ICANN87 Bali | AGM – GAC Discussion on DNS Abuse Mitigation
Tuesday, October 20, 2026 – 10:30 to 12:00 WITA

GULTEN TEPE

Welcome to the ICANN87 GAC Discussion on DNS Abuse Session on Tuesday, 28th of October at 10:30 local time. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior, ICANN Community Participant Code of Conduct, and the 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 and please remember to state your name for the record and the language you'll be speaking in case speaking a language other than English. And please speak at a reasonable pace to allow for accurate interpretation. I will now leave the floor over to Ian Sheldon, GAC vice-chair. Thank you.

IAN SHELDON

Thank you. Good morning. My name is Ian Sheldon, the Australian GAC representative and a current ICANN GAC vice-chair. Thank you for joining us for the GAC discussion on DNS Abuse Mitigation.

We have quite a packed agenda here today with quite a large number of speakers. We're joined by Gabe, Martina, Susan, Mitsuhide, and Ashwin from the GAC, as well as very impressive

***Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file but should not be treated as an authoritative record.***

lineup of guest speakers, Ery, Tatsuo, Leticia, Sam, Rafik, Eunice, Bruce, and Rod. Because we have quite a large number of speakers, just flagging that we will have a seating switch up halfway through this session, but without further ado, I might give the floor to my colleague, Mitsuhide Sakamoto to give an introduction. Thank you.

MITSUHIDE SAKAMOTO Thank you, Chairs. I am Sakamoto Mitsuhide from Ministry of Internal Affairs and Communications Japan, and I am serving as one of the co-leaders for this meeting, together with Gabrielle and Suzanne from the US, and Martina from the European Commission. Allow me to start the introduction.

So, bullet one, DNS Abuse Mitigation is a priority issue for the GAC. Policy development regarding the prevention and mitigation of DNS Abuse has been increasingly called for by various stakeholders in light of the expected expansion of New gTLDs. Bullet two, the GAC 2025/2026 annual plan set out two approaches to GAC work on DNS Abuse, focusing on, number one, advancing ICANN policy work on DNS Abuse before further delegation of New gTLDs. And two, building the subject matter capacity of GAC members on DNS Abuse.

Bullet three, under the ICANN framework, scope of DNS Abuse is clearly and narrowly tailored. DNS Abuse means malware, botnet,

phishing, and spam, when spam is used as delivery mechanism for any of four other type of DNS Abuse.

Bullet four, gTLD registries and registrars are contractually required to respond to report of DNS Abuse. ICANN Compliance audits and enforces these contract requirements. ICANN Compliance update on DNS Abuse will be provided in this session. Next slide, please.

This slide provides an overview of recent ICANN's major initiatives to address DNS Abuse. Bullet one, ICANN83, in June 2025, GAC issues consensus advice to ICANN Board in the GAC Prague Communiqué. It says to urge the GNSO Council to undertake all necessary preparation prior to ICANN84 towards starting targeted and narrowly scoped Policy Development Process, PDPs, on DNS Abuse issues, prioritize bulk registration of malicious domain names. And the responsibility of registrars to investigate domains associated with registrant accounts that are the subject of actionable reports of DNS Abuse.

Bullet two, December 2025, Final Issue Report on a Policy Development Process on DNS Abuse Mitigation was issued. The Final Issue Report suggests associated domain checks and unrestricted API access for new customers should be prioritized for policy development. Regarding associated domain checks, the report says, currently when a registrar found that one domain is malicious, there’s no contractual requirement that the registrar

must investigate whether the same registrant or account has other active domains that are also being used for similar abuse.

Regarding unrestricted APIs access for new customers, the report says, many registrants offer API or batch registration portals according to studies such as informal study. Insufficient gating or affliction for new users to access these batch registration tools can be due to proliferation of DNS Abuse.

Bullet three, PDP1 Associate Domain Check started in March 2026. In January 2026, GNSO adopts PDP Charter for an associated domain check. This PDP seek to create an obligation for registrar to investigate other domain associated with a customer account or a registrant where at least one domain that registrant is found to be engaged in DNS Abuse.

GNSO has published its initial report on 18th August 2026 for public comments. GAC comments were submitted on 28 September this year. PDP2 Safeguards for API access to new customers. PDP2 is currently being chartered by GNSO drafting team. The GAC small group on DNS Abuse provided GAC input on the PDP2 Charter on 25 September. So, I stop here. If there is anything to add, it's okay. So, let's move on to the next agenda.

So, we have four expert presentations. Because of interest of time, I'd like to open the floor for two questions at maximum for each presentation. First, I would like to invite Ashwin Sastrosubroto and

Ery Punta Hendraswara present on, Keeping Indonesia's DNS Secure and Trusted. You have 15 minutes and the floor is yours.

ASHWIN SASONGKO SASTROSUBROTO: Thank you, Chair. My name is Ashwin from the GAC Indonesia member and my college, Ery, from the Indonesian ID Registry. Next, please.

I would like to share with all of you our basic policy and then our data for DNS Abuse. Then Ery will give how we mitigate, we handle the problem that we have, the DNS Abuse here in Indonesia. First of all, based on the Indonesian Act on Electronic Information and Transaction, DNS Abuse is considered as a criminal activity, so it is not allowed. And our law enforcement will do whatever they can to mitigate, to handle this criminal action.

The MCDA worked together with the BSSN, this is the National Cyber and Crypto Agency, and also the Indonesian National Police. We worked together to make sure that DNS Abuse can be minimized. And we also worked closely, the government, worked closely with PANDI Indonesian, the ID registry to minimize the DNS Abuse and to mitigate whatever problem we have. And this is important I think because with the New gTLD where Indonesia also apply for several New gTLDs, we are sure that the problem will also increase and we have to be ready for that. Next, please.

Now, as mentioned before, DNS Abuse by ICANN definition is that one, phishing, malware, botnet, farming, and spam. And this is

interesting because in Indonesia DNS Abuse using malware, phishing, farming, and so on, most likely the problem is with online gambling, where in Indonesia gambling is illegal. You have also illegal content, that's in Indonesia like pornographic, gambling, and so on and so on and brand impersonation and compromise site. But the big problem, as you will see later, is the online gambling. Next.

This is the organization that looks after the DNS Abuse in Indonesia, the Komdigi is the MCDA, Ministry of Communication and Digital Affairs. We have the Indonesian National Police and BSSN, the cybersecurity coordination for the whole country. And, of course, PANDI, the ID registry and their partners. I don't know how many registrars they have. Next.

Then, this is some data that we could like to share with you. From 25-26, we have financial scam report of 700 to 1,000 and so on. Traffic anomalies, 5,000 and so. Gambling-related fund turnover, this is interesting, 4.84 billion US dollar. Oh, a lot of money. Next.

We have outcomes monitored by the ministry. We have 13 million content blocking actions, so when we get the information, whether from our crawling machine or from the people, then we block that particular content, that particular website, and so on. Recently from 2024 to 2026, we handle 5 million or so content handling actions. Next.

Now, this is website content enforcement. We have around 9 million to 2026 is 10 years. We have about 9, well 10 million website

content actions. We have online gambling of 7.8 million, pornography of 2 million and so on. That is the content which cause a lot of problem in Indonesia. Next.

Now, we also take care about the social media because there are many people using that. We have, well, from X, Meta, file sharing and so on, we have 3 million or so between 2016 to 2026. Next. Some of the recent enforcement by the category -- By the way, Komdigi is Indonesian name of the MCDA, Kementerian Komunikasi dan Digital, Ministry of Communication and Digital Affairs. Website social media from 2024 to 2020 is about 5.2 million. Online gambling now. You can see that online gambling had the top problem, 4.1 million. Pornography is less than a million, then fraud slightly below 60,000. Next.

This is recent social media enforcement from the last two years, 2024 to 2026, has 754,000. You can see the social media that get us those problem. Next. Now, website versus social media actions. Website action is from October 2024 to September 2036 we have 4.5 million website actions. Now, we call it actions, we close it or we call them and ask them to follow the Indonesian regulation, for example.

And happily for us, most of the websites, social media and so on, when we invited them to ask them, “Look, you are working in Indonesia, we would like you to follow our legal activities here,” normally they also follow. So, it is kind of, what to call it, government to business relation. And social platform action, you

can see 750, combined total we have around more than 5.2 million. Next.

Now, from natural monitoring to global coordination, perhaps it is important also that we have natural problem, we have the evidence, then we have to have more global coordination. Now, bearing in mind that in 2013, Indonesia hosted IGF-8 here in Bali. Not the same place, but in front of this place, the other conference. And the topic for that meeting is about cyber ethics. In the light that there is no international regulation and internet content, then we use the cyber ethics approach. So next is my colleague, Ery Punta will give more information for this.

ERY PUNTA HENDRASWARA Okay. Thank you. Ery Punta from .id, PANDI Registry. So, I still have only like two minutes, but I'm trying to share on what we do right now. So, of course, when we talk about the DNS Abuse, in Indonesia it's a bit different with how ICANN define the DNS Abuse because DNS Abuse is beyond the DNS itself. Right now, we have like four big issues like phishing, farming, online scam and also compromise side. Of course, when we talk about the compromise side, it's something that we need to do beyond the DNS itself. So, next.

Okay, so what do we do on handling and tackling these DNS Abuse issues? So, first we provide the IDADX. This is the collaborative platform on fighting the DNS Abuse. And then we also invent the monitoring system, we call it BIMA. BIMA stands for the bridge

identification and also the monitoring assistance. So, this is the crawler that patrols and checks which URL, which domain are actually abused or not.

So, how it works, first, it's from the data and report and also coming from the BIMA and also coming from another institution like police and also the MCDA. And then we do the IDADX analysis and then doing the check on that with the BIMA and then we do the coordination. Some of the action, we can do it by ourselves, but some of them we need to do a coordination. Like maybe if related with the content piracy, we don't have eligibility on tackling down, but we will work with other departments, other government authorities handling that. So again, like Ashwin mentioned before, that one of the biggest problem that we have is in online gambling. Second one is phishing and then third one is malware. Okay, next.

So, this is the scale. And we also found out that now increase of the use of the WAF proxy, so many actually are providing a WAF filter, WAF proxy. So, a lot of actually content reside behind the WAF proxy name servers. So, I think we need to discuss on this because sometimes we cannot directly identify, but we can only suspect that this actually abusive domain, but somehow is protected by the WAF proxy name servers. Okay, next.

So, how the evidence verification, the bottleneck that we have, of course, we try to do the detections and then flagging. Because of the number of the suspected from the scan is quite big, so we need to have the system on doing the detections. And then second one

is actually, from the board, it's like how we can do the challenging that this is actually real or abuse or not, like detecting the false positive on that. And then we also have the problem with the delay. Sometimes the verification and evidence is sometimes using or coming from other problem.

We have one of the use cases saying that we have a request to take down the domain because of the content piracy. But when we ask for the evidence, sometimes we have to wait and a lot of process on doing the verification on that. So, these are the numbers that 60% are through the WAF proxy, and then 1,000 actually is institutional ID that also using the WAF proxy in this method. Okay, next.

And actually, how the WAF proxy work, first, the request coming and filtered by the web application firewall, and then the original server are protected by the firewall. From the customer side, maybe they think that they need to protect, but from the authorities asking that actually if the site are actually content having an abuse there, somehow the web application firewall is filtering and trying to protect the illegal content. So, that's the thing that happens in this matter. But other than that, of course, the security is also important, but the other things also increase another problem. Okay, next.

MITSUHIDE SAKAMOTO: Ery, so could you kindly wrap up the presentation? Thank you. Within one minute.

ERY PUNTA HENDRASWARA: Okay. So, this is the thing that actually we propose, that the idea is, how we can have the access from the WAP proxy that we can verify than giving the crawler access to do the verifications on the abusive side. And then, of course, we can do and fight this problem together so we are not against the WAP filter services by some of the cloud services that deliver. But if we can have a collaboration together, we can fight the problem together. Okay, next.

So, of course, it's DNSSEC and ISO. Next. And then I think we can discuss later on. Of course, the regulation is foundation, but enforcement is always hard if we're doing alone. Next. Next, please. Okay. So, I think that concludes our presentation, but last but not least, maybe Pak Ashwin, please.

ASHWIN SASONGKO SASTROSUBROTO: Thank you, Pak Ery Punta. Just small additional information. Tonight we will have the GAC Dinner, and the bus will leave here at 5:30 and arrive at the Taman Bhagawan at 6:20. We will start the dinner at 7:00 until 9:00. At 8:30 p.m., the bus will leave the area, coming back here and arrive here about 9 o'clock. And we invite all of you, that's all.

ERY PUNTA HENDRASWARA: And just to add, the place is very beautiful, I guess all of you should come and join the dinner tonight. And we provide the very nice, very tasty dinner. Thank you.

MITSUHIDE SAKAMOTO: So, thank you very much Indonesian colleagues and your inputs and their hospitality. So, I'd like to move on to the next session. I'd like to invite Ninoseki Tatsuo from Japan Publishers' Manga Anti-Piracy Conference or JPMAC present on Domain Hopping and Registration Data Verification. You have 15 minutes and the floor is yours. Thank you.

TATSUO NINOSEKI: Thank you very much for giving JPMAC the opportunity to speak today. ICANN's definition of DNS Abuse doesn't include copyright infringement. This is also true for the piracy JPMAC works against. However, piracy is different from copyright infringement in general. I will explain this point later. In this presentation, JPMAC will report on what we call domain hopping. Next slide, please.

Let me begin with the key points of this presentation. JPMAC works against online manga piracy. People who act illegally hide their identity to escape enforcement. This is true for piracy and also for DNS Abuse. In phishing, one type of DNS Abuse, domains are often used once and then abandoned. Piracy sites are different. They earn money from advertising, so they normally want to keep the

same domain, but they change domains at short intervals, we call this domain hopping.

We track the same operators over long periods, so we can see how one operator moves from domain to domain. This view may be useful for the work on DNS Abuse. One reason for hopping is that domains are easy to register even with forced data. Registration data verification needs to be improved. Next slide, please.

First, let me briefly introduce JPMAC and explain the serious damage from manga piracy. JPMAC consists of five major Japanese publishers together with lawyers. By the way, I'm one of the lawyers. Piracy sites offer a large number of manga titles for free and make money from advertisements. A government study by PwC covered four areas, video, music, games, and publishing. Parasite losses in these areas are about the same as the overseas sales of Japanese content.

Operators hide their identity and keep hopping, so injunctions and the legal actions are very difficult. Manga artists and the people doing anti-parasite work are overvalued. Honest manga fans who want to support the artists are angry about this situation. Next slide, please.

Let me explain the point I mentioned at the beginning, JPMAC's focus. It is often said that the scope of copyright infringement differs by jurisdiction. This may be true. However, JPMAC is concerned with commercial scale piracy, meaning unauthorized exact copies, not copyright infringement in general. Under the

TRIPS Agreement, 166 WTO members are required to provide criminal penalties for such piracy. So, this kind of piracy is commonly treated as a crime.

The left image is the official Japanese version, and the right image is a pirated version that copies the official English translation. To attract users, operators often translate new Japanese chapters themselves and post them before the official English version comes out. Once the official version comes out, they sometimes replace their own version with it. This image shows such a case. As you can see, the artwork is identical, so copies are easy to identify, regardless of language. This kind of piracy harms right-holders, first and foremost manga artists. And next slide, please.

Next slide, please. For publishing alone, which is mainly manga, piracy losses are estimated at about 17 billion US dollars. This is a conservative estimate because it counts only about one third of what was read. This one third is the share of people who said they were willing to pay. The right side shows visits to English translation piracy sites. The top site alone had about 290 million visits per month. Next slide, please.

JBMAC first noticed domain hopping in early 2020. As the slide shows, operators seem to change domains for two reasons. First, when traffic is spread across several domains, each domain looks smaller so it draws less attention from rights holders. Second, hopping makes it easier to escape enforcement. The early example on the slide shows the first reason. Domain A came back again and

again, and users were sent sometimes to B, sometimes to C. So, total traffic stayed the same, but it was spread across domains, and each domain looked smaller. As listed on the slide, hopping also takes various patterns. Next slide, please.

Recently, the intervals between hops have become shorter. Since fall 2022, certain piracy sites have been removed from Google search results, and operators seem to hop to another domain to stay in search results. From November 2024 to September 2026, JPMAC observed over 450 redirects. Of these, about 82% moved to the next domain within 15 days. 15 days is a verification period now under discussion at ICANN, as I understand.

Early on, operators hopped without any action from us. Recently, many hops seem to be partly a reaction to our countermeasures. We welcome the efforts to shorten the verification period. At the same time, the main cause is weak verification. So, stronger verification is also needed to reduce hopping. We now often see old domains redirected to the current domain. One click, please. Yeah.

When rights holders act against the current domain, the operator moves to a new one and redirects all older domains to a new domain at once. So, the site continues basically without losing users. We understand that associated domain checks are under discussion at ICANN. We have only a general understanding of that work, but we welcome measures that can also deal with cases like

this. The table on the right shows that many different TLDs are used including both gTLDs and ccTLDs. Next slide, please.

This slide shows how domain hopping looks for stakeholders, site operators, users, rights holders and registrars. Because of time I will briefly mention only the registrar's. Registrar sees only the domains registered with it. So, a new domain may look like an unrelated registration even when the same operator is behind it, and when an operator returns to an old domain, there is no new registration so no new verification takes place. Next slide, please.

Why does hopping happen? For operators, escaping rights holders' countermeasures is worse than keeping one domain. One factor is that, domains can be registered cheaply and easily, even with false data. The lower part of the slide shows actual registrations with false data. On the left, David Beckham is entered not only as a name, but also as a street address. The phone numbers are obviously made up. These are real cases. These are not inadvertent errors. The operators know that even obviously fake data like this gets through, and they are gaming the system.

When the data is clearly false, we report it to the registrar right away. Usually, the registrar contacts the operator and the operator replaces the data with entries that look fine, sometimes in a completely different country. To check the new data, we send a letter to the registered address. If the letter comes back, we report that to the registrar. Some registrars still take no action. They say

a returned letter alone does not show that the data is inaccurate. Next slide, please.

As the ICANN79 survey of 15 registrars shows, verification practices differ among registrars. Some registrars spend money on verification and others do not. This means that registrars that act against bad actors and pay for verification are put at a competitive disadvantage. Setting a common minimum level of verification for all registrars can make competition fair. In the EU, as you know, NIS2 Article 28 also requires verification. Next slide, please.

Piracy sites rely on domain names and also on hosting, CDNs, and advertising. The intermediaries have no global governance system and the rules vary by country. Only domain names have a common global system coordinated by ICANN. For this reason, we have high expectations for ICANN. Next slide, please. This is my last slide.

We support a two-step approach. Technical verification team in Japan suggested a similar approach in ICANN's public comment in 2023. Step one is stronger verification at registration. Today verification mainly checks the email address, but anyone can obtain an email address easily. Step two is stricter verification, including the postal address, only when a registrar receives a notice of infringement or abuse with evidence. Here is an example of such evidence.

First, the address or other date looks impossible. Second, after the registrar was contacted, the data was changed, but it still looks suspicious, or a notice sent to the new address didn't arrive. Third,

the domain has been used for illegal activity, such as piracy. The third point is not direct evidence that the data is inaccurate, but some of these facts together are an appropriate trigger for stricter verification. With two steps, we can avoid too much burden on ordinary registrants and registrars.

We also need to keep in mind that in countries with low press of freedom, domain names can be an important place for free speech. And overly strict verification could limit access to the Internet. One more point. The ICANN79 survey mentioned earlier had only 15 responses. So, a broader study on register verification can also help.

We understand that ICANN is a leading example of the multi-stakeholder model. As an organization from the content sector, JPMAC appreciates this opportunity to speak. Thank you very much.

MITSUHIDE SAKAMOTO: So, thank you very much. So, now I'd like to open the floor for only one question, if any. I see none, so let's move on to the next presentation. So, I'd like to invite Leticia from ICANN Contractors Compliance on ICANN compliance update. You have five minutes. The floor is yours.

LETICIA CASTILLO: Thank you. Hi, everyone. My name is Leticia Castillo. I'm with ICANN Contractors Compliance. Next slide, please. The DNS Abuse

Mitigation requirements became effective in April of 2024. Throughout this August, ICANN Compliance has initiated over 650 investigations into compliance with this specific requirements. Of the more than 570 resolved, about 66% resulted in action to stop the DNS Abuse for which the domain name was being used. Approximately 8% resulted in action to disrupt it, and in approximately 21% of the cases, the contracted party found no evidence of DNS Abuse and provided us with an explanation and evidence of the investigation.

We also issued eight notices of breach and terminated one registrar's accreditation, specifically for Baylor to meet the DNS Abuse Mitigation requirements. We completed one registry audit and we are wrapping up a registrar audit that is targeted at registrars with the highest concentration of reported DNS Abuse. Next slide, please.

The biggest impact of our enforcement work comes from addressing root causes, to change the behaviors, not just to address the individual case at hand. When we identified that the gaps in the registrars or registries processes that led to the non-compliance, we required the contractor party to develop and implement a remediation plan so that the root cause can be addressed and targeting for that not to happen again. The remediation can range from fixing an abuse contact that is not working, to completely overhauling the entire process to receive, investigate, and act on DNS abuse.

Between April 2024 and August 2026, more than 70 remediation plans were completed. We have some more on the way, and we track those. We track whether they are working. 87.5% of the remediation plans that have been completed within our cases today have not shown indicators of recurrence. And this light also links at the top two blocks. One explains our remediation approach in general and one provides an example of a remediation so you can see what it looks like in practice. Next slide, please.

And when remediation doesn't work, we escalate. Since April 2024, we issued eight formal notices of breach specifically related to DNS Abuse Mitigation requirements. There was a ninth notice of breach that related to a registrar failing to appropriately investigate reports involving thousands of domain names, allegedly linked to cryptocurrency scams, so not DNS Abuse. But as part of the remediation for that notice of breach, there was a complete overhaul of the abuse processes with impact in DNS Abuse as well.

And in August, we issued a notice of termination to a registrar that repeatedly failed to comply with the DNS Abuse Mitigation requirements. This registrar had implemented remediation plans, but continued to handle DNS Abuse reports in a manner that was not compliant with the requirements so we issue a termination notice. And this is an important point because submitting a remediation plan isn't enough. What matters is whether it leads to sustained compliance because ultimately our goal is not just to address individual cases, but changing behaviors and

strengthening processes and making sure that those improvements last.

And that was my last slide. For five minutes I think pretty condensed.

MITSUHIDE SAKAMOTO: So, thank you very much. Now I'll move on to the next presentation. I can invite Sam Cheadle from ICANN Office of the Chief Technical Officer, or OCTO on associated domain management. You have 10 minutes for your slides. The floor is yours.

SAM CHEADLE: Thank you very much. My name is Sam Cheadle. I'm from ICANN org. I'd like to talk to you today about one particular project that we've recently run related to associated domain detection. Next slide, please.

So, just to give you an overview of where our team sits within the wider org, I work in the security stability and resiliency team that's headed by Samaneh Tajalizadehkhoob and we are within the wider Office of the Chief Technology Officer. Next slide, please.

So, just to give a little bit of background on the areas that we're focusing on and definition of the terms, I think many people here will be aware of the ongoing PDP focused on associated domains. This is related to the concept of bulk registrations, often large numbers of domains registered close in time. Those can be

exploited by malicious actors for various abusive purposes, including phishing and malware distribution.

This is often facilitated by the use of APIs. There's a second PDP proposed and I believe underway in the near future looking at getting access to APIs. This is another motivation for the study linking in with the existence of bulk registrations, the existence of associated domains. We believe that the wider distribution of bulk registrations across the gTLD namespace is not particularly well understood due to data visibility issues and also definitional issues. It's difficult for people to agree on what we mean when we say bulk in terms of the volumes of domains. Next slide, please.

One key area that we were interested in exploring was the different possible source data sets. Lots of the current discussions, part of the ongoing PDP on associated domains focus on the use of internally held registrar data. That may include registrant contact details, account IDs, or payment information, for example. Those can be very useful for pivoting and associated domain analysis, but they're only held internally and they're private datasets.

So, we wanted to look at the possibility of running analysis on public data. Public data refers to the information that's accessible through standard RDAP or Whois queries such as registrar, name servers, and creation dates so rather limited. We're not talking about individual registrant contact details, but non-personal data. Next slide, please.

So, the main hypothesis was that we could take a public data set, what's accessible via RDAP only, and use that to construct high confidence associated groupings. So, clusters of domains we believe are related with a high likelihood to the same registrant.

One of the main goals was to develop a robust methodology. So, this kind of data has been used a lot in the past, lots of past research on reputation scoring and trying to pick out malicious infrastructure, but we were really focused here on the question of, could we construct these high-fidelity, high confidence associations between domain groups? And then, as a second goal, could that information actually be used by defenders, ICANN contracted parties to detect and possibly mitigate malicious activity as a form of proactive detection? Next slide, please.

Just to give a very high-level overview of the data that we consumed and the analysis we performed, we had reputation block lists, that's the feed data. Those are reported domains. They don't necessarily have actionable evidence associated with them, but they're reported malicious only. We combine that with domain registration data, as I mentioned. We have a centrally compiled source of equivalent RDAP data so that's thin registry data effectively. We also performed DNS lookups. We were looking at the underlying DNS infrastructure.

In terms of the analysis we performed, we've got three distinct types listed here. Batch registrations, where multiple domains are registered very close in time, associated with the same registration

properties or DNS infrastructure. Bulk registrations where those registrations can be spread out over a slightly wider time window, and bulk resolutions where we're not looking at the DNS registration properties, rather the underlying DNS infrastructure and the resolving IP addresses.

There's much more information on this in a recently published document, so I won't go into too much detail on the methods, but please, check our OCTO publication list for more method details. Next slide, please.

In terms of the results, we looked at the composition of our reputation block lists. We filtered those down to maliciously registered, and we found that over half of those maliciously registered RBL entries could be tagged as associated. So, that means they were registered with at least one other. We're not saying they were registered in a group of hundreds of thousands of domains, just that they were registered in a group. And that further work is required to investigate more the degree to which those are large bulk registrations, but many are consisting of a hundred or possibly over a thousand domains.

We found that this technique is also helpful for some cases for detecting the abusive activity earlier or at least giving us a signal of high-risk abuse. That was true in 5% of the cases. If we assume ideal data access conditions where we have rapid access to the necessary data, that could increase to 10%. We also found that the

techniques are capable of expanding known abuse block lists and finding at risk domains.

MITSUHIDE SAKAMOTO: You have one minute.

SAM CHEADLE: Okay. So, taking those results, what do we think would be useful for further community consideration? We would like to propose that some of these results could be distributed through our Domain Metrica platform. This may help facilitate the proposed AD checks currently being discussed in the PDP, and this will also be useful for monitoring long-term associated or bulk registration patterns. So, we have a lot of past historical data held within Domain Metrica.

There are of course issues with being transparent around the methods that we use, attackers may evade those, may bypass those, but we're not proposing a static Unchanging method. This is flexible. It doesn't need to be completely transparent, but we want to be open with the community and to try and establish a trusted agreed method that hopefully everyone is on board with.

And lastly, just a point to raise that associative evidence is different from actionable evidence of abuse or direct evidence of abuse, but whether there are cases where relevant parties can take action based on high-confidence associated evidence to known abuse, we think is an interesting question for discussion. Yeah, thank you very much.

MITSUHIDE SAKAMOTO: So, thank you very much. And time is flying, so please, join me in applause for all four presenters. Thank you very much.

IAN SHELDON: Thank you. As foreshadowed, we might have a quick seating change. So, can I please ask the panelists for the session after this one to join, and then I'll hand the floor to Martina and Gabe for our next immediate session.

MARTINA BARBERO: Thank you very much, Ian. And I know it's still early in the day, but we'll try to wake you up with some PDP discussion. So, if we can go to the next slide. Just a very short background from me before I hand it over to Gabe for more contents. But as you know, DNS Abuse, it's a very important topic for the GAC and one that has been covered in many communiqués. Most recently, an important communiqué was the Prague Communiqué in which we should advise to the board. And that has led to quite considerable developments based on this final issue report which followed and which identifies several policy gaps to address.

Two were prioritized, the one on associated domain checks. We just heard OCTO speaking about methodology for identifying associated domains. And the second one was about unrestricted access to APIs for bulk registration. So, in the next couple of

minutes, we will speak about those two PDPs, one which is ongoing and the second which is about to be launched.

But before we do that, I just want to reiterate my usual call for participation in the small group on DNS Abuse. I heard in the first session of the GAC this week that there are 96 new GAC members. So, we have a small group on DNS Abuse, which is very active. We meet very regularly and we prepare the position of the GAC for all the PDP discussion in that group.

So, if you have not joined the group and you wish to join, please let the GAC support colleagues know, and they will be happy to add you. And that's indeed our antechamber of negotiation. So, it's very important to have as many voices as possible there. And now I give the floor to my colleague, Gabe, who can walk you through the advances we made in PDP1.

GABRIEL ANDREWS Hi, y'all. So, this is Gabriel Andrews and I'm going to go through this quickly because we're behind on time. The status of the DNS Abuse is that, about two months ago, the Working Group published an initial report that included eight recommendations on things like what the triggers of a check should be and how it should be conducted. There was then an opportunity for public comment, and a lot of folks offered comment, the GAC is one of those groups that did, we were broadly supportive of the eight recommendations that came in this report. We had small wording changes, we suggested for a couple of them, but the high-level

point I'd like to make is that we're pleased with the majority of what we see. Let's go to the next.

Having had that comment come in now, the Working Group has at ICANN87 four meetings in which we're sort of breaking up those eight recommendations, looking at the first two in the first meeting, then the next, then the next. We're three quarters of the way done now. It's going fast. You may recall that the GAC wanted this PDP process to move swiftly. The Chair is ensuring that it is. That's a double-edged sword because it means that our review of public comment is also swift. That's okay, but it's something we need to really recognize that that's happening.

So, when Martina mentioned that there is opportunity to join the core group, the GAC small group on DNS Abuse, one of the opportunities then if you were to join is, once this public comment is reviewed, we're expecting revised recommendations to come out next month in November. And then and we will take those back to the small group and look at how all the public comment was integrated, and there's another opportunity then to share feedback thereafter. So, if you're interested, come join us.

The PDP will then move on to, gosh, what is the next step we're expecting in December? Yeah, December there will be a republication so it's going to go quick. The last point I think I'll make is that, there is an expectation from the GAC that we might have opportunities to talk about cross-registrar collaboration as a

future point of policy to follow this one. Let's go to the next slide. All right, Martina, back to you.

MARTINA BARBERO

Thank you, Gabe, and very quickly on PDP2, so the second PDP is on unrestricted access to API. It has not started yet, but the GNSO as we heard during the GNSO GAC bilateral is in the chartering process.

Now, the chartering process as GAC colleagues know is not something that is done collaboratively with the other communities. It's something that is in the end of the GNSO, but they have allowed us to provide a one-time input to this chartering process which we have done. So, again, we use the DNS Abuse small group to gather input from all GAC colleagues and we have provided some consideration for the chartering.

For the new GAC members, the chartering means that they are discussing the questions that then will go into the charter of the PDP so it's basically a scoping phase. So, it's important of course that the scoping is done correctly otherwise we will be let down by the results of the PDP. So, we provided some thoughts for the scoping, particularly as you see here, the need for the language to be technology neutral. We speak about APIs, but APIs are not the only way to register in bulk, so the GAC would value a broader approach to cover all the bulk methods that allow you to register domain names.

Also, there are conversation going on remedies for registrants, so this could be from the PDP in particular, but to be part of ampler conversation and a different PDP. And, of course, we need to look at the safeguards as well as the chain of liability with the registrar's resellers, et cetera, et cetera, et cetera. I will not spend too much time because with this is just a scoping exercise and because I want to make sure we have time for the discussion.

IAN SHELDON Thank you, Gabe and Martina. I might pause for a few seconds to see if there are any quick questions noting we can return to this in due course. I see no hands and -- India, please, very quickly.

SUSHIL PAL I have no question, just to kind of reiterate the submissions we have made on the PDP1 and PDP2. Is it the right time or we can come back later for this?

IAN SHELDON As you wish.

SUSHIL PAL Okay. So, with regard to the PDP1, first of all, let me compliment the Working Group which has been working on this. I mean, they're doing a great work. For the PDp1, we just want to make two quick points.

Number one, to support the cross-registrar's information sharing because that is what will actually go a great, long way in establishing the ADC misuse. The other one is regarding the Recommendation 3, which actually provides only for the reasonable investigation to be done by registrars. What we think because clearly, that makes it very subjective, and we understand that registrars have different resources. However, we should provide minimum baseline level of investigations which must be done by the registrants so that would give us some assurance that minimum level of baseline investigation has been done.

And on the PDP2, we have made comments regarding the identity part, identity check. For anyone who is seeking to have an API access for the bulk registration, we just want that they should be a part of the scoping charter. Thank you.

IAN SHELDON Okay, thank you for your comments. With that, perhaps I can give the floor to Susan to take us through our facilitated discussion with stakeholders. Thank you.

SUSAN CHALMERS Thank you, Chair. My name is Susan Chalmers, and I am the GAC representative for the United States. Before we jump into our community discussion, I just want to say that the United States strong strongly supports the ICANN community's concerted efforts to more effectively address the problem of DNS Abuse. And thank

you to all involved in PDP1 for your work to develop a policy on associated domain checks.

So, for the second part of our session, we have representatives from the community joining us today to share their perspectives on PDP1 and particularly on the last mile to finalizing the policy. And whether there are any remaining hurdles in particular that you believe we need to overcome to get there. And after we discuss PDP1, we'll hear from our colleagues on PDP2, the chartering effort for which is currently underway as recently explained by my colleague, Martina. So, let's just dive right in.

The first question is on the screen there. What major hurdles does your constituency see on the way to agreeing to an effective set of policy recommendations for PDP1? I'd like to take answers to all of these questions first, and then we'll discuss, and then we'll move on to the second question. So, let's begin with the NCSG. Rafik.

RAFIK DAMAK

Thanks, Susan. This is Rafik Damak from NCSG. I am speaking here as the NCSG Chair. For the first question, it might be helpful to frame it as, other than speaking about hurdle, but area that might require deeper discussion within and beyond the Working Group. So, this is what we would like to share.

So, in terms of area, three of them come to our mind. First, it's about the definition of reasonable investigation. Second, it's about separating clearly out the steps on ADC. And finally, about the

registrant recourse and remedy. With regard to reasonable investigation, so the first question is, what's the scope of reasonable investigation? What should be the baseline requirement for registrar to review to be considered in compliance with the policy? And from NCSG view, I would like to focus on information reasonably available to the registrar, but we can, of course, look beyond, but they are not required to request to generate new data. And also, that investigation should be reasonable and the keyword for us, proportionate.

For separating out the steps of an ADC, one risk that we would like to flag is that registrar in conducting an ADC will jump automatically from identification of associated domains to medication. And so, for that, from our standpoint, the policy should clarify that these are separate steps. First, identifying potentially as you say domains. Second, investigating whether those domains are actually being used for DNS Abuse. And the key point here is that, as you say, does not in and of itself establish abuse. And third, deciding whether mitigation against a particular domain is justified.

So, when a mitigation is being debated, the registrar should make a separate evidence-based assessment concerning that domain, and if there are legitimate reasons for the domain to be associated, even if one is abusive.

Moving to the last area which is quite important for us and we raised it several times in several venues, which is about resistant

recourse and remedy. The Working Group deliberated whether recourse and remedy of when medication based on the finding of ADC lead to adverse impact such as an erroneous or disproportionate response. And there have to be a means of disputing and requesting a recourse in such situation.

We appreciate that it led to a productive discussion within the Working Group and also to have this broader discussion on options within ICANN to establish a minimum baseline for registrant recourse and immunity, which could then go beyond that. So, this is what we would like to share from NCSG and we're happy to clarify. Thanks.

SUSAN CHALMERS: Thank you, Rafik. We do have 18 minutes left, so we're running a bit short of time, and we did want to set aside some time for discussion on the communiqué, so I'm just going to encourage our colleagues to keep it to the high points. So, next let's turn to Eunice from ALAC. Eunice?

EUNICE ALEJANDRA PÉREZ COELLO: Thank you. This is Eunice from ALAC. I appreciate the opportunity to share the perspective of At-Large Advisory Committee. We believe that when a domain is identified and used for any abusive intent, registrar should not limit the investigation to the single domain.

For ALAC, the main challenge is reaching recommendations that lead to effective investigation, consistent implementation, and verified compliance. We see for many hurdles. The first is clarity about when an ADC should be initiated. ALAC supports making an ADC mandatory when there is action of evidence of DNA Abuse. Action of evidence will mean information that is sufficiently specific and reliable to justify an investigation under existing contractual obligations.

During this PDP1, different interpretations emerging concerning, present or intermittent abuse and the distinction between maliciously registered domains and legitimate domains compromised by clear parties. PDP1 excludes compromised domains from these specific ADC requirements. However, that exclusion must not be interpreted as removing existing contractual obligations to investigate and responding to this abuse.

The second hurdle is agreeing of what constitutes a reasonable prompt and verifying investigation. We need a consistent minimum and standard even though the registrar have different systems and capabilities. However, several indicator points to coordinate campaigns. The investigator should not stop prematurely. The investigation must be proportionate. This means the scope should match the available evidence, the seriousness of the abuse and the specific circumstances it must also be prompt.

A response that come too late may allow further harm for victims. Registered accountability must remain clear when whistleblowers are involved. For a lot, it is essential that ICANN Contractual Compliance can verify whether these obligations are being fulfilled. And the [inaudible - 01:11:47] is how we asset and present human rights impacts.

During this PDP we first conducted a scope impact assessment and later more comprehensive assessment. The human rights impact assessment examined potential impacts on the privacy, freedom of expression, freedom of association, non-discrimination at due process. The methodology considers different dimensions, like what means how likely harms it's to occur. Severity means how serious its consequence will be. And to assess severity, the methodology consider factors such as the intensity of the impact, the number of people potentially affected, and how difficult it would be to remedy the harm.

It also considers existing safeguards and the risks remain after those safeguards are applied. This is where we identify an important methodological concern. The initial report presents an overall conclusion of limit adverse impact. However, a low-risk rating does not necessarily mean that the consequences will be minor for every person affected. And if an incorrect mitigation decision is subsequently taken, a service that many people rely on could be disrupted. That is why in its public comment a lack request that the human rights impact assessment so very clearly distinguish lack of severity safeguards and residual risks, and

correctly identified that they affected groups. The methodology used had been developed through work predating PDP1.

Our experience also showed why individual internet user perspectives should be considered when assessment questions are developed, not only when the conclusions are reviewed, but there is another equally important consideration. Failure to mitigate DNS Abuse also causes harm to people's rights. Victim of phishing or another kind of abuse may suffer financial losses, identity death, and violation of privacy. Therefore, we need to understand both the risk of incorrect policy implementation and the benefit of effective addressing DNS Abuse.

SUSAN CHALMERS: Thank you, Eunice. Eunice, I'm so sorry to interrupt. I'm just mindful the time and I want to give everybody a chance to speak. Also, let me compliment ALAC on that excellent slide. I think it really does kind of capture everything. Let's turn now to Bruce from the ccNSO and then Rod, if you could just follow right up after, with the SSAC contribution after Bruce has concluded. Please, Bruce, to you.

BRUCE TONKIN: Thank you. I'll just make a sort of introductory comment in that the ccNSO itself doesn't form a position on the GNSO's policy, but we do share our experiences and we generally do that through regular surveys of our members. And we've recently completed a survey

and had members representing about 65 country codes and one of the questions we asked is, do these country codes already conduct associate domain name checks? And it turns out that 20% of them do it regularly, 30% do it occasionally, and about 5% require registrars to take action.

It's also worth noting that in terms of the top 10 largest top-level domains in the world, five of them are country codes. And when you're looking at the larger country codes and you look at the top 10 registrars, they're generally the same. So, there's a lot of benefits in coming up with sort of common solutions to these problems.

I'd also comment in terms of the policy itself is to be wary of trying to get too detailed in the how and focus more on the outcome that you're trying to achieve, because this is an area of the people that are malicious actors conducting DNS Abuse respond very rapidly. And when you're doing associate domain checks and you find a bunch of names and you're using a particular method of finding that bunch of names, the next time they do a DNS Abuse, they'll do it differently so that they don't get those names taken down. So, it's constantly moving.

And one of the benefits of ICANN is that the country codes share information on what they are seeing and techniques that we use to combat things. Perhaps ICANN can be doing a bit more training perhaps for registrars and registries on things you can do, but it's continuous. Okay? You'd need to be doing it every year.

Finally, I just wanted to comment, there was a session yesterday on registrant recourse, and I think that's an important consideration as well, because the more you look for associate domains, you do make errors. And it is important that there's methods for registrants to get in touch with the registrar or the registry and ask for the case to be reviewed and an opportunity to potentially appeal the decision. So, that's probably enough for me.

ROD RASMUSSEN

Okay, I'll just jump right in as Susan had directed. I'm Rod Rasmussen from the SSAC. I'm kind of making a little change on the fly here because we didn't get the memo about the two questions. So, this deck is largely irrelevant, but I will take the first slide from it, thanks. And in the spirit of our late and dear friend Bertrand de La Chapelle, we have three points that I'd like to point. Next slide, please. And this will be the one slide I'll actually use.

Three takeaways. The SSAC in general supports the baseline as did most of the public comments by far. So, as far as hurdles go, it's really us getting the details worked out and making sure that the public comments are adequately covered. We will undoubtedly work that out within the PDP. The work has been progressing very collegiately, and we have made steady and rapid progress, as has been pointed out. Making too rapid a process is progress, which I've never said in an ICANN meeting. It may be a challenge just to make sure we're covering everything. However, I think we will get there.

Two areas where I think that will need to be carefully and thoroughly done, not just in the policy, but in the implementation of the other two points here, that's around the associations and how you do them. I've just posted into the chat a reference to SAC135, which we published concurrently with our public comments. That goes into great detail. I believe there's 29 different signals that could be used for associations. Each one is an independent one and certainly not a sufficient one in most cases, a combination of things on how that gets done.

I think OCTO has done some excellent work in this area as well, and being able to provide and make sure the implementation team is aware of these things and takes those into consideration so that they can disseminate that information to registrars is going to be key to making this thing successful. And has been pointed out, it needs to be flexible to change over time as malicious actors change their approaches in response to countermeasures.

And finally, the measurement of this is one area where we've naturally had some, I wouldn't say difficulty, but it's been a challenge to think of ways to measure effectiveness of a policy, especially when you don't have a counterfactual. In other words, if we change things, how do we know what would have happened otherwise?

So getting them and separating the, are people doing these things, which is fairly straightforward from, do these ADCs have an impact and what is that impact? So, I think there's still some work to do

there, but those are the only two areas I see as hurdles, but I don't think they're very high hurdles. It's more a matter of doing a good job. Thank you.

SUSAN CHALMERS: Thank you, Rod. Just a question to Martina and the Chair, should we move to the communiqué consideration or...?

IAN SHELDON: I think we probably have about three minutes for open discussion, and I want to leave two to quickly touch on the communiqué.

SUSAN CHALMERS: Okay, I don't know full, so PDP2 we might save that for another day. Okay, open discussion. Is there any feedback from our GAC representatives? Would anybody like to weigh in at this stage on PDP1?

SUSHIL PAL: Thank you. The short one, we would be supporting the SSAD concern on monitoring the effectiveness of the policy, and for that, it would be useful if there is a mandatory reporting of these abuses on the ADCs by the registrars, if that's also a part of it.

SUSAN CHALMERS: Thank you. Well, maybe I will hand this to you Ian or Martina for a discussion on the communiqué. Thanks.

IAN SHELDON Thank you. Before we move on to communiqué, could you please thank all of our guest speakers on the panel here today? Thank you and with that, I'll give the floor to Martina to give us a bit of a snapshot on communiqué drafting.

MARTINA BARBERO Thank you very much, Ian. So, the topic lead would like to offer some text on DNS Abuse for the communiqué so we will be organizing ourselves to draft some text. And I think the idea we have is to draft something along the lines of what you see here. So, of course, we support the rapid finalization of PDP1 and the launch of the narrowly scoped PDP2. So, these are of course lines that the GAC has already taken multiple times.

But we also need to recognize that on DNS Abuse, we never have a silver bullet. We're always running behind. So, we need other initiatives to complement the ones that are either ongoing or about to be launched. And the GAC has established, let's say, a Christmas list of things that we'd like to see happening at some point so we will remind those.

We have also heard from the colleagues from GNSO that they are doing some prioritization work, so we're also very keen to continue the exchanging with the GNSO to hear what's the outcome of this exercise. So, this is in a nutshell the ideal content of the text, but we invite colleagues who are interested in this text to come and

approach as we can discuss together and add further points if needed.

IAN SHELDON Thank you. So, with that, if you do have any thoughts on issues of importance as relevant to DNS Abuse, please approach Martina or the rest of the topic leads. And with that, I think that concludes our discussion on DNS Abuse. So, please be back in the room at 13:15 when we kick off our substantive discussion on the communiqué. Thank you.

**[END OF TRANSCRIPTION]**