ICANN83 | PF – GAC Discussion on DNS Abuse Mitigation
Tuesday, June 10, 2025 – 09:00 to 10:15 CEST

JULIA CHARVOLEN

Welcome to the ICANN83 GAC Session on DNS Abuse Mitigation on Tuesday 10 June at 7:00 UTC. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior and ICANN Community Anti-Harassment Policy. During this session, questions or comments will only be read aloud if submitted in the proper form in the Zoom chat pod. Interpretation for this session will include all six UN languages and Portuguese. If you would like to speak during this session, please raise your hand in the Zoom room.

When called upon, participants will be given permission to unmute in Zoom. Please state your name for the record and the language you will be speaking when speaking a language other than English, and please speak at a reasonable pace to allow for accurate interpretation. I will now hand the floor over to GAC Chair Nico Caballero. Thank you and over to you.

NICO CABALLERO

Thank you, Julia. Welcome, everyone, and welcome to our topic leads and guest speakers, we have Martin Kunc, from the National CSIRT of the Czech Republic, we have Karin Rose and Greg Aaron from Interisle Consulting Group, we have Graeme Bunton from the

NetBeacon Institute, Susan Chalmers, of course, you already know her, she's a U.S. representative and the PSWG topic lead, we have Janos Drienyovszki from the European Commission and Mr. Miyamoto Tomo from Japan.

Welcome, everyone. We're going to have very interesting discussions on DNS abuse mitigation, of course, and then we'll open the floor for, I hope, an interesting and engaging Q&A session. So without further ado, let me hand the floor to Tomo. The floor is yours. Please go ahead.

TOMONORI MIYAMOTO

Thank you, Chair. Good morning, everyone, and good afternoon, good evening, the colleagues who joined online. I'm Tomonori Miyamoto from Japan, and I'm looking for the fruitful discussion for today. And here's the agenda for this session. After a brief, my introduction, we will have presentation about updates on DNS abuse landscape and mitigation mainly focusing on phishing as the host country presentation, the CZ NIC presents their phishing campaign and the entire present their insights.

And as a second part we will discuss PDPs, Policy Development Process for the next step. We will focus on the narrowly scoped PDPs to shorten our timeline thinking about the delegation of new gTLD next year. Next slide, please. So here's some background of the DNS abuse discussion. The ICANN contracts RA and RAA

requires gTLD registries and registrars to take mitigating actions when they receive actionable reports of DNS abuse.

There are various understanding and context of misuse, maybe including phishing, scam, copyright infringement, like my country Japan has a big issue of manga piracy. However, the definition of DNS abuse in the ICANN contract is limited, perpetuating malware, botnet, phishing, farming, and spam. The amendment in 2024 of this contract is a first step towards DNS abuse mitigation and we consider and take further steps to deal with the challenge of DNS abuse.

So next slide, please. Thank you. Some of you might be familiar with this chart. This shows the whole ecosystem or landscape of this matter. And the ICANN limit or scope of the ICANN contract is a green square on the left-hand side and it is fairly limited. To deal with the problem effectively, we may need to consider the relation in the blue square like the contract between registrars and resellers.

And we may also see cooperation between extended community in the red square like Trusted Notifier program. Today we will mainly focus on the green box for the possible PDPs looking ahead to new gTLD next round in the next year. But we should take into account the whole picture surrounding the contract. Next slide, please. In the previous ICANN meeting in Seattle, we reviewed the situation and evidence on DNA service mitigation, including the INFERMAL report.

And last week, we held the Pre-ICANN83 GAC Webinar, and we had a presentation from the NetBeacon Institute about the possible PDP ideas, and contracted parties shared their perspective and response. In addition, the GNSO Small Team on DNA Abuse started this April, introduced their timelines and objectives. Collaboration with this DNS Abuse Small Team should be our possible further way forward.

And today, in this discussion, we will discuss the policy development. Next slide, please. So this is the last slide for the introduction. This is not 100% accurate, but I visualized and organized some topics and discussions on DNS abuse. You can see the two-way arrow on the right side. Measure during the abuse report and mitigation can be called a reactive measure or abuse handling. Here is the obligation based on the ICANN contract as I said, and we might think of the reporting for transparency in addition to the great work of ICANN compliance team's monitoring.

And we may also think measures for shorter reaction time such as Trusted Notifier Program. In addition to these measures, we can also think about proactive measures including proactive monitoring before the report and some additional rules at the moment of registration like the circle or point on the left side.

And based on the results of the INFERMAL report, restricting bulk API registration or timing of user information verification can be considered. The next slide, please. Now let's move on to the next

part. First, we'd like to invite Martin from CZ NIC as the host country presentation. So Martin, the floor is yours.

MARTIN KUNC

Thank you. So I'm here to share our case about phishing in Czech constituency. Next slide, please. A little bit about our projects, maybe you know about them. Most important ones, I guess, could be the Routing Demon Bird and the registry thread. You may also know the advanced DNS measurements we do and we call ADAM, the NodeDNS server and the TURRIS router.

Next slide, please. So who we are, CZ. NIC is a .cz domain registry who also operates the National CSIRT or CSIRT.cz, and there is me as a Security Analyst in this case. Next slide, please. So the story begins in June 2022 when we saw yet another phishing site, which wouldn't be that much interesting but on .cz it's quite unusual. We try to take care of our domain, and about that same time something called housing allowance came into place.

So there was government subsidies to help citizens in bad situations to get some money extra for their cost of living. Next slide, please. A little bit about the movie characters. We have the Ministry of Labor and Social Affairs. It doesn't play a big role here, but it's just for you to know the brand.

Next slide, please. Then we have something that's called BankID. I assume this is not very common in other countries, but in Czech Republic, banks came together and put together something called

BankID, so you can use the same credentials that you use for your bank to access, let's say, government sites. So the citizens were the victims in this case, and then we have the bad guys.

Next slide, please. Scenario of this phishing is quite common. People got SMS, look, you get some money here, you just click on this seemingly governmental website and you will be, well, not rich, but you will get more money. Next slide, please. And there were quite a number of those osmosis.

Next slide, please. As you can see here, I understand it's real difficult for you to understand what's written there, but basically it's just saying, you just click here, login, and you get the money. Next slide, please. So after you click the link, you end up on a phishing site which requires you to login using your BankID. We have other things, other types of authentication that you can use, but they specifically ask for BankID because there is a clear way how to misuse that.

And the funny thing was that it was only possible during so-called business hours. There was a case in Czech Republic with the Czech Post, that they lost your package or whatever, and you had to access the site only during business hours. And if you knew the Czech Post, that would seem legit, that they have a website that doesn't work 24/7, but in this case, it was kind of a give-off, and they needed this specifically because on the other hand the bad guy was using the credentials in the real time and they also got your confirmation with your second factor.

Next slide, please. This is one of the examples of the site. It pretty much looks the same except the URL of course. Next slide, please. This is another example. Here you can choose the bank. It was not always that you could choose any bank, but they specifically required some that work at the time, I guess. And if it's visible for you, in the URL top corner, there is a number which increased each time a user clicked on this. So we could get somewhat estimate of how successful they are with this campaign.

Next slide, please. This is another view. Next slide, please. So in 2022 they started with just 11 domains per month, which was still unusual and more than enough, but it was not that bad. In February 2023 they had 72 domains registered in a single month, which was really a lot for us, but at that time we were ready and we were taking them as fast as we could. Next slide. So we knew that they were improving over the time and we wanted to also improve on our end. So we started with active searching and we tried to improve the process and we tried to study and make notes because even the little details mattered.

Next slide, please. Among the examples of active searching, we were able to search through the zone and we could see the domains that were registered. So at first we tried to use the similar characters that were used for the site, but most likely because they needed to change and come up with the new ideas, new names, it was not that useful. So in the end, we resulted to looking at just

like last week registered domains and this was our source of information. Next slide, please.

That helped us to have a future phishing domains list and we were able to scan those periodically. That was about five minutes. Each five minutes, we tested them and not a single time we were bounced, not a single time our IP address was blocked, so they really didn't care about us scanning. And as soon as we figured that there is a phishing site up and running, we got a notification actually in our phones and we were really happy to act even outside regular hours to take it down as fast as possible.

I was working on this with Peter, so I have to thank him here. And over the time, we were able to shorten the time for take down, which was really crucial in this case, as you will see later on in the graphs. Next slide, please. We made notes of what we've discovered. So the pattern was clear, website always emerged several days after registration, because first they need to register the domain, they need to set up the DNS records, they need to get the certificates.

After everything was ready, they enabled directory listing on that site and upload the zip file. At that moment, quite a number of times, we were able to pull the zip file of the website and analyze it, and the samples were sometimes same and sometimes they differed as they improved their game. After that, they unpacked the zip file, and the site was up. Next slide, please.

So, just in case you're curious, certificate transparency is really a thing, not only we were able to find the subdomain as an admin panel with no password needed where we could see everything, the attacker would see all the sessions that were created. But certificate transparency currently helps us finding domains that are not on .cz, that are not visible for us beforehand. Next slide, please. In the end, we consider this a victory because they stopped immediately a month after their big try, with just only 28 domains registered in March compared to the February 72.

And we haven't seen anything that could compare in this size since then. Of course, there are several tries with other TLDs and single domain here or there, but nothing of this size. Next slide, please. This might be a little difficult to understand, but I will try to explain. The green color here represents the queries that weren't resolved correctly. Usually that would be in red, but in this case it's in green because we are happy that they weren't resolved because those are the phishing domains we were able to prevent the access to them.

The black ones are those that were resolved. It's important to say that this is not actual number of users, of course, because we don't see how many users are behind a single resolver, but it gives us at least an estimate and at least gives us a number of how are we going and how are we faring against them. Next slide, please. Compared to this, this was much better. As you can see the green graphs are much stronger here, so we considered this as a kind of

victory and that we are getting our game right and we are improving.

Next slide, please. Something about behind the scenes, in our rules, we have Article 17 that enables us to kick out the domains out of the zone which we suspect are disrupting cyber security. At that point, we give them out-of-zone status, which can be kept for one month, which gives us enough time to give the domain owner the chance to come up to us and tell us what's going on, and this is me, and this is something that is supposed to be happening.

So this is kind of, if we do something bad, this is how we can get around it and how we can improve it. And we also publicly list those domains that we block. Next slide, please. That's all from my side. I hope you enjoyed this and I hope you have questions.

TOMONORI MIYAMOTO: Thank you, Martin, for sharing the experience in Czech. And now we try to open the floor for the Q&A. And do we have any questions? Ah, Gabriel. Yeah.

GABRIEL ANDREWS: Hi, this is Gabriel Andrews for the record. And thank you very much for the presentation, Martin. I was really interested in that and really impressed, actually, when you were covering the part where you talked about recognizing that there were suspicious domains being registered, but I think you were saying that you didn't yet see

that the phishing sites were set up, but you started monitoring those domains and setting up rules to check and to alert.

And if I understand that right, that seems very proactive of you, but I'm sort of wondering, did you feel you had to wait because you needed to have a certain amount of evidence before you could take action? And I just wonder if you could expand on that a little bit.

MARTIN KUNC

Yeah, exactly. So at that time, we really waited for the evidence. So we had something to pick us up in case we blocked the domain, and so to prevent some research project or something going on that would not be good, and in this case, we really wanted to wait. And even our process is set up in a way that if we make a file and log evidence, the site at that moment still needed to be up just at the moment of blocking it.

GABRIEL ANDREWS

I can just say I don't think I've ever seen such proactive, or at least I haven't heard of such proactive behavior before. I think that's really impressive and very interesting to see. I know there's been challenges in the past in my own reporting of domains that we think are going to be used in the future, but you don't yet have the evidence, and it's been sort of a challenge trying to figure out where that balance lies.

And the fact that you're able to set up those rules to monitor yourself and take that extra initiative to see the instant that they're

registered or that they're set up to phish. That's really cool, and maybe there's a lesson to be learned there. Thank you.

MARTIN KUNC: Thank you for that. And just to add, this was a single phishing campaign, so we were able to see the important nodes so we could actually detect the domains that there are going to be phishing ones. Otherwise, we don't have anything to catch up on if it's a new kind of phishing case. Thank you.

TOMONORI MIYAMOTO: We have Ashwin.

ASHWIN SASONGKO SASTROSUBROTO: Yes, thank you. Aswin, from Indonesia, for the record. Thank you for the two speakers' presentations. I just want to ask several things. How effective is the use of activation of DNSSEC, secure DNS, in the websites, and also the use of certification of ISO IEC 27001?

Can it help the DNS abuse, or it just doesn't work? And secondly, from the speaker from the SEC .cz, normally you give a lot of examples of phishing and so on. Do they usually use ccTLD .cz, or they use gTLD .com or whatever? Thank you.

MARTIN KUNC I'm not sure if I followed the first question correctly, so please repeat it afterwards. But regarding this, this was specifically focused on .cz domain, so this was easier for us to follow, but we have cases that use any other domains too, but not as big, let's say.

ASHWIN SASONGKO SASTROSUBROTO Yeah, the first question is actually, in the ICANN website, they always urge us to activate the DNSSEC. How effective is the activation of DNSSEC to do something against the DNS abuse mitigation? And also, Indonesia, like many other countries, are a member of ISO and IEC, and together we produced ISO IEC standard 27001, which is a security management system. I want to know your experience. How effective is that certification, 27001, against DNS abuse. Thank you.

MARTIN KUNC Okay, so with DNSSEC, it doesn't help against phishing at all. There's just no way I could see that working. And regarding the ISO standard, I have to say I'm not the guy to answer that question because that's far from my focus. Sorry.

TOMONORI MIYAMOTO And next is Aderonke. Sorry for my bad pronunciation, but yeah go ahead.

ADERONKE ADENIYI

Hello everyone. Thank you, Martin. My question goes to Martin. Your presentation like the previous speaker did say was fantastic, it's novel for me. Well, for the records, my name is Aderonke from Nigeria. My question is regarding the BankId.

Did you consider when trying to mitigate against the DNS abuse, working with the bank regulator, because back home in Nigeria we have something similar called Bank Verification Number that cuts across all banks, considering digital service platforms. But I just wanted to know, at any point, did you work along with the financial services regulator or the issuer of the BankID? Thank you.

MARTIN KUNC

Yeah, so from my point, we weren't really successful to reaching out to them, but luckily, they kind of took things into their hands and they started letting users know about these phishing attempts and they used their apps to send notifications out. So I guess they are trying their best.

TOMONORI MIYAMOTO

Okay, thank you. And now we'd like to move on the next part. We'd like to invite Karen and Greg from Interisle presentation about the scope and distribution of phishing. So over to you.

KAREN ROSE

Thank you, and dobar dan and good morning. I'm Karen Rose and this is Greg Aaron and we're from Interisle Consulting Group. Greg

and I both have 25 years' experience in the domain space and we are very pleased to be able to speak with you today. For the last five years, Interisle has been researching various aspects of internet resource abuse in the perpetration of cybercrime.

And today we've been asked to focus specifically on DNS abuse as it relates to phishing. But you could find a broader take on resource abuse issues in our published reports. Since time is short, we will jump right in. So next slide, please. The bottom line, unfortunately, is that phishing and DNS abuse are growing at an astonishing rate. Over 2 million phishing attacks and 1. 5 million phishing domains, unique phishing domains, were identified in the last 12 months alone, and this is up over 425% on a quarterly basis in the last five years.

And this vastly underestimates the problem as so many attacks simply go unreported. 77% of these phishing domains were specifically registered for the purpose of conducting a cyber-attack. And phishing imposes high costs on society. Over $18,000 in direct financial losses are experienced every minute. And this vastly underestimates the impact as well because most losses go unreported, especially globally. I think we have to conclude here from this growth that DNS anti-abuse efforts to date have been largely ineffective.

And if you're wondering there what that dip is about halfway into the chart, that was due to the shutdown of a company called Freenum, which was a very phish-friendly domain company. The

demise of Freenum set fishers off their pace for a little bit, but as you will see, they quickly picked back up and their abuse rates rebounded. Next slide, please. Phishers tend to exploit two things when registering domain names, cheap prices and easy registration.

The sweet spot for phishers are domain names priced at about $2 or less. And these are price points that are very common in the new gTLDs, which phishers exploit at disproportionate rates. If you look at the top chart there, you'll see that the total market share of new gTLDs, that small yellow red wedge, is only 11%. Yet if you look at the bottom chart, you'll see that new gTLDs accounted for over 51% of all phishing domains in the past year.

That said, com and net also remained quite attractive to phishers at 32% of all phishing domains. One way that phishers can cheaply access .com and .net domains are through things like free promotions and bundled hosting deals offered by some registrars. Phishers also exploit easy registrations and target TLDs and registrars that impose few requirements and few data checks. And my colleague Greg will talk about bulk registration in just a minute.

Phishers also have preferred suppliers, registrars and TLDs that sit at the crossroads of cheap and easy. The most abused companies tend to rank in the top five and top ten year after year. We don't have time to go through these rankings today, but you can find them in some of our recent reports.

Next slide, please. Phishers often register names in patterns, and often these are very conspicuous and very easy to spot. I brought some examples here from actual cyber-attacks for you today. On the left, you'll see one tactic is algorithmically generated names, which are often variations on a theme or even completely random character strings.

Names closely matching brands to dupe unsuspecting consumers, and phishers often use the same registration data over and over again or even clearly false and bogus information. Automated tools, however, can be implemented to screen for these abusive patterns. And some ccTLDs already have specific DNS systems in place to screen, and there are also commercial tools available for things like address validation. Next slide, please.

GREG AARON

Every year we study how these domains get registered, and when phishers and other criminals register domain names, they usually don't just register one or two at a time. It's very common for them to register an entire set. And as Karen said, they're usually following a pattern, and so these tend to jump out. But you can see these if you look at sets of domains registered one after another at, say, a particular registrar.

At least 37% of the domains used for phishing are in batches. And our methodology undercounts. We see which ones were used for phishing, we can see they're related, but there are other domains in those batches that we haven't found and caught just because it's

very hard to capture the data sometimes. Sometimes these batches are extremely large. We found one batch last year, which was 17,000 plus domains used by one perpetrator.

The idea is that phishers especially now are moving quickly. Victimization happens in the first eight hours once a phishing site is launched. So the phishers assume they're going to get caught, their domain name might get suspended at a certain point, but they have others teed up. One of the reasons we see more and more domains being used is because of this automation.

They're ready to churn through lots of domains and keep their attacks going, and as long as they can make a profit and keep those sites up for a little while, they keep going. We see so much phishing because it is successful. So, we have to think about why this is taking place, why we have this constant churn. Next slide, please.

KAREN ROSE

So, DNS abuse is made possible by choices. Choices ICANN makes in the policies and business standards that shape how the market functions, and the choices that companies make in conducting their business. We often hear the mantra that competition is good, so just adding more competition must be even better, right? But from an economic perspective, this is not always the case.

Absent reasonable rules, over-competition can have negative consequences. And DNS abuse and the cybercrime it fuels is like the industry's pollution. It's an economic negative externality

imposing costs on consumers and society. And the DNS market is quite competitive today. There's over 2,000 registrars, hundreds of open gTLDs, and to a cybercriminal, domain names are commodity goods. They're pretty much interchangeable, and these can be produced by the industry at almost zero marginal cost.

So absent effective anti-abuse policies, criminals today are very easily exploiting these market dynamics and choices. What we really need, we believe, are reasonable, proactive measures to help curb domain abuse before it happens and not just mitigate domains after the damage is done and the harm has taken place, although more efficient mitigation will always be useful.

And it's important to do so now and implement policies now, because as new gTLDs enter the market potentially with the new gTLD rounds, this is going to place further downward pressure on domain prices and increase competitive pressure in the market. And if nothing changes, that graph is going to continue to keep going up and to the right. Next slide, please.

GREG AARON So one of the trends that we're seeing, especially in Europe, is that the registry operators are doing new things. Some of them, for example, are not asking all of their registrants to prove who they are up front, but they're taking risk-based approaches. For example, we've seen several registry operators say that, okay, bulk registrations are an example of risk.

We have registrants coming in, we don't know who they are, but they're registering lots and lots of domains. So maybe we should ask them to verify themselves and perhaps not allow those domains to resolve and work until we have some confidence about who they are. So that's a risk-based approach that's now happening in some of these European TLDs. ICANN's current requirements for verification are very minimal.

And in fact, one of ICANN's recent compliance efforts found that 20% of the registrars who were audited were not doing the currently required minimum validation steps. So we see this as an opportunity to look at risk-based approaches, to do verification, and to do prevention, which will make it harder for criminals.

Next slide, please. So our ideas for discussion include strengthening verification requirements, looking at those bulk registration problems. And these two things, by the way, can go hand in hand. Another fact that you may not be aware of is that ICANN's contracts require registry operators to do business with any and all ICANN accredited registrars. Now, there is a good reason behind this. People didn't want companies squeezing each other out, we do want a competitive and even playing field for all the companies involved.

However, registries are still required to do business with registrars who bring them lots of bad business. And that is a situation that we suggest be looked at because that puts sometimes a registry in a bad situation and then makes them look bad because they have

bad registrants flowing in. So perhaps there are some things we can do there.

And of course, registries and registrars do have tools. Some of them are experimenting with systems to find abusive domains before they happen, and there's some discussions taking place this week about those kinds of solutions. So we want to leave you with the fact that there are some tools and solutions out there and also possibly some policies that could improve things. Next slide, please.

KAREN ROSE

So we have some new reports with data coming out in Q3 this year, so be on the lookout for those. If you'd like to look at our reports, again, we don't just look at domain names, we look at things like abuse and hosting, abuse and subdomains, and some of our research also looks at phishing, spam, and malware. So we invite you to take a look at our reports, and there's the website.

Our data sources, our methodology, and additional data is on a website of ours that's called the Cybercrime Information Center, which is a project of Interisle. And we have extensive data and extensive rankings there if you'd like to take a look. We're also on Substack and release blog posts every few days, a couple times a week, so take a look there, and of course our website and we'd be happy to communicate with you via email. Thank you very much.

TOMONORI MIYAMOTO: Thank you, Karen and Greg, for your presentation. And for the sake of time, let us move on to the next part. If you have any questions, then please cancel it, later on this session. So I'll pass the button to Janos. So please.

JANOS DRIENYOVSZKI: Thank you, Tomo. And now we would like to turn to next steps in terms of policy making and potential micro-PDPs or policy development processes that could address the issues that have been discussed. So I would like to give the floor to Graeme from NetBeacon to provide his presentation.

GRAEME BUNTON: Thank you. Good morning, everybody. My name is Graeme Bunton. I'm the Executive Director of the NetBeacon Institute. NetBeacon Institute is a part of Public Interest Registry who operate the .org TLD in furtherance of their not-for-profit public benefit mission. Relatively recently, about two weeks ago now, we published a white paper proposing five potential PDP ideas that we wanted to share with the community.

I don't have a ton of time, so I'm not going to go into the particular details of these PDP ideas in depth. I will get the link to the whole long 22-page white paper that you will all enjoy, I'm sure. But I'll just cover it very highly here. Next slide, please. A brief note on why we did this work. So the NetBeacon Institute spends all day every day thinking about how to reduce DNS abuse. But we're also a part

of a contracted party, and so we have this relatively unique perspective.

We do pretty similar work in many ways to what InterIsle does, where we have a project to measure and understand DNS abuse across the ecosystem called NetBeacon Map. We also run a centralized abuse reporting service called NetBeacon Reporter, where we see tens of thousands of abusive domain names flow through this every day. And so building on that data and those insights, we wanted to provide… slow down. Yes, sorry, far too fast.

We wanted to see if we could support community conversations to put some ideas forward that we think would be able to be achievable in a timely fashion, incrementally impactful on issues of DNS abuse, and really show this community what we think narrowly scoped PDPs might mean. Next slide, please. So I'm not going to go into these in detail. Briefly, an associated domain check, this would be an obligation for registrars to pivot on reports of abuse.

They receive a well-evidenced, actionable abuse report for a malicious domain name. A registrar would be obligated to see if there are others related to that domain name and take action where there is evidence of abuse. Next slide, please. Gating APIs; one of the key outputs from the informal report from ICANN, and kudos to the ICANN OCTO for that report, was that ungated APIs were, I think it was 401%.

So a registrar with an ungated API was 401% more likely to have abuse. And so what can we do about this? How can we put some friction in place before registrants have access to these sorts of tools that enable that sort of large bulk registration behavior? Next slide, please. Subdomain abuse contacts. This is a proposal to see if we could take the DNS abuse obligations that exist at the registrar level and apply them to registrants who offer subdomains to third parties.

Next slide, please. Registrant recourse mechanisms. In the context where we have registries and registrars working diligently to try and combat DNS abuse at scale, mistakes are going to be made. And we need to ensure that registrants incorrectly impacted by abuse mitigation have a clear path to address mistakes being made. Next slide, please. Botnets and DGA coordination. Right now, to disrupt botnets and domain generation algorithms, law enforcement typically have to approach each individual registry independently, and this is inefficient.

And so, we're proposing here a centralized function within ICANN to collect and then disseminate that work and bring more efficiency to the disruption of botnets. Next slide, please. So I could talk about each one of those individual potential PDPs for quite a long time, and I would be very happy to do that if you want to find me in the hallways.

But I think there's a couple of key takeaways for this audience that I want to make, which is there is a real opportunity right now to

move forward in this community on PDPs, on policy development, to make a real difference on DNS abuse. But we really have to ensure that we're all collectively committed to doing narrowly scoped, issue-constrained processes. No one can get everything they want. Progress is going to require focus. Timely progress is going to require very intense focus. These issues are complicated as we get into the weeds on those potential ideas should the community choose to adopt them.

There's real operational impacts, there's real issues that need to be sorted out, but we can make some wins. We can have some small, incremental, timely wins, and that is better than none. I think the size of bite we take has a real relationship to how much chewing we've got to do. And I think we really want to see if we can get this community to take some small bites, chew, and have a nice meal, make a difference on DNS abuse in a timely fashion.

And then a last piece I'll make that I want to really reinforce is, and building on what Interisle was saying about the patterns they see in DNS abuse, is that thematically, we need to move from individual abuse reports to addressing DNS abuse at scale. So the contractual amendments that were put in place last year are great. We see in our data all the time registries and registrars suspending malicious domain names. But the obligation is at the level of the individual abuse report.

And so two of our proposals, the first two, the associated domain check and the restricting access to bulk API, are trying to see if we

can move reasonably and responsibly into a place where we're addressing abuse, not just at the individual report level, but at the scale of abusive campaigns. And that is, even if these aren't the specific right ideas, I think the way that this community needs to be thinking about how to address abuse going forward. And so from our perspective, having published that white paper, we've achieved our goals.

The community is talking about ideas, they're talking about constrained ideas, ideas that we think could be successful. And even if it's not these, they're scoped right. And so that's what we would like to continue to see in this community. We hope the community continues to talk and discuss and move forward on ideas like this. So thank you very much for the opportunity to be here today. I really appreciate it.

NICO CABALLERO

Thank you so much, Graeme. Before I give the floor back to Tomo, I would like to kindly ask our distinguished GAC representatives to take into account the need for swift action given the fact that the bad guys are at this very moment watching us. So if we develop a PDP and in five years we decide -- they're already you know two or three steps ahead of us. In my humble opinion we should really act fast. Back to you, Tomo.

JANOS DRIENYOVSZKI

Thank you, Nico. So now moving on what we believe the GAC should focus on in terms of potential narrowly targeted PDPs. Before jumping to my presentation, I wanted to also quickly go through the ideas presented by the contracted party house yesterday in a meeting, four ideas, because I believe this is beneficial to our discussion today.

So one of the ideas was to create a requirement to pivot an actionable report of maliciously registered domains. This would lead to disrupting other malicious registered domains in the same registrant account. Second idea was a potential contract amendment to ensure registrars that offer an API or reseller program to have necessary contractual means to impose DNS abuse mitigation requirements on their resellers.

Idea number three was to develop an operational framework to provide all gTLD registry operators with a verified list of botnet generated domain names. And the fourth idea was to develop best practices for reporting phishing to improve the quality of reports. Now, turning on what we believe the GAC should focus on or ideas to be further discussed, a lot of mention has been made today of proactive measures and bulk registrations in particular.

So we are at a stage now where we're exploring the wide landscape of useful proactive measures and as well as mitigating or reactive measures. But if the objective, as Nicole also alluded to, is to achieve something quickly and something meaningful before the new round of gTLDs in particular, there should be some sort of

prioritization on some specific actions, which also links into what Graeme said about very narrow and targeted PDPs.

So in the Seattle communiqué, the GAC put forward to consider it important to look further into the topic of bulk registrations of domain names as one of the most correlated drivers of DNS abuse, also according to the INFERMAL report that was referenced. So, of course, bulk registrations carry, as has been shown this morning, bulk registered domains carry a higher risk of being associated with DNS abuse and their impact is also higher compared to single abuse domains.

And the INFERMAL study also found that stricter registration policies and proactive verification measures can be conducive to mitigating DNS abuse. Therefore, it is clear that some additional friction should be built in the process of bulk registering domains. Now, we believe one idea could be in this regard to require contracted parties to implement proactive measures with regard to bulk registrations.

This can include restricting bulk API registrations, for example, by restricting API access to known or vetted users, either based on identity verification or registrant activity or reputation, as also was put forward by Graeme in his presentation. And this idea we believe it is one of the most realistic to achieve on a consensus on a short term. There could be also high requiring higher pricing for bulk registered domains, delayed registration or limiting registration volumes, et cetera.

So such proactive measures would complement the reactive measures or mitigating measures set out also in the contracted party house proposal to pivot actionable reports as well as NetBeacon's proposal to check associated domains and take appropriate action upon confirmation of a malicious registration. So we would achieve in this way a combination of proactive and reactive measures with regard to bulk registrations.

Now turning on to other proactive measures that are possible and other mitigating measures. Both in the Hamburg communiqué, the GAC reiterated the importance of proactive monitoring, and in the Seattle communiqué, also, there was a mention of proactive practices for addressing DNS abuse and links between addressing DNS abuse and work on domain name registration data. And the GAC encouraged registrars to explore the use of AI-powered DNS abuse detection systems.

So, in this regard, monitoring and registration behaviors could be another area to explore. This would mean identifying indicators of malicious registrations that would trigger action from contracted parties, either at the time of registration or shortly after. This measure would be in line with recommendation number one of the DNS abuse small team report to the GNSO Council, which was issued back in October 2022. This would mean that all registrations that present a certain level of risk of malicious registration should undergo an identity verification.

Here we have examples of for proactive practices from the ccTLD space from Europe which entail the use of AI-powered DNS abuse detection systems another measure could be also periodic verification during the life cycle of a domain name. So this would mean checks when the domain is renewed or transferred. And with that, I would like to give the floor to Susan.

SUSAN CHALMERS

Thank you kindly, Janos. I'm just going to speak briefly to a third idea for a PDP that has been discussed by the GAC topic co-leads, which are reporting obligations. So, sound policy is built from evidence, relevant evidence for the GAC to consider when contributing to DNS abuse policy. And ICANN includes information from measurement platforms such as those provided by ICANN, Domain Metricon, the NetBeacon Institute provides measurement.

We can also look to reports from cybercrime research from firms like Interisle, we heard from today, the INFERMAL Report, which was widely discussed in Seattle during ICANN82, is also relevant evidence, ICANN Compliance produces monthly reports on DNS abuse, that is good evidence that can inform sound policy, and we have a good sense of how the contracted parties are implementing the 2024 DNS abuse obligations from compliance reports.

But we don't have a full picture. There are no requirements for the contracted parties to themselves publicly report on their DNS abuse mitigation activity or their implementation of the amendment. So one idea. Therefore, it could be focused on abuse

statistics reporting for the contracted parties. So that is just another suggestion to add to the collection of ideas that we've heard about yesterday and today.

Next slide, please. So, these are the next steps and the avenues for policy action at ICANN. If you attended the pre-ICANN83 webinar that we put together, we heard from the GNSO small team on DNS abuse. That small team is underway. Their assignment is essentially to evaluate DNS abuse mitigation efforts to date and to determine whether further policy work is needed. The draft findings and recommendations are due by September this year with a final report by October.

Now, we understand that this timeline could possibly be shortened, but I won't certainly won't speak for the small team on DNS abuse today. But I just want for GAC reps to be aware that this work is ongoing at the GNSO. We have a bilateral with the Board today and if I may ask support staff to flip to the question that we have proposed to them. So we will discuss this with the Board. I think if you turn to anybody at ICANN, any colleague, it's more likely than not that folks will agree that PDPs should proceed on a shorter timeline. Some PDPs take years.

I think the question here that we will put to the Board is how, and this isn't specific to DNS abuse, but how can we prompt a step change in PDP processes so we're seeing results delivered quickly? Not 10 years, not five years, not three years, how about 12 months

or less? So this is something that I would encourage GAC representatives to pay attention to this afternoon. Thanks.

If we could flip back. Now, many GAC reps are familiar with how GAC representatives can participate in and help to effectuate policy change at ICANN. For those who are new, I thought I would just very briefly go over some of these avenues. The first are the policy development processes, that's really what we have been focused on today. The multi-stakeholder policy development processes at ICANN involve the broad participation of stakeholders from across the ICANN community, including GAC representatives.

PDPs result in consensus policy. Consensus policy becomes part of the contract and is therefore binding across the parties. The next avenue for policy change at ICANN can be contract amendments. So policy can be put in place via amendments to the contracts between ICANN and registries and ICANN and the registrars, but unlike the multi-stakeholder policy development process, amendments are negotiated on a bilateral basis.

So we had a suite of landmark 2024 DNS abuse amendments that were put into place. They went into force on April 5th last year, I believe. And those established foundational obligations for ICANN registries and registrars, but they were the result largely of bilateral negotiations. There was a public comment process on the proposed amendments, but unlike PDPs, stakeholders who are neither ICANN nor the contracted parties are not directly involved in the process.

And as for GAC representatives, of course, our primary tool is GAC advice and it is our ability to produce consensus advice to the ICANN Board. GAC advice, when well considered and coordinated is the GAC's most powerful tool in effectuating policy change at ICANN. So I just wanted to provide that short overview, especially for new GAC representatives. Next slide, please. And so i believe we have 15 minutes left. Okay, good. We wanted to be able to save time for GAC discussion.

So the chair issued, as he normally does, a call for issues before the ICANN83 meeting. And the GAC DNS abuse topic co-leads provided some text to the GAC list in advance of the meeting. Now here, I've just highlighted the headlines that we provided. So for issues of importance, that's where we can discuss what goes on during the meeting pertaining to DNS abuse and particularly during the session.

We've suggested focusing on reviewing the landscape of DNS abuse and mitigation topics for PDPs and next steps. We also suggested encouraging targeted, narrowly scoped PDPs that deliver consensus outcomes on a much faster timeline. And so we wanted to sensitize this with GAC representatives, put this in front of colleagues, and open the floor for discussion.

NICO CABALLERO Thank you very much for that, USA. If we can go back, please, to slide number 12, the last slide. Yeah, right there. No. There. So as regarding the policy development, and before I give the floor to

Indonesia, sorry to keep you waiting, or is that an old hand, Ashwin? Is that an old hand? Your hand is up. So before I give you the floor and before we actually open the floor for questions or comments, one very important thing to take into account is the PDP, that is the policy development process participation for GAC members.

We want to make sure that you feel comfortable, that you have the chance to participate in a, I would say, meaningful way, that you feel comfortable, that the chairing of those sessions, the point being… what would be the point in participating in a PDP process if you don't have the chance to speak your mind, to say whatever you might need to say if, for example, and this is just an example, I'm not saying it is happening, but if the chairing is not that, I would say, efficient, your ideas cannot be conveyed, the floor is given to somebody else before any kind of issue you might have during those PDPs.

The idea is to make sure, again, as I said at the beginning, that you're comfortable participating in those PDPs. And of course, I totally agree with what the U.S. has already mentioned in terms of having shorter, faster, and way more efficient PDPs. We can't spend, from a governmental perspective, two, three years, four years, or even, I would say more than one year, it doesn't make much sense. I don't need to explain the cycles in which governments work.

Some countries have presidential terms for four years. Normally, our ICT ministers or foreign affairs ministers are in their positions for two years, three years, one year. It depends, of course, on the country, but you see what the point is, right? So again, sorry to keep you waiting, Indonesia, the floor is yours.

ASHWIN SASONGKO SASTROSUBROTO: Sorry. Thanks, Nico. Actually, my question is also the same as my last question to our friend from Czech, about the ISO IEC standard 27001, whether it is strong enough for preventing DNS abuse or what is your experience with this? Now, I'm asking this because, one, DNS abuse is a big problem in Indonesia, that's a very big problem today.

And secondly, Indonesia, of course, and other countries are also members of ISO IEC. And third, ISO IEC has a joint committee one, which looks after ICT, and subcommittee 27, especially look onto cyber security. So my proposal is that if the 27,000 standard is not enough for DNS abuse, then we must tell the ISO IEC organizations, we will have the general meeting next September, and we'll tell them, look, why don't you review the 27,000 one?

Because there, they also have the so-called PDP DECO policy development there. And one of the policy developments is to use the 27,000 certification systems to protect our system. Now, if from the experience at ICANN, it is not enough, then we will tell them and review it or whatever we can discuss with them. Even, Nico, you

can even send a letter to IEC. It is not a problem, of course. Thank you.

NICO CABALLERO Thank you, Indonesia. Well noted. I have India next.

SUSHIL PAL Thank you, Chair, and thank you to the panelists, especially the Interisle and the NetBeacon for the informative report. And we are more than happy and very supportive of this shorter and narrowly scoped PDPs. However, I still think that we are focusing more on the symptoms rather than the cause. We are looking at the correlation between the bulk generation, the cheaper cost, the ease of access, without the malicious domain name use, and these are, to my understanding, they are just the symptoms and not the cause.

I think the cause lies actually in the accuracy of the WHOIS data and as well as the identification. I would like to respond to maybe the panelists on this issue, because I'm just drawing a parallel from our physical world. I think we live in our physical world, but we definitely know who lives in our neighborhood, right? And I still think that these malicious domain names, they arise only because of the anonymity.

There is no accountability on the part of the malicious domain registrants, which actually gives them a free hand to get away at any point in time. All that we can do is to take down that domain

name, nothing beyond that, right? So drawing this parallel, I don't think increasing the $2 cost to $10 or $20 will actually going to reduce the number of malicious domain names because the benefits of benefits are too large as we saw roughly about $18,000 per minute.

So in our view there is a need for us to bring in accountability, not only in the part of registrars but also on the part of the registrants as well. And at the same time, it will be additional cost to the registrars and registrants, both but then I think we should be looking for that solution. Thank you.

NICO CABALLERO

Thank you for that India. We have seven minutes and one, two, three, four, five, six, seven, seven speakers. So I would kindly, kindly, kindly ask you to be brief and straight to the point. Susan, is there anything you would like to say before the -- No? All right. So let me give the floor to the European Commission. Please go ahead.

GEMMA CAROLILLO

Thank you very much, Nico. Gemma Carolillo here for the European Commission. Thank you for the colleagues from the GAC who organized this very informative session for our guest speakers. I would like to refer to what is asked in terms of communique consideration and possible way forward. So from our point of view, it's really good to see that there is this momentum.

A lot of parts of the community seems to be interested in moving forward on DNS abuse after the contract amendments, which we assess very, very positively. We have seen from the contracted parties' house, from the initiatives like the one from NetBeacon, we are hearing now. results from studies from Interisles, there is a lot of momentum.

So I think we should definitely take it and collaborate with the other parts of the communities. Considering the priority for the GAC has been always to get to some new measures before the new round, we should also be pragmatic and seek to identify achievable measures within the time frame that we are given. This means prioritizing while not just forgetting the broad picture but just seek to prioritize.

And from this point of view, we think it's important that we consider the possibility of an advice concerning targeted narrowly scoped PDP, but we would suggest for GAC considerations also that we identify these priority topics. We have heard today the possibility of combining some proactive measures like the monitoring of the patterns of behavior for registration data and the bulk registrations.

We have seen that there are a few proposals on the table that we think should be explored, and also we think it's important to consider the transparency obligations. This was part also of the GAC very early position when there was the public comment on DNS abuse contract amendments. Thank you.

NICO CABALLERO Thank you so much for that, European Commission. I couldn't agree more with you. And by the way, we'll have six communique drafting sessions, so we'll have more than enough time to discuss that. I have Canada, Netherlands, Switzerland, and Denmark. Canada, please.

IAN SHELDON Thanks, Nico. And thank you to all the presenters, this has been really, really interesting. And I'll be brief just because I know that there's a big queue in the Zoom room. But thank you again, Graeme especially, thank you for the NetBeacon report. I do like your point about not letting sort of progress or perfection stand in the way of progress and we see momentum here.

And I think it's really important to consider narrowly scoped, well-defined PDPs for timely outcomes. So just to urge GAC members to take a read of the NetBeacon report. It's very well crafted, it's a policy discussion, it's not overly technical, and there's lots of really good suggestions there. But again, thank you so much, and certainly looking forward to future discussions in the GAC around how can we move forward with these PDPs. Thanks.

NICO CABALLERO Thank you, Canada. Netherlands.

MARCO HOGEWONING

Thank you. It's Marco from the Netherlands speaking for the record. And I'll join the other speakers in thanking you for this very informative session. I think as my Canadian colleague just said, we have to consider perfect is the enemy of good enough.

And as my EU colleague already alluded, I think it's time to start narrowing down some of the options, and I hope that in the next reminding to all of us, together with the GNSO and the Board, we can actually find some consensus or one or two topics to take forward in the period up to the next meeting. Thank you.

NICO CABALLERO

Thank you, Netherlands. Switzerland.

JORGE CANCIO

Thank you, Nico. Jorge Cancio, Switzerland, for the record. Yeah, let me join the previous speakers, I think it's important to see what we discuss with the GNSO and with the Board, in what direction it goes. But I see definitely potential in this idea of targeted, narrowly scoped PDPs. And maybe just a slight correction to the optimistic assessment of Susan. I don't think there was ever a PDP that was below one year, but I stand to be corrected. Thank you.

NICO CABALLERO

Thank you so much, but let's hope we can change that. Thank you, Switzerland. I have Denmark next.

FINN PETERSEN

Thank you, Chair. Finn Petersen from Denmark for the record. And thank you for the presentation, much appreciated. We do concur that it should be narrow scope PDPs and we would like to see them before the next round embarked. So it should be quite early. What we will especially look for is proactive measures, I think the bulk registration has been one of them.

We would also like to see that the identity requirements or checks on contacting data and so on are more stringent than they are today. So that is what we will be looking at. Of course, there's other things, transparency, but if we should prioritize and have something before the next round, then it, for our view, should be focused on proactive measures.

And then this will only be another step on the way to Nirvana, or I don't know where we are going. One question to Interisle is bulk registration, do you in your study and consideration have defined what a bulk, where should the limit be? Should it be five registrations in a row? Thank you.

GRAEME BUNTON

Very quickly. Hi, this is Graeme from the NetBeacon Institute. Re-bulk registrations, I think you run into issues very quickly trying to define a specific limit on the number of domains available for purchase at any one time. Bad actors will just immediately go one under and automate it. It also impacts the marketplace in

interesting ways as when domains are revealed in a search result, you can add one two tend to a cart, and the number of domains that are available in that search result is going to be impacted by a limit like this. And so now we're really messing in the marketplace.

And so that's why I think that sort of approach is risky. And when we were thinking about how to address the issue of bulk registrations, especially as it was raised in INFERMAL, we thought two things. One, the access to APIs, which enable this sort of thing, build friction into accessing the tools rather than specify exactly how those tools are used, was going to be a more effective way of coming at it.

The second is that pivoting on the associated domain check, checking associated domains is going to disrupt campaigns. So that's a good reactive piece. But if a registrar has an obligation to go look at all of the domains in a customer account, there could be 10, 20, 30, 100, it's effectively a tax on a registrar, it costs them money to do that.

And they're going to therefore be incented to make more careful choices about who they let access large volumes of domains because they're now going to have an obligation to go look at them all. And we hope that, and that's why we put it in the paper, is that we think that is going to be impactful in the industry, it will encourage the right and incent the right behavior that we're looking for to address bulk registration issues. Thank you.

NICO CABALLERO

Thank you so much. And we need to wrap up. It's kind of like a blessing for our souls to see the broad consensus in this regard, given the international situation. Let me tell you that, consensus is not a very popular situation nowadays. So I see broad consensus regarding the approach to this communique consideration issue and the three topics under issues of importance, I'm not going to read the whole thing again, or advice. But for the closing, Susan, is there anything you would like to add in this regard, given the fact that you're the topic lead for the PSWG?

SUSAN CHALMERS

Well, thank you, Chair. Just very briefly, from the United States perspective, the timelines for PDP must be reduced significantly in order to achieve policy wins before the DNS expands as a result of the next round of new gTLDs. The last thing I will say is for the broader ICANN community. We have heard proposals from NetBeacon, the Contracted Parties House has produced proposals.

The Commercial Stakeholder Group has ideas. The At-Large Advisory Committee has ideas and policy priorities for DNS abuse. The Non-Commercial Stakeholder Group, which is committed to offering constructive input and policy advice, has priorities for DNS abuse policy. But we are all seeing that there's movement, we're heading in a shared direction, and the multi-stakeholder community at ICANN should work together towards DNS abuse to

provide a result. It's a very important time right now for ICANN to produce a policy result. So thank you so much.

NICO CABALLERO Thank you so much, USA. And that's all we have time for. Just a quick… and sorry for going over time, we'll have a coffee break now for 30 minutes. Right after that, we'll have a meeting with the GNSO and then with the ALAC, 45 minutes each of those meetings, and then a lunch break. Thank you so much. Enjoy your coffee.

[END OF TRANSCRIPTION]