YEŞIM NAZLAR: Good morning, good afternoon, and good evening to everyone. As part of the At-Large ICANN68 Prep Session, welcome to the webinar on DNS Abuse: An End User Perspective, taking place on the Wednesday, 10th of June 2020 at 13:00 UTC.

We will not be doing a roll call. It is a webinar but attendance will be noted on the wiki agenda page after the webinar.

Please note all lines are kept muted as it's a webinar. If you would like to ask a question, please raise your hand and your line will be unmuted once the floor is given to you. Alternatively, you may use the Q&A pod to ask your questions. Only the questions shared on the Q&A pod will be answered, not those on the regular Chat pod.

One final reminder is for the real-time transcription service provided on today's webinar. Please click on the link that I'm going to share on the Chat pod shortly and please do check the service.

Thank you all for joining today's webinar. And now I would like to leave the floor over to you, Joanna. Thanks so much.

JOANNA KULESZA: Thank you very much, Yeşim. That is a wonderful introduction. This is Joanna Kulesza for the record. It is my pleasure to welcome all of our attendees to the second edition of the DNS Abuse webinar that is focused on end user – protection on end user interests.

We are happy as the Capacity Building Working Group to welcome again Jonathan Zuck who is the Vice Chair of the ALAC, who focuses on policy. He coordinates the Consolidated Policy Working Group together with Olivier Crépin-Leblond and Drew Bagley who is the Director of Operations at Secure Domain Foundation. As I have noted, we have hosted our guests before on this very same issue, however, we felt it would be relevant as part of preparations for ICANN68 to offer this webinar again. DNS abuse has increased in the times of the pandemic and it is of highest concern to all end users. So this exercise is to provide information on what DNS abuse is, as it might be somewhat ambiguous. What are the end user interests that should be protected by those within ICANN's remit?

I will give the floor to our speakers in just a moment. But before I do, I would like to beg our attendees' patience with us. We are testing Zoom webinar, as Yeşim explained in much detail. We highly appreciate you bearing with us and using the Question pod and raising your hand. We would love for this to be an interactive exercise, so do feel free to raise your hand and ask your questions. We are more than thrilled to exercise also this opportunity that the webinar option gives us.

Without further ado, I'm going to give the floor to Jonathan to start us off with introduction to DNS abuse and to try to draft this unique end user perspective. Thank you again for joining us. Jonathan, the floor is yours.

JONATHAN ZUCK: Thanks, Joanna. I think I'd like to begin by playing a quick video and then answer any questions. So, Yeşim, if you could play the video, that'd be great.

[VIDEO PLAYING]: Good morning, good afternoon, and good evening, or for the less fortunate, good middle of the night. Today we're going to discuss DNS abuse, which has only become worse during the COVID-19 crisis. We often hear the term cybercrime, but what is DNS abuse?

We're all pretty familiar with the DNS or Domain Name System by now. It's a fairly sophisticated system of questions and answers that get you to where you want to go on the World Wide Web. It's a bit like a scavenger hunt where you need to ask the person for the name of the person who knows the number of the person you want to reach. Of course, as they say in the movies, all that asking around can get you noticed by the wrong people – just as Dorothy as she asked around for the Wizard of Oz.

Simply put, DNS abuse is attacks on or criminal use of the DNS. Some people will try to parse this definition further by calling attacks on the DNS "DNS abuse" and attacks using the DNS "DNS misuse." But for our purposes, we're going to call it all DNS abuse.

Now we're going to talk about the different types of DNS abuse. Hey, what was that sound?

It's Quiz time. That's right. You put them to sleep and I wake them back up. Your first question is what is the DNS? A) The Delaware Nature

Society, B) The Division of Nuclear Safety, or C) The Domain Name System. If you chose C, the Domain Name System, you would be correct. To be fair, the Delaware Nature society and the Division of Nuclear Safety are DNSes but not the kind we've been talking about.

One of the best known attacks on the DNS is a Distributed Denial of Service or DDoS attack. Here, a perpetrator uses a network of zombie computers to make so many requests that a server is overwhelmed. Sometimes a criminal element gets in between you and the servers from which you request information. This can be done with a so-called man-in-the-middle attack or DNS cache poisoning. Simply put, the idea here is that your queries are intercepted and you're given the wrong number for the site you wish to visit.

These server side redirects can be used for something called a pharming attack, sometimes called "phishing without a lure." Here you are simply redirected to a site that looks just like the one you intended but it's just set up to capture your login credentials. You think you're logging on to your bank but really you're just filling in a form for hackers to go and use on the real bank website.

One of the most common abuses using the DNS is phishing. A far less technical way to get you to the wrong server is simply to ask you to go. In this case, you receive an e-mail suggesting something is up with your bank account and that you need to login to fix it. However, when you click the link, you're taken to a pharming site. This process is called phishing because you are lured to the fraudulent site.

Here's an example of what such an e-mail might say. You can see there are some key elements to such e-mails, some kind of crisis with a short time to remedy so that you don't think about it too much, and a call for you to log into your account. Of course, taking you to a fraudulent site isn't the only use of e-mails. Sometimes they have attachments that contain malware directly.

One area of particular concern to the At-Large is Internationalized Domain Names or IDNs, those domain names using non-Latin characters. These relatively new domains are essential to get the next four billion users on the Internet. 70% of the world uses non-Latin alphabets, and finally in 2012 we got the ability to register domain names in languages such as Russian, Arabic, and Chinese.

Of course, with every new innovation comes matching innovation by the criminals and IDNs were no different. It turns out that a lot of letters in non-Latin alphabets look a lot like letters in the Latin alphabet. Who knew there were so many ways to spell Bank of America? When someone sees one of the spellings while quickly reading an e-mail, why wouldn't they go ahead and click? In addition to collecting your credentials, these –

That's right. It's time for another quiz. What is a Denial of Service attack? Is it A) When a waitress is upset with you, B) Too many requests to a server, or C) Coming to the store without shoes? That's right. It's B, too many requests of a web server. Now, it's true that showing up to a store without shoes might lead to a denial of service but let's be honest. In that case, it's you who's doing the attacking.

In addition to collecting your credentials, these fraudulent e-mails and websites have as a primary objective to plant software on your machine. This software is broadly called malware. But there are many, many varieties of malware. You've heard of these types of programs before and many of you or your friends and family have fallen victim to them. While we don't have time to go into each of them in detail today, suffice it to say, whether it's spyware or ransomware, you don't want them on your computer. Unfortunately, malware infection is on the rise. In the last 10 years, malware infection has gone up nearly 700%. As just an example, ransomware attacks have risen 350% in 2018 alone.

In fairness, especially after the review of the 2012 round of TLDs for competition, choice, and consumer trust, the folks in ICANN Contract Compliance are doing their best. The Compliance team began publishing much more granular data about complaints and began to make its audit process a little less random, but it's still not good enough.

You might have heard of something called Domain Abuse Activity Reporting, which ICANN began a few years ago. While the monthly DAAR reports provide just enough data to know there's a problem, they don't provide enough data to do anything about it such as avoiding a domain or registrar that seems to be up to no good. However, using DAAR, we can determine that the percentage of detected abuse has gone down less than 1% since its inception two years ago, so we can all agree DNS abuse is a major problem for individual end users. But what can the At-Large do?

The At-Large plans to take a two-pronged approach to combating DNS abuse: outreach and ICANN policy development. The At-Large will

develop educational materials for individual end users to better protect themselves against DNS abuse. The At-Large is unique in its structure, making it possible to distribute information to the Regional At-Large Organizations or RALOs who in turn can distribute these materials to the At-Large Structures, each of which have individual members to which they can finally distribute these materials. The At-Large has been developing this network for years and what better use than to protect users from criminals on the Internet. There are a number of messages we can deliver to help people avoid the traps being set for them every day.

It is the enduring irony that criminals get most of the information they need from users, not by being clever computer engineers like in the movies but by being clever social engineers. In short, if they want your password, they basically just ask for it. This was true before the Internet and it remains true today. The At-Large needs to educate users to be on the lookout for news that's too good or too bad to be true.

We'd like to make fun of those phishing e-mails because of their bad grammar. What we don't realize is that the bad grammar is intentional. Writing this way simultaneously triggers the deletion by those who recognize the scam and sympathy from those who are less sophisticated. The At-Large can certainly help end users to discern the authenticity of an unexpected e-mail.

It should go without saying, but the At-Large will say it anyway over and over again, that individual end users should have virus protection software on their PCs and mobile devices. In fact, in the United States where you would expect considerable sophistication by end users,

nearly 50% of computers like virus protection. The At-Large must encouraging users to ask their employers if they have DNSSEC-enabled servers to prevent events such as men-in-the middle attacks. These are just some of the ways that the At-Large can educate individual end users to protect themselves.

The other place the At-Large needs to be heard is in the hallways, meetings, and conference calls that make up ICANN policy development process. The At-Large will engage in ICANN policy development at every point of entry. In one case, it might be a conversation in a hallway or participation in a work group or review team. We will actively engage in advocacy for reforms, both inside ICANN and among the businesses that serve end users such as registrars and registries. In other words, if someone asks us about the weather, we stick our hand and look up at the sky and say, “It feels like DNS abuse.”

Thankfully, we’re not alone. The majority of the ICANN community is concerned about DNS abuse and hesitant to allow a new round without significant reform. There’s simply no way that a minority of voices should be able to drive ICANN to a new round without real buy-in from the rest of the community. The At-Large has and will continue to partner with other groups within ICANN community to sound the alarm regarding DNS abuse and actively promote reform. Our task is to hold the line. There should be no new round until DNS abuse is addressed in a meaningful way.

Compliance needs a holistic view of DNS abuse. They cannot simply react to complaints but must use their audit power to recognize high

percentages of abuse and take action against TLDs, registries and registrars who are part of the problem.

One thing we should make sure to do is limit volume registrations because there's a high correlation to DNS abuse. Of course, there are legitimate uses for bulk registrations and such uses will only increase with the Internet of Things, but the At-Large will continue to advocate for increased friction for such activity, perhaps requiring authentication as legitimate bulk registrant.

The CCT Review Team and consequently the Security and Stability Review Team have both suggested that ICANN design incentives to adopt best practices. The At-Large will continue to advocate for such incentives.

Certainly, more research can be done and has been recommended by the CCT RT, the SS RT, the ALAC, and now Verisign. There's now essentially $20 million more in the budget to invest in security and stability of the DNS.

There were certainly those registries and registrars that are investing significant time and money in combating DNS abuse. In fact, 48 companies have signed on to a commitment to best practices. That's awesome but we still need reforms to better address the bad actors and, frankly, even the good actors could be doing better. So the At-Large won't be easing up on those guys anytime soon, either. It's like that old Dilbert cartoon, in which we are reminded that once everyone has adopted so-called best practices, these practices become the new

normal and are no longer the best. The criminals are not satisfied with the status quo and neither can we afford to be.

All that is to say that this is a crisis from which no one is immune. Incredible research is happening in machine learning to better detect abuse in real time and predict that a registration is intended for illegal use. Early tests of such technology by .eu showing nearly 80% accuracy in such predictions. We need to ensure that such research continues and systems are put in place to protect us from the next generation of attacks.

That sound means it's time for your last question. Which of the following are tools to combat DNS abuse? A) Education, B) Implementing DNSSEC, or C) End-to-end encryption. If you chose all of them, you are correct. If you didn't, please stay after class.

When all is said and done, there's really only one constituency: end users. It's the interest of those end users the At-Large was created to advance. DNS abuse affects all of them. Say it with me: "We have no use for DNS abuse."

Go to atlarge.wiki/DNSabuse for more information.

JONATHAN ZUCK: Okay. Thanks, everyone. I hope that wasn't too fast. It occurs to me that I might have been speaking to quickly in that. But I see one hand up and there's a question in chat from Michele. So I'll go ahead and call on – oh, did somebody lower their hand? Do you have a question? Okay. Does anyone have a question?

YEŞIM NAZLAR: Jonathan, actually we have one question from Bill Jouris on the Q&A pod, if you could please kindly check that one.

JONATHAN ZUCK: "Can we expect to see a massive increase in bulk registrations as companies and other organizations try to protect themselves and their customers from pharming attacks following IDN roadblocks? All those variants on their names, variants which ICANN is doing nothing to restrict."

Bill, sure. I don't know that those would even constitute bulk registrations, but you will see some defensive registrations. Although the massive expansion of available TLDs in 2012 did not lead to the level of defensive registrations that we expected instead because of the costs involved in that, and so there's been more monitoring and other tools to try and combat malicious registration by trademark holders than there's been the defensive registration, maybe because defensive registration as a strategy has become a little bit more overwhelming for companies to engage in.

Then I've got a question from an anonymous attendee, "Do we have a commonly agreed definition of DNS abuse?" and the answer is yes and no. In other words, there are definitions of DNS abuse on which we all agree, and then there are many definitions of DNS abuse on which there is still disagreement. And so that's an ongoing discussion within the ICANN community about what a more expansive view of DNS abuse might look like. But there are well-established sort of baseline

definitions for DNS abuse and those were the things that were covered in this video. So other types of DNS abuse are sort of still under up for debate and being discussed inside the ICANN community. But there's certainly things that can be done to combat the abuse on which there is agreement, and then the definition could change and simply change the instances in which we use our new enforcement capabilities. It doesn't need to precede it.

Any other questions? Okay, seeing no more questions, I'd like to hand the microphone over to Drew.

DREW BAGLEY: Thanks, Jonathan, and hi, everybody. My name is Drew Bagley for those of you who don't know me, and I help lead a nonprofit organization called the Secure Domain Foundation, which focuses on DNS abuse. I'm also the Vice President and Counsel for Privacy and Cyber Policy at CrowdStrike, which is a global cyber security company.

Jonathan wanted me to go over several of the examples that we're seeing in the real world today tied to both the COVID-19 crisis as well as DNS abuse, and so I'd like to share some examples with you today and what we're actually seeing in play and then have a few quizzes, of course, along the way to continue the theme, to really help everybody get a picture of DNS abuse in the real world specifically during this era. Next slide, please.

This is an interesting era as it relates to the threat vector for bad actors. Many organizations have naturally shifted to remote work, but some organizations have done so in a way that's been a bit ad hoc, where

instead of employees using corporate laptops or their organization's laptops, which may have security software on them, some people are being asked for a temporary period of time to use their own personal devices to then connect to their organization's network. And then naturally, we're even seeing that there's a lot of different types of devices now being used for work that, again, and in more traditional times, maybe would be subject to a bring-your-own-device policy with some security protections in place, and instead right now are not necessarily always being done that way. And so as a result, the dynamics of even workflows have changed, and where sensitive data is going, including personal data, and how employees are using that data.

Simultaneously, there are people that are seeking resources with regard to testing that's available or with regard to other information about the pandemic. And so as a result of everyone attempting to keep safe and figure out what's best and seek information, you really have an environment that's kind of ripe for some of the types of phishing that Jonathan alluded to and some of the types of attacks that can be used to harvest credentials from people. So naturally, a consequence of that is that the DNS is being abused to carry out cyber attacks.

Some of these cyber attacks can involve the delivery of malware, but some of them are really used to harvest credentials for what we can anticipate maybe later attacks down the road or identity theft, even in the immediate term. And so a lot of the campaigns that are set up to go after victims are attempting to spoof COVID-19 related themes, World Health Organization themes, Centers for Disease Control related themes, or other similar things in an attempt to get a victim to trust whatever it is, whether it's a text message or an e-mail that they're

receiving and then to input information or to install a file. And so I'll go over just a couple of those examples where the DNS has specifically been used for that. Next slide, please.

In Australia, early on in the lockdown portion of this pandemic, what we observed is that the domain name covid19-info.online was registered, and rather than merely they're being a malicious e-mail campaign from this domain name, instead what was going on is that users were receiving SMSes trying to direct them to go to the domain name. And this was a domain name that was being used, as I was alluding to a moment ago, to harvest credentials from people who would go to the domain name.

Of note, long after the domain name was recognized by the cyber security community as being malicious and published in widespread fashion on many cybersecurity blogs including government alerts, such as the one cited at the bottom of the slide, the domain name was still active and could still be used to perpetrate harm against victims. And so, this is an example of that lag between victims and governments, even, identifying that a domain name is being used for malicious purposes and then the fact that the domain name is still persisting thereafter, potentially being able to continue victimizing others who are not aware of the alert. So that's one example from Australia, but this really is a global phenomenon. Next slide, please.

Similarly, in the United Kingdom, there was a domain name uk-covid-19-relieve.com that was registered, and that was used to lure people into revealing their passport details as well as other personal information. Similarly, this is one where the UK government then eventually was

alerted and was warning their citizens about this, and yet the domain name remained registered thereafter. In this case, you can see again a situation in which there's perpetrators who right now are taking advantage of this as an opportunity to focus on harvesting information that they can use later for identity theft or for some other sort of financial theft, and perhaps even for other sorts of cyber attacks in the future. And so one of the issues here is that with these domain names that are registered with COVID-19 in the name that's naturally going to be something that can lure people who are seeking information again about testing or just about public health information. And so that's where it's really important for end users to be vigilant about whether or not a domain name is likely to be legitimate or not to be legitimate. Similarly, even with e-mails, it's really important to pay attention to whether or not an e-mail itself looks legitimate, which brings us to the next slide and our first quiz. I do not have the theme music Jonathan had for quizzes.

So the quiz question is a true or false one. "It's easy to tell if an e-mail is legitimate." All right, so we have most people saying false. It could be that those who chose true are really good at dissecting headers and doing the analysis. Or it could be that perhaps you will learn something today, so we'll see. Next slide, please.

So here's a great example of a commonly used tactic, especially right now, whereby a sender's e-mail address is spoofed. So in many e-mails, of course, we've all experienced some form of phishing and we can all tell when an e-mail is very poorly written or it's so obvious because of the sender's e-mail address that it is a fake e-mail. However, there are other situations, especially right now, that are along the lines of what

Jonathan was describing with homophone attacks where you could have a domain name that looks and sounds nearly identical to the legitimate domain name but would be substituting zero instead of an O or something like that.

However, there's a whole nother class whereby senders are making an e-mail appear as if it really does come from a legitimate organization, and that's an artifact of the ways in which many organizations are not requiring authentication on their e-mail servers. And so as a result, what we've seen in the real world in this era or e-mails like this, where the sender's e-mail address is a legitimate e-mail address that actually exists and is associated with WHO, however, this e-mail is not legitimate.

So, several campaigns have been doing this in an attempt to deliver some form of malware. Again, a lot of the malware even has been used to harvest some sort of credentials, whether they be user credentials or other personal information from user's computers. But here, you see it, you have the logo, you have something that looks otherwise legitimate, and again you have that lure where people are obviously interested in these times on information about vaccines and trust the World Health Organization as a legitimate source. So that's what makes this e-mail even more compelling.

So here's one where you would need to actually dissect the e-mail headers, pay attention to the IP addresses, pay attention to which domain names appear in the headers, which other domain names because that can be indicative of where the e-mail may have originally originated from and whatnot. And so this seems to be happening on a weekly basis. Some other examples of e-mails that have been seen in

the wild include those spoofing eurohealthycities@who.int, donate@who.int, healthcaresupport@who.int. Next slide, please.

As you can see that 80% of you said that it was not always easy to tell if an e-mail was legitimate or not. That's really a great example of that. That's the reason why you really have to really stop thinking connect and you have to pay attention to those e-mail headers if you are using an e-mail platform that allows you to view the source of those headers. That's where you can look at IP addresses. And again, there's other domain names that could be mentioned that might not be that legitimate domain name. And always be suspicious if you weren't expecting anything from a particular organization or you certainly weren't expecting an attachment. Even with the domain names, sometimes if you're getting an e-mail or one of these text messages that's trying to tell you to go to a domain name, it's great to at least look at the WHOIS record for the domain name. WHOIS, naturally, is a lot less useful depending on the TLD these days, but you can at least look to see how recently a domain name was registered, whether or not there appears to be any public contact information, which isn't always indicative one way or another of legitimacy. But nonetheless, if you're talking about a big international organization, that's where you might be a lot more likely to expect some sort of contact information disclosed in a WHOIS record than if you're talking about a small business or something else. But it's really important to, nonetheless, leverage that.

And then of course, as Jonathan was alluding to, it's very important for everyone to protect their devices with effective Endpoint Protection because the reality is that you're bound to find some situation where you could inadvertently open an attachment, and so you want to make

sure that your system is up to date with software that can actually tackle not just is this file good or bad. Because it could be the first time it's ever been seen, but actually protect you from what that file may attempt to do to your computer. And so that's where you want to pay attention to the next generation endpoint solutions that do that. If you're part of an organization, it's really important especially during this time to provide cyber security training that includes a literacy component as to how to better scrutinize domain names that could be fraudulent e-mails that could be spoofed that come from seemingly legitimate-looking domain names, and then otherwise just good cyber hygiene about not opening attachments from untrusted sources and whatnot. And also some common sense, thinking about how information would be communicated from your organization to employees and and how that likely would not come from an external organization if, for example, your organization was going to communicate information about an internal health program, internal vaccine program. Because that's another trend we've seen, as we've seen covid19- a company's name .com being registered in another TLD. So it's really important to incorporate that into training.

Then also with regard to attachments and even URLs, there are so many great free resources available. I've included just one of them here but there's several out there in which you can test files before opening them by simply uploading them or paste URLs to see whether or not they're appearing either on block list or some like the one in this example, hybridanalysis.com, will actually run the file or URL in a sandbox to show you what it would have done and then produce a report as to whether or not it was legitimate. Next slide, please.

Now we're up to our next quiz question. This is “What's an example of proactive anti-abuse?” So Jonathan gave an explanation about the fact that parties can be reactive or proactive when it comes to anti-abuse and fighting DNS abuse. Here's some examples in the multiple choice of what can potentially be proactive versus reactive.

All right, great job again, everyone. This is a great group. So, the correct answer is both C and D. And so while it really can, of course, depend on what you're dealing with, with regard to the type of DNS abuse – and there's many, many ways to be reactive with anti-abuse and there's sometimes we're only being reactive as possible, there's other times where there's many methods to be proactive. As we can see with this current phenomenon – and I'm just going to really focus on that today – a lot of these domain names are registered with COVID-19 in them or with coronavirus in them or by spoofing the names of the World Health Organization or similar health organizations specific to our individual countries. And that's where for something like this, it's a lot easier to identify a potentially maliciously registered domain name. At the same time, of course, you do have legitimate users registering domain names associated with these themes, but the high volume we're seeing of domain names associated with DNS abuse including these keywords is a good way that domain names could at least be flagged and better scrutinized either at the point of registration or at least once they've been reported by cyber security companies as being used in these different campaigns.

Similarly, with regards to traditional DNS abuse and past studies, you can often see a single registrant accounts associated with a large number of registrations that are going to be used for a concerted

campaign. So that way, if one domain name gets taken down, they have others in their infrastructure. It's an investment in infrastructure. So there are opportunities at times where the registrant account itself may already be associated with several known reported instances of the their domain names being used for abuse and it's only a matter of time until other domain names in their account will be used for abuse. And so there are potential proactive measures to take there as well, rather than wait for people to be victimized and wait for a data breach to occur in line for people's personal information to be harvested. Next slide, please.

I apologize for the formatting. I think this was an artifact of the presentation being converted to PowerPoint and perhaps a missing font. But essentially, there's a lot of legal reputational and even financial variables that create common incentives for not only this group who is representing the end user but also for the contracted parties for ICANN and for the community as a whole. So, ccTLD and gTLD registrars naturally face pressures to respond to abuse complaints in the form of contracts and language that already exists in ICANN contracts as well as in local laws and community best practices and, in addition, in some of the recent calls from the community in the reports that Jonathan has studied.

Similarly, there's also reputational incentives too because if it's known that a registrar is a clean registrar versus there's another one that's known for being associated with a high level of DNS abuse, then that's something that can really be incentivizing for a for a registrar to want to maintain their reputation as a clean registrar and to not be associated with high levels of DNS abuse. And so this is something that is naturally

going to vary depending on which registrar, depending on if you're talking about the ICANN world and depending on which agreements you're talking about. If you're talking about gTLDs versus new gTLDs and some of the safeguards there, if you're talking about ccTLDs which is outside of ICANN but nonetheless is subject to the rules in their own country, you can really see a some overlap in some of these reputational incentives, along with some of those pressures from various policies that are either at the government level or from ICANN.

Then similarly, when you're talking about some of the bulk domain name registration that can be associated with DNS abuse in something specific to this era, just the COVID example, if I have a bunch of those from one registrar, you could potentially be dealing with credit card charge backs and whatnot if you're having registrants that are using even some of these fake credentials. They're harvesting to then create credit card accounts and then registered domain names and whatnot.

Then similarly, again depending on whether we're talking about certain countries that ccTLDs are subject to the laws of or to certain categories of gTLDs, you can deal with all sorts of other pressures from just litigation that parties could be involved in or the threat of loss of accreditation and whatnot.

So what this means is there's many levers here, but it's not always clear, I think, to Jonathan's point as to which levers are going to be most useful and helping to incentivize and prevent the type of abuse that we're seeing run rampant, for example, right now. We are right now still witnessing domain names that incorporate these themes being registered and being used to target people, and so this is something just

really important, especially for this group representing the end user to consider and think about in your discussions. Next question, please.

So this one is “Who is affected by DNS abuse?”

Another fantastic job by this group. Yes, everyone. That’s the thing. This can really be something that can deeply impact end users who can have their own personal data stolen, have their money stolen, and all sorts of things, or even lose access to their data. It can harm organizations, it can harm the contracted parties if contracted parties are having to spend their time dealing with all this DNS abuse because they're being used for all these sorts of registrations or having to fill all the complaints. Similarly, ICANN itself, both the community and the organization are affected by DNS abuse, and consumers who can be defrauded, whether you're talking about again consumer being lured into sites that appear to be real like what we were talking about with the COVID-19 examples or other examples that you may know from other instances. But it really is everyone. And so that brings us to the next quiz question.

“Who has the ability to prevent DNS abuse?”

100% great job, group. We all do. And that's exactly right. Obviously, the debate is over how best to incentivize different parties to take different actions within their control, how best to educate, and that's part of what this session is all about is educating this group on what we're seeing right now related to COVID-19 and DNS abuse but there really is a role for everyone to play in helping to prevent people from being victimized by DNS abuse.

As Jonathan mentioned in the intro presentation, there's reactive and proactive anti-abuse. There really is an ability, of course, for the end users to make sure that they're not only being educated themselves but helping to educate others on how best to scrutinize potentially fraudulent e-mails and domain names as well as ensuring that ICANN org pays attention to the hard work done by the ICANN community with many recommendations that are already available from groups such as the one Jonathan and I worked on, the CCT Review Team as well as work being done by other groups like SSR2. So it's really important as well to pay attention to the data that's available from the community because there's been a lot of studies done that show correlations to various types of DNS abuse and various types of registration practices or just various types of safeguards which could be more effective or not, in addition to of course there's data on the extent to which safeguards already put in place are effective or not with regards to DNS abuse. So that's where there really is a role for everyone in the ICANN community to play on this because this is not a problem that will be going away.

And so that brings me not to quiz questions but to two quick poll questions where there's no right or wrong answer. But this group is getting all the questions right anyway, and so we'll go to the next slide, please.

“Have you personally been targeted by COVID-19 related phishing campaign?”

Okay, so it's great to hear that apparently not many of you have. But unfortunate to hear of course that you have, and then many of you do

not believe you've been targeted so hopefully that's correct and you have not been targeted.

Then there's one more question. “Have you received additional cyber security training from your employer since the COVID-19 pandemic began?”

Many of you have not. Some of you have. And so this is something that to the extent you're able to in your organization to really be the thought leaders on this and help promote the need for training, I would encourage you to do so because I think that cyber security training is a necessity in any organization in any time, but particularly right now I think we have some pretty unique dynamics, because of the rush to remote work for some organizations which weren't already set up for remote work, which obviously many of us in the ICANN community have experienced with remote work but nonetheless, that's something that I think is really helpful for everyone to take back to their organization and keep people vigilant about cybersecurity.

So with that said, that concludes my presentation. Feel free to reach out should you have any additional questions. I look forward to seeing all of you in person somewhere in the world someday again.

JOANNA KULESZA: Thank you very much, Drew. Thank you very much, Jonathan. Those were most informative presentations, and we've had quite a few questions. I believe those who are answered in the Q&A pod, I've noted the comments coming from Bill that those answered questions seem not to be displayed when you join the webinar a little bit later on. I

understand. We're looking into that technical issue. We're trying to use the Q&A pod. Thank you for bearing with us and I hope that we will come to a useful solution on how to best pick up questions.

I am not seeing hands up. I've seen a lively discussion in the chat. But I did not see any of the participants of that chat exchange raising their hands. So I'm going to assume that matter is covered.

I see one more question from Pablo: “Domain names are the first step into the Internet deciding what is a valid domain name or not sure sounds like the internet police.” That looks more like a comment, and so that comment is duly noted, Pablo.

I see thanks coming from participants. Thank you for attending. I would with that assume we’ve attended to all the issues that might have come up. I see two hands up. That is wonderful. Thank you very much for raising your hands. I'm going to let Yeşim handle the technical side of things. Olévié was first and Pablo was second. If you would kindly pass them the mic, Yeşim, that would be wonderful. Thank you.

YEŞIM NAZLAR: Olévié, this is Yeşim speaking. You should be able to unmute yourself now. Olévié, if you are speaking, we cannot hear you.

OLÉVIÉ KOUAMI: Hello. Can you hear me now?

YEŞIM NAZLAR: Yes, we do. Thank you.

OLÉVIÉ KOUAMI: Okay, it's Olévié from Senegal. I'm happy to follow-up this webinar. And I would like to [inaudible] on the last part of this presentation, which I have noticed that more than 70% of organizations have not trained their employees on cybersecurity. But in Africa, in place of that, most of the people are not able to use and train, to use the video conference tools as we are using on the At-Large. So we have to train people to how to work online first and to add the cybersecurity issues. This is my [point] on this. Thank you.

JOANNA KULESZA: Thank you very much, Olévié. That is duly noted. If our panelists wish to address it, I'm happy to give them the floor. If that is not the case, we can swiftly move to Pablo. I see one new question coming up in the Q&A pod that we will attend to after Pablo. Thank you.

DREW BAGLEY: I'll just give a really quick 10-second answer just to say that I would encourage you to check out a website, just some of the major cyber security companies because a lot of them, especially right now, have a lot of good free training, free webinars available, as well as some of the nonprofit groups that focus on cyber security. So I would encourage you to use those resources if video conferencing itself is not available.

JOANNA KULESZA: Thank you, Drew. If we could go to Pablo, Yeşim. Thank you. The floor is yours.

PABLO RODRIGUEZ: Thank you very much. First and foremost, I want to thank ALAC for this fantastic webinar. You guys have done a fabulous job and it is extremely informative. So thank you very much.

There are two points that came to my attention and one is the regulation of both registrations, and the other is the proposal of identifying potentially malicious domain names and the prevention of registrants of registering or conducting their activities online. As you saw in the question and answers, Jonathan and I were having a back and forth with that because I claim that registries nor registrars can become the Internet police. Jonathan said there's a responsible way of doing things. But how? That is that is easy to say when you can think of large registrars or large registries that have the people, the equipment, and so on. But for small companies and for others, I believe that this is a very slippery slope because the domain names are the first step into the Internet, and if I have the power to decide who goes in and who doesn't based on a criteria that I developed regarding whether I decide that what you registered is valid or not, is malicious or not, this is not this spirit of the Internet that we have worked so hard constructing. Thank you.

JOANNA KULESZA: Thank you very much, Pablo. I'm going to give the floor back to our panelists. I think it's a very, very important issue that you are raising. I'm

glad we're having this conversation. Please let me note this is a capacity building webinar so we're trying to show or discuss the policy positions or the facts. Policy work is done elsewhere within At-Large and we see these capacity building webinars as the first step to a policy discussion. So it's wonderful to have those divergent voices, different perspectives shared here. I hope sincerely that this will encourage our participants to think about DNS abuse to try and decide which side is that of the end user, and then facilitate those policy discussions.

I understand that this also is a reflection on the question of [Javier] asked in the Q&A pod on international law regulations or standards for DNS abuse. I think it's a fascinating topic, but I'm trying not to lose my moderator hat here so I will stop. I would like our panelists to pick up that comment if they wish and to also look into the question that [inaudible] posted in the Q&A pod how to check a valid domain name. It's a very brief but substantial question. And once we have feedback from our panelists, I will give the floor to the ISOC Chapter support who have raised their hand. Drew and Jonathan, would you like to address the comments and the question? Thank you.

DREW BAGLEY: Yes, I'd be happy to. Pablo, it's good to hear your voice. With regards to the bulk registration, since we're not going to get into who should be regulating or whatnot, I think the discussion's best focus right now is on best practices rather than whether or not they should be mandated or not here just because there's already been work done elsewhere in the ICANN community on those things.

With regards to bulk registration, there was a report that came out in October of last year showing that association that Jonathan cited and that was prepared by Dave Piscitello and his group showing the association of bulk registration with certain types of DNS abuse. So to the extent that bulk registrations also obviously used for legitimate purposes too, I think that that's where there can be various ways to address this issue. But the notion that if we have known behaviors like that that are harming users and we know we could potentially do something about it, where if there's – like Jonathan said, there could potentially be accreditation, but there could be other things too where, even just with bulk registration, kind of like with domain names registered with this COVID thing, if all the sudden domain names with the registrar with these names start appearing on block list and they're all associated with the same registrant, then that's a point where if you have 500 domains names registered and 100 of them have already appeared to be associated with something malicious, then there might be something to do before waiting for the next 400 to harm victims in terms of reaching out to the registrant, scrutinizing what they're really using this for and whatnot. There's obviously no way to completely predict everything. There's no way, in the very beginning, if you're dealing with all other things looking the same between a registration that's going to be used for legitimate purposes and when it's not. But there's some of these things that are very obvious where the data is already there.

And so that's where I think it's probably best for the community to direct its efforts for best practices and figure out what is the way to use this known phenomenon and do something constructive without

obviously doing something that that goes down, a path that no one wants anyone to go down. But the notion of doing nothing, I think the stakes are too high right now and we finally have some data. And to the extent more data is necessary, then I think they'd be great for contracted parties to be partners in helping to figure out what data is needed next and be part of that solution because I don't think it's necessarily binary.

Jonathan, I'll defer to you if you wanted to jump in.

JONATHAN ZUCK: Thanks, Drew. Obviously, this is a hot topic because many of the things that we're suggesting have an economic impact on some of the contracted parties. So there's obviously some tension around that. But at the same time, there have been good experiments and predictive analytics, as I mentioned by .eu and there's a study up on the At-Large DNS abuse page and website that goes into some detail, something like 80% accuracy in predicting potentially benevolent malicious registration. So there are some tools that can be put to use. I really take to heart Pablo's concerns about the comparative resources of smaller and larger registries and registrars. And one of the things that At-Large has recommended was that ICANN be involved in or find a more generalized system that could potentially be used by contracted parties, rather than making that responsibility to create a custom solution that fall on every contracted party. So I think there's a lot to be discussed about the best way to approach this. It's clear, though, that status quo is insufficient.

JOANNA KULESZA: Thank you very much, Jonathan, I fully agree with that. This is why we're starting the discussion here and we hope for it to continue in the Consolidated Policy Working Group on various issues that closely relate to DNS abuse.

We have a question. Seeing how to check a valid domain name, I'm wondering if you guys want to pick it up? I see a hand going down. So we have three open questions in the Q&A pod starting with Laxmi, then one coming from Mohan, and then one more from Pablo. I'm wondering if you guys would like to address these.

DREW BAGLEY: Sure. I'll address the question about the domain name. One of the best ways is of course to start with WHOIS or RDAP and scrutinize the record. But then, to the extent that information is not helpful or just an addition, it's good to utilize many of the free services out there such as the one mentioned in one of the slides, hybrid-analysis.com, but there are several others where you have free multi-scanners. So if you look up "URL multi-scanner" then you'll be able to find websites where you can put in the URL, and then that will check ahead of time to see whether or not it would be legitimate.

JOANNA KULESZA: Thank you very, Drew. I understand that there are technical means and ways and websites that we should make end users aware of for them to have an easier tool to verify the credibility of a website.

We have two more questions in the Q&A pod. Mohan asks, “A malicious registrant can be known only after a [fraud] is committed, am I right? Can it be known before?” I think it refers to this notion of Internet police. And again, Pablo, “Can you imagine forcing hardware stores to identify the intent of those who are trying to buy – I assume commit a crime by a hammer [inaudible]. I’ve heard that argument before, but I would love to hear responses from our panelists, if you would like to pick up those two questions. Thank you.

DREW BAGLEY: Oh sure, yeah. I think there’s already analogies to it. There’s people making certain purchases in some countries, they’re limited in how much of a quantity of something they can buy at once for even a legitimate purpose. So, one example would be even prescription drugs and whatnot. So I don’t know. The hammer is the is the best analogy but there’s plenty of other analogies, especially when you’re talking about chemicals that could be used to make explosives and whatnot, where that sort of behavior does get flagged and at least scrutinized where then an ID needs to be presented or something else. And so that’s something where, to the extent, there’s common indicators. Again, maybe there’s several different methods that could be used. It doesn’t necessarily mean that all registrations are blocked, but maybe registrations are delayed from going into the zone or maybe they go into the zone. But then that’s where, again, there’s that scrutiny of matching those domain names to what’s appearing on suspended domain names or on a block list rather because there’s so many [feeds] out there. There’s so many different ways to address it.

So that's where I would encourage people to again not accept the status quo of people being victimized and they're being "nothing we can do about it" as being acceptable, and then similarly, not assuming that the solution is so draconian that everyone is policing every single domain name before it goes into the zone because there's data and there's indicators there, and then there's a lot of different things that can be used. I think it was a great point that – I forget who raised it. Or maybe it was you, Pablo – but the fact is, not every registrar is going to have the same resources as everyone else, and that's certainly true. So that's where it might not be that a one-size-fits-all is going to work for this problem, but I think that there's enough data out there that we shouldn't do nothing about it.

JOANNA KULESZA: Thank you very much, Drew. I see no hand is up. I would be happy to give you the floor, especially since the question is still up in our Q&A pad. If you would like to elaborate, that would be great. Mohan, the floor is yours. If you're speaking, Mohan, we can't hear you. You seem muted on the participants list. I know. Make sure [inaudible] to that. Please make sure your mic is enabled.

K MOHAN RAIDU: Hello?

JOANNA KULESZA: Yes, go ahead.

K MOHAN RAIDU: My question is, how do we know the intention of a registrant before a crime is committed? Only after the crime is committed, we will know about it. Is there a method to know the intention of the registrant beforehand?

DREW BAGLEY: Sure. That depends on which data a particular party has access to because you could have a registrant that is hopping from registrar to registrar to perpetrate malicious spam campaigns or whatnot. And so that's one where only if a party was in a capacity to know the registrant's e-mail address that had previously been used, in that sense, would you know if it's your own brand new customer. But then there can be other indicators as well. So if you're a registrar that's attempting to comply with the WHOIS accuracy specification and a registrant is giving you inaccurate information, and granted that can happen for variety of reasons, legitimate or not legitimate, but that would be one point where before a domain name has been registered, if the information itself isn't checking out because they're giving a postal code associated with United States but an address associated with Ireland then that's something where something's not adding up in the beginning and that could be an indicator.

So there can be indicators beforehand, potentially. On the other hand, there can be times where there's no indicator at all. And to your point, you don't know anything until the first thing is done. That's why it's imperative on everyone because this isn't something where contracting parties are going to magically solve this problem at all, whereas there's places where there's this repeat behavior where it's known that things

are coming from one registrant account or the domain name is being used to continually victimize people and it remains up, that's where there's data that's showing people that there's something wrong. That's where I think creative energy can be spent to do something about that. Similarly, if a registrant is using the same e-mail address within a party or within a group of registrars linked together to create different accounts, and of course that will depend on their own policies and whatnot, but that's something where you might be able to prevent it within a family of companies a registrant from hopping around and whatnot. I mean, I think that's the key here is you look at where is their data, where is there something where we can ask ourselves why is this repeated abuse happening, and why do people continue to be victimized, and what can we do something about it? But there's not going to be something you can do about every situation beforehand.

JOANNA KULESZA: Thank you very much, Drew. Again, I see a conversation going on in the chat. I see Mohan's hand is still up. I will give you the floor again, sir, in a moment. This is an interesting conversation. So regardless of what your strong position is, I hope that this discussion is of capacity building benefit to all of those participating and just learning the ropes of DNS abuse.

ICANN is contractually based. As we noted, there are different legal categories that usually are used but those seem to be out of scope for this particular discussion. So I believe that the discussion in itself, even if we differ in our positions – and I thank you sincerely for sharing all of those ideas and observations – the discussion itself is a capacity building

exercise. So thank you very much for taking the floor and for offering your views, even if those are contradictory. I think it's beneficial to everyone participating.

I'm wondering if we have any hands up. I would love to hear from those participating in the chat as opposed to us reading out the comments. I don't see any questions at this point. Is there any comment?

Jonathan Frakes: "Who subsidizes the costs of all of this?" That's the question that came up in the chat as well. Not a [typical] one. I'm wondering if Drew our Jonathan wants to pick it up. Thank you.

DREW BAGLEY: Sure. Really, it depends on what we're talking about here. Because again, if we're talking about using the data that we know about some of these types of abuse and then correlating that with best practices, that's one where there can be financial incentives potentially. So that's something that the CCT Review Team, for example, explored where ICANN – and again I know we're not getting into specifics of policy discussion – but the CCT report has some suggestions there. But basically, there's a potential for ICANN to provide financial incentives such as fee discounts if certain best practices are adopted. That could be one direction. On the other hand, there could be other practices to address other types of problems where maybe the cost of doing so up front about flagging something some sort of repeated behavior or whatnot is saving money on the back end with regard to charge backs and everything for fraud prevention. It really depends on the types of anti-abuse measures and whatnot, but this is something that I think is

absolutely one where incentives can be explored because that's something that's already been proposed by the community and even by ALAC. ALAC was represented on the CCT Review Team, that was a cross functional team, so there's a lot of different areas where that could happen. I mean, I think that's the key is to figure out what problems here are solvable, where we have data that something is a solvable problem, and then how can we incentivize that behavior. And I haven't been able to pay attention to the whole discussion, unfortunately, but obviously this is something that I don't think there's any party here that is pro abuse. However, there are very legitimate concerns over, of course, not shying away – legitimate users not preventing legitimate users from accessing the internet, not becoming overly burdensome on small businesses and small registrars and whatnot so that you only level the playing field for big registrars. However, that's part of where I think those inputs can then shape some things that makes sense. And I think there are ways to incentivize the sort of thing rather than all of us throwing up our hands when we see abuse that that is so obvious after the fact, that we can scratch our heads and say, “Why couldn't anything be done about this?” or “Why couldn’t we stop this same person from repeating this and doing a whole entire campaign and stop them after they already were caught?” I think that's the sort of way to focus this.

JOANNA KULESZA: Thank you, Drew, this is wonderful. I just wanted to emphasize that all of those questions are not targeting our presenters. Thank you for accepting the invitation. We’re rather trying to figure out what the facts behind DNS abuse are.

I see Michele's hand is up. I'm happy to give you the floor. We have seven more minutes. Working on capacity building webinars, we would like to learn your [inaudible] on the quality and the scope of this specific webinar. I would be inclined to give Michele the floor for comments. Thank you very much for raising your hand. I see one more question in the Q&A pod. We will try to pick it up, time permitting. If not, we will address this as a typed-in answer in due course. So, Michele, the floor is yours. Thank you.

MICHELE NEYLON: Thank you. Can you hear me okay?

JOANNA KULESZA: We can hear you fine. Go right ahead.

MICHELE NEYLON: All right, thanks. I think I generally disagree with pretty much everything that Drew said apart from the last bit around incentives. The entire kind of negative tone around this and the overly complicated overly technical approach to a lot of this would have a lot of people running, screaming to the hills, and avoiding the Internet completely if you were to believe everything that came out of his mouth.

I mean, the reality is that over the last few months, with more people working remotely working from home, there may have been a rise in cyber security issues in general, but to link the two to all domain names containing terms related to the COVID-19 is farcical. The data doesn't support that. The reality is that a very large proportion of the domain

names that registrars such as ourselves, all being registered across multiple TLDs, gTLDs, and ccTLDs, were being used by governments, semi-state agencies, volunteer groups, and legitimate businesses. Unfortunately, people in the “security industry” have an awful habit of creating very blunt tools including block lists that were made up basically on keywords. So, many domain names, including one that was actually being used by [inaudible] of the Irish police force ended up on a block list that people couldn't even access the URL. I have another security vendor was basing their entire block list off the block list, which was absolutely fantastic. Well done. Pat yourselves on the back.

The fixation with bulk registrations – there's no data to support that. It was one what I would consider a very badly written report that was drafted by two people that completely fixated on that. And it's one of those things like, “Okay, well, what constitutes bulk registrations?” I mean, as even Jonathan and Drew both admit that there's plenty of legitimate reasons why you might want to register larger volumes of names, but nobody's actually defined what bulk registration is. Is it 5 domains? Is it 10 domains? Is it 500 domains? Is it 5,000 domains? If you want to move things on in terms of incentivizing registrars and registries to take to take greater measures, that's fine, but you need to provide reasonable incentives and not fixate on that, and what I would consider to be pre crime, which is absolutely ludicrous.

I think Pablo’s thing about buying hammers is a very, very good analogy. Just because somebody registers a domain name which contains a particular term, it doesn't mean that you can work out immediately what they're going to do. You have no way of knowing what they're going to do with that domain name. The kind of thing we've seen over

the last few years in multiple jurisdictions is wher ccTLD registry operators or governments or both together have decided to come up with string matching lists. So they decide the certain terms are “bad” and that they try to restrict or block them in some way. I mean, the most recent one here in Ireland was where they were one group tried to block all registrations containing the term “bank”. As a native English speaker, you'd realize fairly quickly that if you block all terms, all domain names containing the string bank, you're going to end up blocking such terribly dangerous things like on the banks of the River Lea.

So I think that this kind of thing needs to be more of a dialogue. I think as Jonathan points out, who's going to actually pay for any of this? I personally do not see ICANN as being an entity that should be involved in coming up with any kind of centralized system of any kind whatsoever. For those of us on the contracted party side of things, I think our level of confidence in ICANN’s ability to run those kinds of systems is particularly high and I wouldn't want to see them pouring more money into some kind of system that probably would be ineffectual that wouldn't be widely adopted. Many of us are using our own systems for dealing with issues. If there are specific issues or clusters or things like that where particular registrars or registries are not taking action on clear kind of sequences of infrastructural abuse, then that should be dealt with. But coming out with these broad sweeping statements, when there's actually no real dialogue with those of us who actually do this for a living, I find quite offensive. Thanks.

JOANNA KULESZA: Thank you very much, Michele. We are almost out of time. Thank you for speaking up. As I already said, this is supposed to be an opportunity for the participants to gather information, to collect information, and then participate in policy discussions.

I would love to give the floor back to our presenters for a brief summary. If you guys would try to do that in one minute each, I believe that would be perfect. And then I would beg our attendees' patience for five more minutes for the feedback survey that would help us to plan better for future webinars. I would start with Jonathan, and then go to Drew for a very brief one-minute summary, if that is at all possible. Thank you.

JONATHAN ZUCK: Sure. Thanks, Joanna. I don't know my one-minute summary is … There's obviously a lot of issues to be addressed relating to DNS abuse, but it's very clear that the status quo isn't acceptable that there are very high rates of abuse and that abuse is going up, and that there are, as Michele pointed out, certain registries and registrars that aren't doing anything, and yet the current contract structures prevent taking action against them and they often go on about their business for years before anything is done. And so finding a solution that isn't unduly burdensome on those who are attempting to be good actors is certainly the objective, but it's clear that something has to be done and we need to figure out what that is. Thanks.

JOANNA KULESZA: Thank you, Jonathan. Drew?

DREW BAGLEY: For sure. Yes. I was a bit confused by Michele's response in that sense. In a sense, this webinar is intended, of course, to focus on DNS abuse in the time of COVID-19 and note these examples of issues that we shouldn't just accept. And so I think that what the solutions are, that's something that's forthcoming by all of us as we continue to have this dialogue and recognize the problem and continue to share data. And if there's data that can be shared by others too, that's absolutely part of this dialogue rather than it merely being a bunch of stories of what the burdens would be if we did a policy proposal that hasn't even been proposed, necessarily. And so that's where I think that instead, we should be working together to really figure out, where can we find these common denominators? Where can incentives be created so that this is something that can be incentive-driven because we should take the mindset that DNS abuse is a problem for all of us to solve and not something that's merely for end users to address, either by being victims or trying to escape being victims of it, and we should figure out where those commonalities are and that's how we should develop the incentives.

I think there's already been a lot of great work done by the community that can inform this, and then there's certainly more that can be done, and then there's been plenty done by outside researchers. I don't think that merely even looking to one report is enough. There's been work done for over a decade, really, on a lot of these things related to DNS abuse by a lot of different authors, and I think that it would be foolish for us to ignore that work as we think about a data-driven approach in ICANN.

JOANNA KULESZA: Thank you very much, Drew. I would just like to thank our speakers. I kindly ask Yeşim – for those of you who would be willing to do so to give us a few responses on your expectations and the outcome of the specific webinar. Yeşim, the floor is yours for the survey. Thank you.

YEŞIM NAZLAR: Thanks so much, Joanna. Here is our first question. How did you learn about this webinar? Twitter, Facebook, At-Large mailing list, At-Large Calendar, Skype, colleague, or other? I'm just going to give a couple of seconds more before I move to the other question. Okay, thanks so much for your answers.

Let me pull up the second survey question. What region are you living in now? Is it Africa, Asia, Australia, and Pacific Islands, Europe, Latin America and Caribbean Islands, or in North America? Thank you all for your answers again.

I'm going to quickly move on to the third question here. How do you feel about the timing of the webinar, which is 13:00 UTC? Is it too early, just right, or was it too late for you?

Okay, let me move on to the fourth question then. The fourth question is, did the webinar duration allow sufficient time for questions? Yes or no. Thanks so much for your answers again.

Moving on to the fifth question. The presentation was interesting. Do you strongly agree, agree, disagree, or strongly disagree? Okay.

And here comes the sixth question. I learned something from this webinar. Do you strongly agree, agree, neither agree nor disagree, disagree, or strongly disagree?

And now, here is our last question. I would like to participate in other At-Large webinars. Do you strongly agree, agree, neither agree nor disagree, disagree, or strongly disagree?

Thank you all very much for your answers and back over to you, Joanna.

JOANNA KULESZA: Thank you very much, Yeşim. I'm going to close the webinar in a second. I just wanted to thank our presenters today. Thank you very much for starting this discussion. Thank you to everyone who participated, who shared their thoughts, ideas, concerns. I know that everyone who's a volunteer at ICANN does this because of the good at their hearts, and I know we're here to solve problems. And my understanding is that getting our facts right is the first step to doing so. I'm hopeful that this exercise was a step in that direction.

Thank you very much, Drew and Jonathan, for helping us better understand what DNS abuse is and what it isn't. The Capacity Building Working Group will provide further materials on understanding DNS abuse. And as Maureen noted in the chat, there will be DNS abuse-focused sessions also set up by At-Large during the virtual ICANN68.

Do feel free to reach out if there are any issues we failed to address, if there are any questions you need to have answered. Thank you very much for taking the time to participate. Thank you to our staff, to our

technical support for making this happen. Thank you for your patience with us, even when there were any technical challenges. Stay safe. This webinar is adjourned. Thank you very much.

YEŞIM NAZLAR: Thank you all very much for attending today's webinar. This webinar is now adjourned. Have a great rest of today. Bye-bye.

[END OF TRANSCRIPTION]