down, staying the same, or going up?

And part two. I'm joining you this evening from a very not-sunny Brussels, so I've got a really practical question, as I work very often with the European Commission. Now that you've done this wonderful study, do you have any idea what they're going to do with it? Do you know what the next steps are? Thank you.

MARCIEJ KORCZYNSKI: Thank you for both questions. So I could not answer the first question, unfortunately. The reason is very simple. The study was very complex and we were performing measurements—real-time measurements, for example—with the uptimes and so on and so on. So we only see, let's say, a small part of it. We saw only the second quarter of 2021. I think, to draw such conclusions, ICANN is in a better position because they have the DAAR project. So I cannot conclude from the study.

That said, what I can observe in comparison to the [Sadek] study that we performed for ICANN a couple of years ago is that we can see many, many less new gTLDs with extensive numbers and concentrations of DNS abuse.

So, for example, in this study—this is a great slide—41% of all abuse domains in the new gTLDs were registered with only two new gTLDs. And from the top of my head, I think 6 [were] most abused, and new gTLDs account for 60%, whereas, in the previous study, we could see 15 or 20 with really huge abuse rates.

So perhaps also the previous study, perhaps also DAAR, is there and provides some statistics that already influence that list of new gTLDs and other intermediaries to perhaps more actively on DNS abuse. But, once more, I cannot conclude because of the limited timespan of the study.

Regarding the second question, I think obviously this question should not be directed to me. We just did the technical part of the study. But from the discussions in open forums also, where the European Commission participated in previous presentations like this, this study is not related to any, I would say, ongoing legislation at the EU level. It's more to really assess the DNS abuse phenomenon to dive deeper into potential recommendations and start discussions that could lead potentially in the future to applying those recommendations.

So, sorry. At the end I did not respond to any of your questions.

MASON COLE: Thank you, Marie, for the question. I think we have one more, Maciej, if you could. That's from Tim Smith.

MARCIEJ KORCZYNSKI: I would love to.

MASON COLE: Okay, thank you. Tim Smith, please go ahead.

TIM SMITH: Hi. Thanks very much, Mason. Maciej, I heard you use the word "sanctions against parties" earlier on in responding to Steve's question. But we just came out of a Board meeting in which one of the topics we were talking about was the DNS Abuse Caucus of the Board at ICANN, where there seemed to be acknowledgement that all parties have a role to play in addressing abuse. So I guess I was wondering whether you've had conversations with members of the contracted parties and what their reaction is to this and what they see as being potential uses of this and their role to play in addressing this as one of the parties—or several of the parties, perhaps.

MARCIEJ KORCZYNSKI: So you're talking about intermediaries, like registrars and registry operators?

TIM SMITH: Exactly right, yeah. And you were also mentioning hosting providers and resolvers. I'm just wondering whether there's receptiveness to working collaboratively to address the situation.

MARCIEJ KORCZYNSKI: So we'll be presenting this study to a registrar. So I'm thinking that, in a couple weeks, I would be able to answer your question. But generally speaking, I think, after the [inaudible] study, we had those conversation with registries and registrars. And perhaps one of the main arguments is that there are many ccTLDs, for example, that make a great job in preventing abuse and also mitigating abuse effectively. And they give also a great example. So I know that they are very open to these kind of initiatives, and they do it even before the recommendations come.

But I cannot speak for the whole market, and I think, as mentioned before, we will be smarter after the discussions with the intermediaries, which will happen in a couple of weeks.

MASON COLE: Tim, thank you very much for the question. And thank you, Maciej.

Any other questions for Maciej while he's available to us?

Mark?

MARK DATYSGELD: Thank you very much for being with us today. This is Mark. I'm with the GNSO Council, currently Co-Chairing the DNS Abuse Group over there. My question is a little more towards the methodology side. I wonder if you identified any particular method that's best—not necessarily the only method—to identify patterns of abuse. Were you guys looking more towards keywords, towards patterns of registration, towards specific ID blocks? What exactly did you find to be the most effective in

that sense? And if there was nothing [to doubt], what would your thoughts in what direction we should be looking towards trying to keep up with the abusive registrations?

MARCIEJ KORCZYNSKI: So the answer will come from very different research projects and more from the experience of our entire team. I think, for spam, one of the best is taking a look at the registration in bulk. And of course, we as a community, do not see all the registration data, but registries and registrars do. And I think registrations in bulk can be a great starting point, and things like even very simple sanity checks, like if the e-mail provide by the registrant is a temporary e-mail address or the actual e-mail address and, I would say, things like payment methods used by the registrants. Perhaps there are legitimate cases, but straightaway, if I see the registration with cryptocurrencies, then it raises straightaway a red flag.

Other things? They provide some more anecdotal evidence or, I would say, they give us an indication of potential abusive registrations without hard evidence—so things like, as you mentioned, specials keywords, like verification, like bank. So we did such a keyword analysis for the other project (the COMAR project), funded by AFNIC and SIDN. But this is, I would say, to distinguish the candidate domains, especially in phishing, because, for example, in spam or in malware distribution domains, we would not see those patterns.

For example, for DGAs, for domains that are used for command-and-control communication, I would not expect here [inaudible] DGAs can

create even up to thousands of domains per day, then only one needs to be registered to perform reliable communication between the compromised host and the botmaster. But still, perhaps some patterns could be there, like numbers or words that are not humanely readable, perhaps to avoid collisions with legitimate already-registered domains.

So I could think about a lot of things, but a lot of them cannot be measured by, for example, researchers because of the lack of WHOIS information. So I hope that that answers your question.

MARK DATYSGELD: Thank you very much. It answers it very well.

MARCIEJ KORCZYNSKI: Thank you.

MASON COLE: Thank you, Mark.

Other questions for Maciej?

All right. The queue appears to be clear. Maciej, we kept you a bit over time, so thank you for indulging us.

MARCIEJ KORCZYNSKI: No problem. It was a pleasure. Thank you so much.

MASON COLE: It was a pleasure to have you with us. You're welcome to stay for the rest of the meeting if you'd like. It's an open meeting. But we look forward to hearing from you again. And thank you again for joining the BC today.

MARCIEJ KORCZYNSKI: Thank you very much.

MASON COLE: Okay, thank you.

All right, folks. We're on to Item #3 of our agenda, which is, for the benefit of our guests, is just a policy calendar review that Steve DelBianco heads up for us, and then we'll move on with the rest of the agenda.

So, Steve, over to you, please.

STEVE DELBIANCO: Thanks, Mason. I'll display the policy calendar we circulated yesterday … once I find it. Okay. All right, hopefully you can all see that now. And since our last meeting, we've only submitted one incremental comment, which had to do with us approving or supporting the proposed ICANN bylaws change by the ccNSO back on the first of March.

Now, in our last BC meeting, which was the 24th of February, we discussed on that day the BC's response to the Board's questions about the next steps to take on the SSAD Operational Design Analysis, or ODA.

If you recall, we drafted those responses specifically to match the minority reports that we had put in, along with our colleagues in the IPC. And those responses to those questions now are being melded along with the other representatives of the small team and will be presented […] To the extent that we can determine if there was a consensus, then those will be advanced.

Now, a lot of you have heard discussions of what to do with the SSAD ODA this week and even today. And at this point, it's preliminary to suggest where there's consensus, but I don't want you to believe that there's somehow a consensus over a pilot project.

And let me just take a little indulgence and make a distinction for you. A pilot project for SSAD might be implementing nearly all of the SSAD for a small region of the world or a single country or a single registrar/registry or single category of abuse. But that's very different from what the BC and the IPC recommended. We suggested that ICANN do a full-fledged implementation of a ticketing system. That is one component of the SSAD, but that is not the same thing as a pilot. A ticketing system would be along the lines of what Alex Deacon recommended about two years ago, the idea being that, if ICANN were not going to impose obligations on disclosure of registrant data, the very least it could do is to obligate a system that tracks requests, the legitimacy of the requests, and then measures when and if those requests were honored by the registrars. So I don't want you to assume that we have a rapidly forming consensus around a pilot because I think that term can mean two things.

So let me turn to what's open right now in terms of ICANN public comments. The Name Collision Analysis Project is open until March 18th. So we have a little bit of time, but at this juncture, I am desperate to find a volunteer or two to help me assess the SSAC's study and to comment on that.

Now, a couple of years ago, Mark Svancarek and I did it with respect to their Study #1, but we do need some technically skilled BC members or staff members of those of you who happen to be on the phone to see if you can contribute to this effort. It's due the 18th of March, so we are at the point now where we need to develop our comment.

Do we have BC members on the line who have a question about this or would be even remotely interested in helping me?

All right. I don't see any hands or anything in the chat yet. But please get to me in the next couple of days if you can assist.

Mason, the second one up has come back. Do you remember the UDRP? That's the Uniform Domain Name Dispute Resolution Policy. The UDRP has been with us as long as ICANN has, and it was not, well, technically the result of a PDP. It's something that came in very early on and works rather well according to most participants. But there are a backlog of suggestions, improvements, or reforms to the UDRP. And that will be done as Phase 2 of a working group on a brand-new PDP that was launched several years ago to review all of ICANN's rights protection mechanisms. So Phase 2 is looking at the UDRP.

So ICANN is looking for comments on the efficiency, fairness, and abuse, which I think is helpful with regard to DNS abuse discussions that we've just had. This is an opportunity to help respond to the staff report—it's like an issues report—so we can determine whether they have really covered all the issues. Have they prioritized the concerns? Have they walled off certain issues, assuming that they're out of scope for ICANN? And this would be the time to catch things like that because, when the charter is developed for this PDP, it's almost too late in the charter to suggest that it was scoped improperly. This is the time for us to [e]ffect the scope.

So let me ask for BC members who would help to volunteer on drafting our comment and assessing that issues report. Anyone who's working on DNS abuse is probably rushing to click on the hand-up button right now because that's the perfect combination for this.

ANDY ABRAMS: Hi, Steve …

STEVE DELBIANCO: I see Zak and Ann-Marie. Thank you very much. And I heard somebody say something but I think you were cut off.

ANDY ABRAMS: Hi, Steve. This is Andy Abrams. I'm happy to volunteer as well.

STEVE DELBIANCO: Thank you, Andy. Much appreciated. All right, that's three all-stars between Zak, Marie, and Andy. I appreciate that.

Let me go to the next one.

MASON COLE: You got a hand up, Steve, from John Berard.

STEVE DELBIANCO: Go ahead. John Berard, please go ahead.

JOHN BERARD: I was just volunteering as you asked.

STEVE DELBIANCO: You're the best. I appreciate it, John.

JOHN BERARD: Thanks.

STEVE DELBIANCO: That's a creative context.

All right. Number 3 is the BC's advocacy at the European Parliament, European Commission, and the national governments with respect to the NIS2 regulations and the extent to which they can be used to return the operation of WHOIS, the interpretation of GDPR, to more balanced

approach that allows legitimate requests for registrant information to be fulfilled.

I wanted to mention that, just last week, thanks to Drew's hard work, we prepared a multi-page response to the European Parliament who has a new project on anti-counterfeiting. They're looking to put together a toolbox for the EU and the EC's initiative and gathered input week. It's an extensive and, I think, excellent document. I want to thank Drew once again.

And, Drew, I'd love to give you an opportunity to talk about what's in there or what the next steps might be.

DREW BENNETT: The anti-counterfeiting toolbox being developed by DG GROW and the European Commission did have an aspect of it whereby they were looking for input on tools that could be developed in the domain name space. Insofar as it is abused and exploited in counterfeiting efforts by counterfeiting networks. So therein we thought that there was important input that the BC could give based on our experience in the community and with links to NIS2 here in that, as the commission acknowledged, NIS2 would be one legislative development whereby tools could be surfaced and, in the future, accessed against counterfeiting.

And we reiterated some of what we said in the proceedings on this, too, but also drew extensively from the DNS abuse study that led off this session. And we used that as a lot of evidence about the problems in the

space and, as well, borrowed from some of the recommendations in that report that we thought could be applicable to the toolbox.

I'm not sure exactly of next steps in the toolbox, per se, but at a high level, folks are probably aware that NIS2 is undergoing negotiations between the European Parliament and the Council of the EU, hopefully heading towards a final draft, a negotiated draft, within the next three months.

STEVE DELBIANCO: Thanks again or your work on this. I see the work is fulfilling two needs for the BC and our members. One is to increase tangible measures that will justify the NIS2 changes that we're looking for but in addition, the longer-term concerns we have on DNS abuse and addressing those problems within other aspects of ICANN because this will contribute to that as well. I appreciate your help.

DREW BENNETT: Thank you.

STEVE DELBIANCO: Any questions for Drew and the other members of the drafting team?

Okay, great. Thank you. I'll go back to sharing the policy calendar. We'll get right through this. Back to the policy calendar, I want to turn to the next channel. For those of you who are guests of the BC, we typically separate public comment from that which happens from the GNSO

Council. And then Channel 3 will be the cooperation we have with our members of the Commercial Stakeholders Group.

So Channel 2 is led by our two elected councilors on the GNSO Council: Marie Pattullo and Mark Datysgeld. And what we have on the screen was a recap of the meeting on the 17th. We covered that on our last session, so I thought I would scroll right down to the March 9th highlights of the agenda, and that's a meeting tomorrow.

Marie and Mark, over to you.

MARIE PATTULLO: Thanks, Steve. Before we go into this, can I just check? John, is that an old hand? John Berard?

JOHAN BERARD: Yes, I'm a very old hand. Sorry.

MARIE PATTULLO: You know what I meant. I just wanted to make sure. If we do have any guests on the call, I'll kick off, as we always do with an open meeting, by explaining that Mark and I, the two councilors from the BC, are directed. And what that means is that every member of the BC has a voice, has an opinion—they all have an opinion—and we are told when we go into council by the BC how to vote. So if you do have any business interests and you're interested in the ICANN world, come and talk to us. And believe me, your voice will be heard.

Now, Steve, thank you for putting up the highlights of tomorrow's meeting. You've already talked about what's going on with the SSAD, and you are certainly the best-placed of us to do that because you're one small team there.

On the SubPro—as we all know, that's wonderful ICANN-speak for the next round of new gTLDs—there's also an ODP (Operational Design Phase), and we're going to be talking about that tomorrow because a couple of things have happened.

First up, when the SubPro report came out, there was no such thing as the ODP. So everything has been put back by almost a year, actually. So we understand from the Board, who have written to the council, that they are thinking that maybe some work could start before they actually adopt the recommendations. In particular, they're looking at various things to do with closed generics, possibly things like applicant support, and some other bits that you get into the "Is it policy? Is it implementation?" question on but may be some things [that can be] moved forward.

The other thing is that ICANN Org—so the organization itself—has issued a request for people to perform a study to analyze the costs and benefits of the new round.

Now, this is in response to repeated requests from the GAC that happen, although the GAC did not know that they were about to issue this request. So there's going to be a whole [inaudible] of conversations about those two subjects.

And then there's going to be everybody's favorite subject. And here I stop talking and hand over to my co-council, Mark, for DNS abuse. Mark?

MARK DATYSGELD: Thank you very much, Marie. So I've been pretty laser-focused on this. We sent out the survey to some of the interested parties to start collecting feedback on the community's thoughts on DNS abuse. And what I have to say is that, so far—and I would like to stress "so far"—this has been pretty well-received. This initiative by the GNSO Council was being seen as very legitimate. I think that the leadership, between me and Paul, is business but we are a little off the main path of business, so to say. We are just coming from a different director. I am coming from the SME angle.

So, so far, we've been pretty well-received, which is good. People have been pretty willing to talk to us in a more honest and direct way. So this is giving me hope that we can actually start getting this project in a good direction. The evidence that I have so far has been very good.

We have been talking with some of the industry members directly because they have reached out to us, which again is a great sign—that they're willing to talk us in that manner. Some are reporting via a more structured manner, directly to the staff.

What are next steps? So when we get all that feedback, at least what they have in mind right now is to try to make this very, very narrow and use it as a way to leverage this process forward. So whatever can do to

make the scope very actionable, very tangible, we'll guide it towards that and then try to make a big push with all the stakeholders that are behind this to really get this going and get the attention on something that's not just discussing definition endlessly with the CPH or listening to them say that some of them are doing a good job, which they are. Some of them are doing a great. The problem is with the ones that aren't.

So I'm … "Optimistic" is such a strong word. I think I'm looking forward to seeing how this develops. There's a lot of potential here. And please let me know any of your personal impressions. Feel free to reach out directly to me or to Paul. Were definitely very cognizant our trying our best while remaining impartial and trying our best also in making sure that the BC users are being accounted for. So if you want to reach out directly to any of us, now would be a great time. Thank you very much, everyone.

STEVE DELBIANCO: Mark, question for you. Given the dialogue with Goran and the Board and the CSG, do you believe there's any pushback or mid-course correction on the scope and incidence of DNS abuse that would be appropriate after what just happened over the last couple of hours?

MARK DATYSGELD: Yeah. I think that this certainly has brought a certain realism to the situation: even though the community will have our backs, eventually we won't be able to get Goran on board, at least not as our first move,

which is a little disheartening. I think that it would be helpful if he was, but then again, there is a second step, which is trying to reach out to him. We know from experience that, whenever we get on two sides of the fence with him, it gets … [prickly]? Complex?

So our next step is trying to really narrow down, why does he see the idea that a slight decline—potential decline—in DNS abuse means that we somehow have a hold over this issue? This could be a statistical variation. This could be anything. And it's still high and we still have incidents in the wild. So we'll try to start cornering that. It is very much within the scope of what we were trying to do. And we [inaudible] to support us, provide us with data, and help keep this project strong.

STEVE DELBIANCO: And then the final item for tomorrow's council is to dialogue with Org's management [in] Global Domains and Strategy Department.

Are there any questions from our BC membership or guests for our councilors?

All right, I'm not seeing any hands. Anything else to add, Marie?

Okay. We'll be watching during council tomorrow.

There are several other council items, not all of which require an update right now. But I certainly wanted to thank Zak and Arinola for the work they're doing on the Transfer Policy Working Group. We've discussed this extensively on the last two BC calls. The current pending open item is that, before Zak and Arinola get to the next opportunity to give input

on that PDP, we want to hold a BC member call (30-60 minutes) dedicated exclusively to what the potential notification changes would be in the transfer policy. We don't have the space to cover that here and now, and I'm relying on Zak and Arinola to let us know when the time is right to actually tee up what is being proposed and to give the BC an opportunity to have a consensus about what we want Zak and Arinola to say on behalf of the BC.

Is there anything, Zak, that you'd like to add to that.

ZAK MUSCOVITCH: Hi, Steve. If we had a meeting in about two to three weeks' time, that should be great. Thank you.

STEVE DELBIANCO: All right. Thank you, Zak.

Any questions for Zak on that project?

All right. The next one up is the council as a continuous improvement work that's going on. Susan Kawaguchi is on there, along with Imran.

Susan, do you have any update for us on that?

All right. Hearing none, I'll move on to the … I represent the BC on yet another small team on modifying consensus policies. And we are currently waiting for Org and the interested Board members to reply to our letter.

All right. With that, I can go to the third channel here, which is the Commercial Stakeholder Group, which is the IPC, the BC, and the Internet service providers, who together are labeled as the Commercial Stakeholder Group. But it's not a separate entity. It's just a label for three distinct entities.

And having clarified that, our elected liaison to the CSG is Tim Smith. So, Tim, I'll turn it over to you. And tell me how you'd like me to scroll the screen.

TIM SMITH: Thanks, Steve. And I'll just walk through the reports, Steve, just summarizing them as we go. As indicated here, we did have a meeting with the GNSO-appointed Board members last week and met with Matthew Shears, Avri Doria, and Becky Burr. And it was an opportunity for us to have an informal conversation and to discuss issues and compare notes. And we did talk about the EC's study on DNS abuse and we also spoke with the Board about their DNS Abuse Working Group, their small group. And it was very interesting, actually, to find out that they see the matter of DNS abuse as being a critical issue and declared that almost all members of the ICANN Board are part of that group, which as of today I think is now being referred to as the DNS Abuse Caucus, based on a meeting earlier today. So we had good discussion on that.

We also were talking about the SSAD, and they were feeling very good about the exchanges that were taking place with the GNSO Council, [and] felt that things were moving more quickly than they usually do

with a former process of letter-writing. So that seemed to be a positive step.

And then prioritization was also an issue that was being discussed. And your report is a little different than mine. How about that? So we were advised that the planning prioritization framework pilot was starting to take shape, which we had heard about, and that meetings were going to be taking place over the next little while. And as a matter of fact, that CSG representation was going to be sought to be part of the discussions leading up to the pilot. And as of today, actually, Susan Payne from the IPC has agreed to be the active participant on behalf of the CSG. And Wolf-Ulrich Knoben of the ISPC will be the alternate on that. So that was that.

And then later in the week last week, we also met with the Public Safety Working Group to discuss common interests and to see progress. And the DNS abuse study, the EC study, was also discussed.

We also talked about malicious versus compromised domains. And the GAC had not had an opportunity to discuss that, to deal with that, but I believe may have done that by now. And so there could be an update I the coming days on their view on that.

So that was basically it. However, as mentioned here, we did meet with the ICANN Board—CSG did—earlier today. So just to give you some highlights of that, which is not in this written report, we presented to the Board, as they had requested, our priorities, which we stated as having coordinated action with GNSO on areas of common interest, improving access to registration data, and helping to successfully

mitigate DNS abuse. And then we will watch, as time goes on, how we address those in those three buckets.

And this prompted a discussion on data protection and an indication that Board has asked Org to develop hypothetical scenarios to present to the EU Data Protection Board to proactively seek direction on what data can be obtained and who is to respond, which we thought was a pretty positive step. And it's a proactive step on the part of the ICANN Board.

Also related to priorities was appreciation of support for contracted party volunteer efforts to address abuse in which we hope to collaborate with contracted parties.

The issue of DNS abuse was further discussed. And the Board small group, which I mentioned a bit earlier, which is now being referred to the DNS Abuse Caucus, acknowledged that all parties have a role to play in addressing DNS abuse and that they hope to find ways to bring us all to a common place with agreement on shared understanding in this problem space. So that's pretty positive, too, and perhaps a bit reflective of Mark's experience that he's having within GNSO.

Then also other topics that were discussed were government engagement, the work prioritization pilot, and the last round of auction proceeds, which were told that the Board hopes to have a proposal on within the coming month.

So that's the report on what we've experienced so far in ICANN73 with relation to that. And with that, I'll turn back to you, Steve.

STEVE DELBIANCO: Thank you, Tim. Mason, I'll turn it back over to you with one final word. Prior to this, I sat in on the 90-minute session of the GAC Public Safety Working Group presenting to the GAC and teeing up with what they think should be the advice of the GAC in ICANN73. There was an excellent presentation with a dozen slides prepared by Laureen Kapin. I'll put a link to that again in the chat. And I strongly recommend that for BC members. It covers DNS abuse, WHOIS, SSAD, and NIS2. And it suggests that the GAC is finding its voice and will probably be rather forceful in the ICANN73 advice. I hope it comes out in a way that will drive forward some of the work on DNS abuse and how to appropriately interpret the GDPR. So back to you, Mason. Thank you.

MASON COLE: Thank you, Steve. Thanks, everybody, for running through the policy calendar. That was fairly extensive. We have 25 minutes remaining in the meeting and we have a couple of agenda items left, so let's proceed to Item 4. And we'll go over to Lawrence. Lawrence, over to you.

BRENDA BREWER: One moment, Lawrence. I see your note.

LAWRENCE OLAWALE-ROBERTS: While I'm being granted sharing rights to be able to project my screen, my presentation basically, well, first of all, I wanted to welcome those who are joining us for an open meeting

and are not currently members of the BC. We normally would use the opportunity of having this open meeting to showcase how the BC interacts. And basically, this is another opportunity so to do.

So I guess you're able to see the BC's finance and operations report for this meeting. And basically, kicking off with some open ICANN announcements, ICANN yesterday announced their decision of the Board to allocate an initial sum of one million dollars to provide some financial assistance and support for Internet infrastructure. This is basically targeted at the happenings in Ukraine. The Board's resolution basically read that this support will start in FY22, which is in less than four months to go. Detailed information, including the Board resolution, can be found on the ICANN Board website.

My interest, as the Finance and Operations Vice-Chair, was, knowing that this wasn't captured in the budget for FY22—this is supposed to take off in FY22—is I'm wondering if the BC might want to ask some questions in this regard, seeing that we have also gone past a FY23 budget planning phase.

So I just want to maybe pause to ask what's the BC's thinking around this. Would you think that this is something that the BC might want to possibly do a note to encourage or to ask some questions around it, especially since there are talks about it being permanent, so to say? Any comments?

Okay. So I'm not seeing any hands. Just in case I miss it, please let me know.

So to the report that Marie also spoke about earlier in her presentation, there is also a proposal for top-level domain operating model study that was issued today. Details of this can also be found on the ICANN website. This is supposed to improve diversity in the new gTLD coming rounds, so to say. The study is supposed to help improve diversity. So it can be interesting for some BC members who might also want to put in a proposal or make some improvements to the process.

We want to keep encouraging BC members to help reach out for new members. One-and-one referrals are effective. This has helped to grow the BC's membership strength within this period that we have been operating virtually. And so we want to encourage BC members to reach out to contacts, companies that you feel could derive a lot of value from a BC membership and especially those who might also help to improve our diversity, and not forgetting that trade associations have a very wide reach. These will be our targets as BC members and would go a long way to improve our diversity.

Currently, we have 65 members in good standing. Those are members who are fully paid up and are eligible to vote and be voted for in the BC while we are working with nine members to see them through the current FY22 to be able to fulfill their fiduciary responsibilities and become financially compliant.

I see Mark's hand. I want to pause and yield the floor to Mark before continuing with my presentation.

MARK DATYSGELD: Thank you very much, Lawrence. This is not a question or anything. I literally would like to publicly acknowledge your work. I think you've been doing an awesome job these past few months, helping to steer a lot of things in the BC. Thank you, everyone, for the effort on the newsletter, and to [Matt] and Zak for the incredible article. But overall, thank you very much for helping to steer us through these difficult times. Just a bit of public acknowledgement. I know you don't need it, but still, it's always good to acknowledge the people who are doing such hard work for us. Thank you, Lawrence.

LAWRENCE OLAWALE-ROBERTS: Thank you, Mark. That definitely means a lot. And thanks for the encouragement. We'll continue to push on and do our best to keep the boat sailing.

So we have the ICANN73 newsletter out and published. It's a very interesting piece. We want to thank everyone, starting from the staff: Brenda and Chantelle and others like Carlos, who helped with edits. A special thanks to [inaudible], who had always bailed us out, and also to the ExComm and Communications Committee for doing excellent work at editing the proof.

The ICANN73 newsletter is available on our website. If you get to icannbc.org and you check newsletters, it's going to be right there at the top, the March 2022 edition. Please take out time to review the newsletter. It has a warming welcome from the BC Chair and a lot more articles that will definitely catch your fancy. Again, many thanks for all those who helped to ensure that this was a possibility. So please go to

the icannbc.org website under "Newsletters," and you'll find this article there. You could also find other newsletters if you missed previous editions. You can always get to review those.

We have a few companies, like I said earlier, who we're working with and we're expecting their FY22 dues to come in. Please reach out to me at invoice@icannbc.org if you still have any challenges. We would love to work this out before we get into the next financial year so we're not carrying over so much work.

FY23 invoices are going to be due by the 1st of May. We're going to sending out those invoices. Please watch your inboxes. If by the 5th of May you didn't get an invoice, then you need to start disturbing us because something went wrong. We might need to maybe update the contact of the primary representative. Please, we'd like all primary representative to kindly update their records. There might be a few changes. We have reached out to a few companies, but if we missed yours, start getting worried if, by the 5th of May, you don't get an invoice so that we can help work through any difficult areas.

Of very keen importance is the BC's Council and NomCom elections. There is a requirement that causes us to present names of the BC's NomCom and Council to ICANN Travel 120 days before the AGM. And so, working back from those dates, we have to start the process of filling our BC councilor and NomCom seats—not that we're ejecting the current people who are there, but these seats would only be assumed after the AGM of ICANN75. That would be sometime around October or November, I suppose.

So this is for the GNSO Council seats of Mark. And Mark has been very diligent and, like we heard, and is also the Co-Chair of the DNS Abuse small working party within the Council and has definitely proven his worth on Council. But his seat is up for reelection, and Mark is also eligible. We are hoping that he will be throwing in his cap for the second run of this work ahead. Thank you for all you've done for the previous years.

The BC is privileged to have a large business seat and a small business seat on NomCom. We know that this has been a tussle within the community for a while, so we make it an effort to ensure that we're putting our best legs forward in terms of those who go to NomCom to represent the BC because it has a communitywide impact. And also there's a lot of focus on the BC.

Both Tola and Scott—Tola, who is the small rep, and Scott, who is the large business rep—are term-barred and cannot be reelected into this position. So for this cause, we are soliciting for BC members who understand the NomCom, the process involved, and who have the time and the bandwidth to also carry on this very important work to put themselves forward.

The nomination period is for two weeks, which will be starting on Sunday, the 27th of March, and the process will end in April. We would expect that nominations by financially up-to-date members of the BC nominating their candidates of choice will be posted to the BC private list. And, thereafter, the candidates, where they accept the nominations, will need to provide a candidate statements by Monday,

the 18th of April. We will have a candidates discussion, which is a tradition and a norm within the BC, on the 24th of April during the BC's meeting for that day. And thereafter, on the 22nd, we will start the process of elections, which will conclude with an announcement of who the delegates for Council and NomCom by the 20th of May, 2022. So please, to fully participate, we want to encourage those BC members who are yet to pay to plug into this process and make this work as we always do.

The next BC meeting will be on Thursday, the 24th. I know they have Daylight Savings, so the time might change. We will be advised by Brenda regarding this. So if there's any questions, I'll be posting this information on BC-private, especially with regards to [inaudible] and some more details. And so you can watch out for the announcements on the private list.

If you have any questions for me, I will be standing by. Otherwise, I will yield the floor back to Mason. Thank you, all.

MASON COLE: Thank you, Lawrence. Extraordinarily thorough report. And let me just echo Mark's compliment of you and all the work you've done to prepare us for this meeting and for getting the newsletter ready and everything else. It's been outstanding work. So thank you.

LAWRENCE OLAWALE-ROBERTS: Thank you.

MASON COLE: All right. Any questions or comments for Lawrence?

Okay. I don't see any hands. All right. Any other business to raise for the BC today?

Looks like the queue is clear. All right, ladies and gentlemen, in that case I will yield another ten minutes back to you. As Lawrence said, our next meeting is Thursday, the 24th or March. Watch out for the time change so you don't miss the call. And I believe that's everything.

So I wish you a successful ICANN73. See you in the next set of meetings. And the BC is adjourned.

[END OF TRANSCRIPTION]