ICANN68 | Virtual Policy Forum – GAC DNS Abuse Mitigation (with PSWG) (1/2)
Monday, June 22, 2020 – 11:30 to 12:30 MYT

GULTEN TEPE: Good morning, good afternoon and good evening. This is Gulten. Welcome to ICANN68 GAC session on GAC DNS abuse on Public Safety Working Group. We will not be doing a roll call for the sake of time but GAC members attendance will be noted and in the annex of the communique and in the GAC minutes of this ICANN68 meeting. GAC representatives and delegates are encouraged to share their name. Surname and country or organization they represent in the zoom room. Chat, accurate attendance records and facilitate time the queue for comments and questions during the session it would be helpful if you would like to ask a question or make a comment please type it in the chat by starting and ending your sentence with question or comment, and please keep them short if possible Interpretation for GAC sessions which will include all 6 U.N. languages, and Portuguese. And will be conducted using both Zoom and the remote simultaneous interpretation platform operating by congress rental net group. Information how to install and use this application will be available in the chat pod. Our technical support team is monitoring the Zoom room and are the only ones with the ability to unmute speakers following the GAC support's request to do so. If you wish to speak please raise your hand in the Zoom room, while speaking please make sure to mute all your additional devices. With that I would like to leave the floor to Manal Ismail. Over to you, Manal.

MANAL ISMAIL, GAC CHAIR: Thank you very much, Gulten. And I'm sorry, it took me a while to unmute. Welcome back everyone to the first GAC session on DNS abuse mitigation as we have 2 sessions scheduled for this topic, one before the cross-community panel that will take place later today and the second is scheduled for tomorrow. The Public Safety Working Group of the GAC will be leading this session which is scheduled for an hour. 11:30 to 12:30 Kuala Lumpur time. 3:30 to 4:30 UTC. Over to Gabriel and Laureen. I'm not sure who's going to start.

GABRIEL ANDREWS: Hi, good afternoon. Good evening, good morning and happy father's day to dads connecting from the western hemisphere. I see we have a few topics we are going to discuss today if we move to the agenda. Thank you. We are going to cover the lessons learned from the COVID-19 response. This is the hot topic going on now. There's been a number of parties that have weighed in with their own perspective and we will cover the highlights and share some of the Par pecuniary I was in the law enforcement and public safety perspective. We have shift and do an overview of recent developments related to DNS abuse. Next steps for the GAC and relevant ICANN68 sessions, on DNS abuse that might be of interest to the those in the GAC. Next slide please. So in the past few weeks there were some very interesting presentations on lessons learned from the analysis of COVID-19 related domain registrations. I'll summarize some of the key points hopefully accurately that he woo took from presentations from, from

ccTLD managers and from ICANN's office of the chief technology officer. And we will share some experience that my team had as a U.S. law enforcement agency conducting referrals of similar demands. Firstly ccTLD managers report having taken proactive steps to include registration monitoring along with additional identity verification and they worked closely with local law enforcement, and teams. They further report seeing large spike in COVID-related registrations within which only a very small amount of criminal activity was observed. You'll see that message repeated by the contracted parties, and by OCTO. Some contracted parties reported similarly conducting additional reviews of those domain registrations with COVID terms or key words that's that participate in the framework to address abuse caught out the necessity of taking action to address abuse which risks physical harm which COVID-related domains from the potential for if used maliciously. As an aside, I found that as a federal law enforcement agency that many of the signatories to the framework did, in fact, make a noticeable effort to engage in law enforcement conversations direct communication us with and with partner agencies and found most registrars were responsive to outreach and these deserving of recognition. As before the contracted parties reported only observing very small amount of confirmed abuse within a very large number of COVID domains registered. As seen on this slide in somewhat small text you will see 70% of such registrations were simply parked and not used. An approximately 25% were used for legitimate or beneficial purposes and only 0.5% were observed as evil. Additionally, there were reports of domain blacklists developed by community or security firms which end up being perhaps over

aggressive with some potentially high impact false positives amongst them, by which I mean beneficial sites or neutral sites erroneously included on the blacklist. Some contracted parties felt frustration were being tasked with determining what was or was not harmful versus legitimate or even who to direct the criminal referrals to within a given country depending upon the type of abuse observed. Next slide please. The analysis conducted by ICANN's office of the chief technology officer, I personally felt was fascinating. They recognized potential for fraud and abuse related to the pandemic and they set up to create a system to identify, and refer dangerous domains to relevant parties. To so they performed keyword searchs of COVID related terms and look alike domains known as homoglyphs and so across 16 languages which is ambitious and checked them against new registration notice the TLD. This he went through a number of additional validation steps like comparing against open source security intel feeds or white listing common false positives, for example, in English the word "coronation" contains the word "corona", and if enough information was gathered to make a conclusive case they referred those domains to registrars and registries. Having identified hundreds of thousands of pandemic related domain registrations, they ultimately referred and reported on 10s of domains. So again. Same theme there of there being very many registrations within which an only small number were conclusively evil and that a high level overview but if you're interested and missed the on original GAC briefing and the 15th of June it's worth a watch. Go back and watch the session. Next slide please. Now, I'm going to spend sometime on our perspective. And what I say our I want to

acknowledge that there are multiple nations and even multiple agencies within the United States that did similar processes but impersonally speaking on behalf of my agency as a single law enforcement entity within the United States. Which is to say this is going to be U.S. centric but I do want to recognize that we were far from the only ones doing this. So obviously law enforcement is going to be going off the bad guys much the ones that are most egregiously seeking to exploit the pandemic to commit fraud e-mail, phishing or spread malware but we made the decision to be as transparent as possible with the complaints and reporting that we were receiving. And to share as much of the anonymized reporting as we can with the registrars. To go after the worst of the offenders but not simply sit on the rest. Our source data is very different than the data that's used by ICANN or the contracted parties. Because rather than starting with the hundreds of thousands of domain registrations, we started with the much smaller data set, still in the thousands but much smaller of instances in which domains have been reported to us as having been used to commit fraud. Or to spread malware or engage in phishing. Now this included reporting not just in FBI field offices or partner agencies like FTS or even the Internet crime and complaints center IC3.GOV but we try to encourage reporting of Internet crime but it included valuable data from private sector partners. Partners like Microsoft who operate a major Web mail service and who in realtime reviewed every leak sent through their Web mail service and forwarded to us those which both matched COVID key words and were believed to have been used in phishing or malware spread. Used with permission obviously here. Fisht labs used with permission also

shared with us valuable real word usage. This is intended to highlight how much of a partnership the fight against cybercrime S it's partnership between public safety officials, and cybersecurity practitioners in the private sector and I wanted to highlight how valuable it is to us to have the [inaudible] as we adjust the complaints we were concerned about false positives. So we read every complaint and as we received feedback from the registrars we were passing data do we sought to include more and more information that registrars might find helpful to make a decision on what action might be justified. We used again the help after private sector partner in this case risk I request. To provide safe pictures or screen captures so register stars wouldn't have to visit these risky sites themselves. We pulled virus total and domain tools. ... for easy reference and checked EPP codes to minimize the amount of referrals for sites already down. And we tried wherever possible to include samples of the anonymized complaint itself. When we referred these domains one additional thing we did which was unusual for us we sent alongside them the preservation letters to the registrars. Asking for all the registry information to be preserved. And I'm going to talk to you more later about why that preservation letter was something we felt necessary. Because it's kind of a pain point for us. Next slide please. So numbers. We referred 1,349 domains as of June 12th. Now this number could have been a lot higher but again, we wanted to minimize the number of false positives. And send only domains with enough supporting information that we felt a registrar would be likely to act. We sent these referrals out we can weekly. Go back please. Thank you. That one still is good. We send these referrals out weekly. And our peak

occurred on April 17th on or about with more than 350 domains referred to that week. Now for comparison the next slide which you can proceed to is stolen from ICANN's chief technology officers presentation, and you'll see that their peak of COVID themes domain registrations not use mind you but registrations occurred on or about March 25th. Ours again was April 17th. So our curve similar in shape appeared to follow OCTOs by 3 weeks and it's tempting to draw conclusions from that to say that it might take about 3 weeks for a domain to go from being registered by a bad guy to being used by a criminal, noticed by a victim. Reported to us. Reviewed, and sent as a referral. I am confident that scientists in the audience would throw tomatoes at me for that leap but it's tempting. It does highlight law enforcement referrals which are only valuable because they bring reports of real world use, they're always necessarily going to be reactive. And rarely are such referrals going to be proactive. It's just not a role that we're in a position to effect proactive efforts will almost always have to be in the hands of the registrars themselves. Next slide please. In terms of the number of registrars we sent referrals to. 104 as of June 12th. Shown here are the top ten with a very long flat tail off screen to the right. Now this is not an indictment of GoDaddy. I need to make this clear. GoDaddy were among the registrars communicative and responsive throughout the process. Many others were communicative and helpful in our conversations. They just have bigger market share and I don't think there's necessarily anything more than to than that. The domain that we did it's worth mentioning they went beyond just instances of phishing or malware spread but did include fraud reporting and I wanted to give one example of that.

As came from our Boston field office, who notified us of a veteran's family receiving violent threats at their home. Apparently someone had been selling COVID masks on-line and fraudulently listing the business address as this veteran's residence. So customers who were angry about having paid for masks and never receiving them, had mistakenly directed that anger at this veteran's family and thankfully the registrar in this case TUKAUS was quick to respond to your reach. Very quick and given the threat of physical harm worked with us to suspended the domain it's exactly at that sort of responsiveness that is greatly appreciated by us by our Boston colleagues and I'm sure by the family and this is just one of the 1,300 or so referrals but we appreciate all the occasions in which the registrars felled we pro provided enough information to take objection to protect not only the user of the DNS system but also those who could be threatened by its misuse. Next slide. Having said nice things I am going to say a few things about this pain points now. But remember how I said that we had to send preservation letters with our referrals this is why. 65% of the referred domains that I reviewed shows the registrant used a privacy proxy service typically one affiliated with the registrar of record. I would like you to imagine your a public safety officials who's investigating the fraud and the phishing and the malware using COVID themed domains. And you have identified several hundred each week. What is something you would want to do immediate through to start work on the worst most prolific of the fraudsters and criminals that are doing this? I mean you would want to immediately as soon as possible start comparing registrant data right. To prioritize your efforts. We wanted to do that. We simply decided that we couldn't in

if realtime at least and it just wasn't feasible to do it. Under ICANN policy, and as is currently incorporated in the temp spec a privacy or proxy service can post its own rules how and when they will respond to public safety requests for registrant information and the industry standard response has been send us legal process. When I say that I mean subpoena or court order. Where it once took a public safety official maybe 30 seconds to look up WHOIS data where there was no privacy or proxy used now with criminals overwhelmingly using such privacy I proxy services it takes on average 3 weeks or so to obtain that same data. And so, to ensure that data would be there for us when we came back with legal process, we've been sending preservation letters along with the referrals and there will be follow up rounds of legal process. Probably a lot of it. And it's going to be extra work for us. And extra work for the registrars, and this may be the new normal. Next slide please as for general Internet crime of all types during this COVID pandemic, it's worth noting while we are all at home and more people are in front of computers teleworking, more complaints have been coming in to our IC3.COV Internet crime and complaint center, in the middle of the chart you will see April 2020 received more than 2 and a half times as many cybercrime complaints as April 2019. We are in a vulnerable time right now so extra vigilance is justified. And I thought this was just worth highlighting. Next slide please. This is the final slide on the COVID-19 issues. We wanted to call out that my colleagues Laureen is going to be representing the GAC on the ICANN68 cross-community plenary session that will be immediately following this session. And speaking of Laureen, I'm going to ask me

please in mute her so I can transition to her for assistance with the next slides.

LAUREEN KAPIN: I think I am now unmuted my microphone icon is indicating that. So I'll ask for the next slide. And also thank everybody for participating. I know this hour isn't as convenient for some as others, so well -- recent developments regarding DNS abuse. Some very welcome others a little more challenging first of all quite recently just a couple of days ago the contracted parties registries and registrars adapted a definition of DNS abuse, and they indicated that they defined this as composed of 5 broad categories of harmful activity, insofar as they intersect with the domain name system. Namely malware, phishing farming and SPAM when it serves as a delivery mechanism for the others. So SPAM for example that contains a link that if clicked on might install malware on your computer. And this is consistent with their earlier framework to address abuse. And also, the competition consumer trust and consumer choice review team also indicated that this is consistent with a definition of DNS security abuse. And the GAC going back a little bit earlier also defined security threats consistent with this definition. So as there's been a lot of discussion about whether there is an agreed upon definition of DNS abuse, this is a welcome development that at least there is agreement on a core of certain malicious activities that could constitute DNS abuse. Now, there may be different definitions about whether to expand this core, but that is another topic. We welcome this development. Another development that this relates to is the recommendation by the

consumer trust review team recommendation 14, which really discussed community efforts to develop a definition of abuse to inform further action. So this is certainly very relevant part of the community, and again, we welcome this effort. Now, on the perhaps more challenging side of the equation, there are still enforcement challenges for ICANN compliance, and these challenges stem in part because of the language used in contracts that define the rules of the road for registries and registrars, and we'll be talking more about this particularly in the ALAC session on the public interest commitments and challenges regarding those commitments and that's also later on in a couple of hours. But just to give you an high level overview there are requirements in the contracts for example, from registries that have downstream requirements to prohibit DNS abuse, and what I mean by downstream requirements is that the standard registry agreements do say that registrars have to have provision in their contracts to prohibit their registrants from engaging in DNS abuse. And also registries themselves have to monitor for DNS abuse. But, what the contracts lack are consequences, and I'll put it very broadly. Consequences if bad things happen. So, for example, there's an obligation for -- to monitor for DNS abuse by the registries, but there isn't much meat on the bones for what happens next, and, of course, what happens next after you sought DNS abuse would be very important. Correspondingly, there's obligation for registrars to prohibit their registrants from engaging in this type of abuse but the obligations aren't as specific in terms of how they have to respond from the registrant engaged in such abuse. So there's still, there's still some challenges and improvements that can be made in the standard

language of contracts. I also want to point out in terms of DNS abuse you recall that I said now that there's some good agreement on the core of what might constitute DNS abuse, and specifically these malicious activities that constitute security threats, but the consumer, the consumer trust review team had a broader definition to capture the range of malicious conduct that can take place to exploit the DNS and what the review team recommended, and a full disclosure I was on that review team, and focussed on these issues -- the review team pointed out to a broader definition namely what's on your screen, as something intentionally deceptive cop surviving or unsolicited activities that actively make use of the DNS and or the procedures used to register domain names. And does not include -- and this is a negative, a carve out. -- does not include certain forms of website content ... and this relates to the framework to address abuse, which had a certain exception to this carve out, when contend abuse is so egregious that the contracted part should act when provided with specific incredible notice so that's a lot of words and concept but I this think the bottom line there is that review team that focussed on these issues is advocating for a broader concept of DNS abuse to capture malicious activities that exploit the DNS, so while we welcome we very much welcome there has been some movement here to agree upon at least a core of what constitutes DNS security abuse we think there's room for further discussion to broaden that concept. Next slide, please. I also want to go to -- and I see questions in the chat, and I'm going to -- I think I'm going to advise that we scroll back at the end of the session so that Gabe and I can answer a few of these questions if there's time, and I just wanted to point that out because I do see these

questions, and I'm going to -- hope we can have time to deal with them at the end. Other developments regarding DNS abuse, and here I'm going to focus on certain other recommendations made by the consumer trust review team, some of which are still in appending status by ... some recommendations were accepted, some were rejected, and a good number were put in a, pending status. So there -- there was a suggestion by the CCT review team which was passed onto the subsequent procedures PDP, about making suggestions with respect to mitigating DNS abuse, but at least as of April, regrettably there wasn't a plan to make any recommendations on this topic, and I think that there is a concern that we have contracts that apply to what are now the new gTLDs, we have contracts that apply to the I'll say the legacy gTLDs, and now there's a potential second round and there's a concern about different standards. I would say if we're going to improve the ecosystem of DNS abuse that raising the bar might serve as a model for everyone to strive towards, and in that regard, you could look on this as an opportunity rather than a negative development. Certainly there's room for a discussion there. We will point out certain GAC advice on this topic of the consumer trust team recommendations that specifically focussed on DNS abuse, and in our Montreal communique, the GAC actually explicitly advised the ICANN Board that before there is a next round of gTLDs that, that consumer trust review team recommendations identify as prerequisites to the second round or a high priority item should be implemented. And in our contribution to the subsequent rounds PDP, the GAC expressed concerns with the subsequent round's approach and reiterated the need to implement the recommendations regarding DNS abuse before

the next round. And there's currently consultation on this topic, I think the COVID-19 issues have highlighted that its a very important topic because especially in times of a public health crisis, or some other type of crisis such as a natural disaster, then we know that that inspires not only the good in people to come together and help one another, but it also inspires people who want to take advantage of the situation and take advantage of the public, and part of those activities involving exploiting the DNS. Next slide please I also want to point to the activities of another important review team, the stability security and resilience SSR2 review. They delivered a draft report in January. Many of their recommendations also focussed on efforts to prevent and mitigate DNS abuse and the GAC actually filed an input on that, a public comment endorsing many of those recommendations, and one of the particular things that we endorsed was efforts to approve the DARR system that stands for domain abuse activity regarding and strengthening compliance mechanisms and we will see the final recommendations of that team in October. And then also another, another welcome development is the SSAC is now -- has a working party on DNS abuse issues, and, of course, the SSAC has very special expertise and knowledge won we welcome their input and we anticipate they will discuss... malicious activities and there are a number of sources out there referred to as blacklists among other things, they're also focussed on reviewing affected practices currently takes place in the industry. We know there are a lot of innovative practices among certain domains, among certain ccTLDs, and they will consider new approach ises and make recommendations to the ICANN community perhaps so that these good practices can become more

widespread, and a member of the Public Safety Working Group has been invited to take part. And my PR announcement here the SSAC will be holding a public session on Tuesday the 23rd that you may be interested in joining. Next slide please. So I want to point out for GAC colleagues and any one who is tuning in, there are going to be a number of sessions where DNS abuse topics are covered, there will be a session on... for a meeting with the ICANN Board coming up, first, 7 o'clock UTC, there will be our second GAC plenary session on DNS abuse coming up on Tuesday, and then there will be our meeting with the Board on Wednesday. And some of the topics that we anticipate the GAC will be considering is issues related to privacy proxy services, and you heard my colleague, Gabriel, talk a little bit about that. This privacy I proxy services can make things more challenging for law enforcement's efforts to find out who is behind malicious activities related to certain domains. We'll also be further discussing proactive anti-abuse measures, and again these relate to the consumer trust review team recommendations, and finally, the WHOIS accuracy reporting system, that is an ICANN project that had been active to assess the accuracy of domain name registration information, regrettably its activities were suspended with the advent of the temporary specification, and the changes that took place as a result of EU privacy law, but both the CCT review team and the RDS WHOIS 2 team have recommended that that project resume particularly because it had not yet reached a phase where it was going to measure and assess the accuracy of the identity of the information given related to registrants and, of course, that out of the 3 phases that was the third phase, is perhaps the most important so there is a call for

that project to resume. Both these review teams. Next slides please. And I'm going to preview now. I know that this information has also been distributed via GAC communication but I'm going to preview some possible questions to the ICANN Board, and Gabe, I think you're going to take over this first question regarding privacy I proxy services.

GABRIEL ANDREWS: We are almost done folks but, yeah, just to go back to the notion of privacy I proxy because I called it out early why I I just wanted to remind you why it is that this question exists. And we've just discussed during this pandemic law enforcement has seen an overwhelming number of the criminals we are looking at but mostly criminals there's always the chance there is tea false positives or sites compromised but the majority of these have been behind privacy proxy services and there have of these we were suggesting the question what does the ICANN Board intend do to ensure that such services can't continue to facilitate the threats to the security of consumer trust the DNS. Which in ... can't continue to protect the bad guys.

LAUREEN KAPIN: Thanks, Gabe. The pause sometimes you share because there's little bit of a pause to unmute us. Moving on to questions about proactive anti-abuse measures, the CCT review team has recommended that ICANN negotiate contract provisions providing financial incentives for contracted parties to adopt anti-abuse measures. This was part of recommendations aimed at encouraging these proactive measures.

This is in a pending status and there had been indications that there was going to be facilitation of community efforts to develop a definition of abuse, so we're wondering what steps ICANN has taken to facilitate community efforts, we also have a question about why the existing community developed definitions of DNS abuse aren't sufficient, and the CCT review team pointed out existing definitions, and the last question is whether ICANN would consider incentivizing validation of registrant information by registrars, and what do I mean by that? That means a system to ensure that the information you're getting concerning a registrant. Their name. Their contact information, that that is, in fact, accurate information, and, in fact, currently there are, there are registries and registrars that engage in this process. Next slide please the next question relates to accuracy of gTLD registration data. So that also relates back to our last question in a sense is the follow-up. The issue of the lack of accuracy of domain name information is something that has been pointed out for a long time now. And you'll see here on the slide some background information relating to observation by the first WHOIS review team, some background about the WHOIS accuracy reporting system, again, the CCT review team recommended resuming this project to move into the last phase of identity validation, and this was actually placed in, pending status until the outcome of the WHOIS 2 review, now we have the WHOIS 2 review team recommending the same thing, and that recommendation is also placed in pending status by the Board until the expedited policy development team -- full disclosure I'm also part of that team -- addresses the matter. And now we know that actually Phase 2 of the EPDP team isn't going to have

recommendations that relate to the accuracy reporting system, so there doesn't seem to be any far to resuming this project. But we do know that data inaccuracies are an ongoing problem. So our question is what does the Board intend to do on restore ICANN's ability to address gTLD registration data inaccuracies including but not limited to resuming the case reporting system project identity validation phase. Next slide please. I think we're almost at the end. This is our public service announcement for other session that is you may find of interest. If you tuned in here you may also be interested in our other fine programing so there are other ICANN plenary sessions, we're going to be having the plenary session on DNS abuse and malicious registrations during COVID-19 later on. There's also going to be a session about the DNS and the Internet things, opportunities risks and challenges and as we all know, from whether it's our smart thermostats or Alexa or the systems in our cars, the Internet of things it very much a part of our lives but it also in addition to giving us great convenience, can also present some risks and challenges so I'm sure that will be a very interesting session. The at-large sessions also are dealing with these topics so there will be a DNS abuse and COVID-19 and users issues session, also coming later on. And then DNS abuse setting an acceptable threshold and that will be on Wednesday, and then we also have a session by the ccNSO dealing with ccTLDs and COVID-19 so as you can see this is a very hot topic. There are a number of sessions devoted to these issues where I'm sure you will get a variety of perspectives, and with that, I think we are at the close of our session, and we can have an opportunity for questions. So great I'm going to turn it back to Manal whose hand is up because I'm

wondering what the best way to to deal with questions would be, so Manal, I welcome your insights on this.

MANAL ISMAIL, GAC CHAIR: Thank you very much, Laureen, and Gabe for the interesting presentation. I tried to keep track of the questions. I hope you didn't overlook any. So first question was from -- from Nepal, and the question is is it possible to explaining DNS abuse interesting bot nets, phishing farm and SPAM with the help of a diagramatic name or algorithm rather than... sentences so that it is easy to understand.

LAUREEN KAPIN: I am so wisely going to pass that on to, Gabe.

GABRIEL ANDREWS: Okay. The short of it is you don't want cops writing ... but there are certainly graphics that could be entailed and maybe maybe I'll do so in a future presentation. I don't have any on hand, but I think that especially discussing botnets and so forth these things are easier to visualize if you have a picture and I will take this as a learning point for future conversations.

MANAL ISMAIL, GAC CHAIR: Thank you very much, Gabriel. There was another question from... and the question reads have you heard any response regarding the SubPro letter about the... of not addressing DNS abuse. Isn't this decision thought dangerous in light of the raising numbers just

presented? And although I hope Keith doesn't mind reading one of his responses in the chat, where he said the GNSO council has received a referral letter from the SubPro PDP working group and will be discussing possible next steps on the ccTRT related recommendations related to DNS abuse ago we are looking at the range of possible options that need to be informed by the goal of the word to determine the most appropriate path forward. So I think I can go directly to another question from from... asking Laureen, you mentioned the wider scope of DNS abuse cited in the CCT review and indicated at that content is outside of that definition. Can you help us understand where you see the line being drawn? Example some concert examples of DNS abuse within ICANN's reremit that falls outside the behaviors identified by the CPH. So, and between brackets identified as security abuse by CCT. So, Laureen, can I hand over to you?

LAUREEN KAPIN: Sure. And it's a fair question, and I would love to have our report in front of me because it probably does contain some examples. And I think what I prefer to do Becky is take a closer look at that to see what the team -- and I suspect this goes back to the DNS abuse study that was -- that was commissioned by the CCT review team, that came up with some very interesting statistics related to some examples of systemic DNS abuse, and I -- my thought would be that if there were scenarios where specific malicious activities, and deceptions for example, were being conveyed perhaps through the use of a demain name itself, that that might fall outside of the core of DNS security abuse, but still be an example of exploiting the DNS, and that is

something that would still be within the remit of ICANN to deal with because it would be an exploitation of the DNS. But I do also want to do some further digging about that, but that might be an example that helps, and I think we see in the context of COVID-19 for example, that is exactly the type of scenario that law enforcement has been engaging with registrars in particular on, where we've been looking at just the domain names in particular, because those domain names have an inherent message of deception, for example if you have a domain that says effective COVID-19 vaccines, or effective COVID-19 cures, there are no vaccines now that are effective, and there are no cures now that effective. So the message of that domain name itself indeed could be problematic. So that's one example, and there are likely others, but I hope that's helpful.

MANAL ISMAIL, GAC CHAIR: Thank you very much, Laureen, and I hope I haven't overlooked any of the questions typed in the chat. I think there's quite interesting discussions in the chat, and I invite everyone to have a look at them, and please, if I overlooked your question or comment, please type it again, and I will make sure to read it out loud. Meanwhile, any other questions or comments? Okay, I see none. Then thank you very much again, Laureen and Gabriel, for this very interesting presentation. We are giving everyone 5 minutes back. It's now time again for a 30 minute break. Please make sure to attend the cross-community plenary on DNS abuse, and malicious registrations during COVID-19. It's scheduled for an hour and a half, 1300 to 1430 Kuala Lumpur time, 500 to 6:30UTC and the PSWG was part of the organizing team and

Laureen is participating on the panel. This plenary will be followed by a 30 minute break, then we will reconvene here in the GAC Zoom room so please be back in our room at 1500 Kuala Lumpur time, 700UTC to start preparing for our meeting with the Board. Thank you everyone. Enjoy your break.

[END OF TRANSCRIPTION]