ICANN87 Bali | AGM – GAC Discussion on WHOIS Registration Data Issues
Sunday, October 18, 2026 – 10:30 to 12:00 WITA

ICANN ANNOUNCER

Welcome to the ICANN 87 GAC discussion on WHOIS and registration data issues on Sunday, 18 October, at 10:30 AM 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'd 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 you're speaking a language other than English. Please speak at a reasonable pace to allow for accurate interpretation. I will now leave the floor to Ian Sheldon, GAC Vice Chair. Thank you.

IAN SHELDON

Thank you. Good morning. My name's Ian Sheldon, the GAC representative from Australia and one of the current GAC vice chairs. I'd like to welcome you all to the GAC session on gTLD registration data issues. We have quite a packed agenda here today

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.

with quite a good breadth of guest speakers and paired up with GAC representatives. We might kick off pretty quickly, and I'll let each of the speakers introduce themselves at the agenda item. So without further ado, I might hand it to Gabe Andrews from the United States to kick us off on law enforcement authentication. Over to you, Gabe.

GABRIEL ANDREWS Thank you kindly, Ian. So this is Gabriel Andrews, United States and co-chair of the Public Safety Working Group. And if we can go to the next slide. I wanted to give some quick background on where we are on the law enforcement authentication topic and how we got here. As many of you may remember, back in 2022, ICANN had published an operational design assessment of their SSAD, the Standardized System for Access and Disclosure, which carried a pretty hefty price tag, operational cost estimates between $14 and $106 million, and authentication challenges were a key cost driver in that. And this led to various conversations in the community. It led to the creation of a lighter weight RDRS model, and it led to conversations within the Public Safety Working Group about whether and how we could employ existing or aspirational law enforcement authentication tools that might be applicable to the ICANN use case and might offer some help. We formalized those conversations over time. This involves communications between PSWG and GAC and the Board at various points, culminating in a Board resolution in ICANN84, which asked the ICANN President to encourage ICANN to collaborate with the PSWG on possible law

enforcement authentication. This is all very much appreciated. This has all been tremendously helpful, and as is the ongoing collaboration with ICANN Org staff.

Let's go to the next slide. As many of you may recall, the model that we were putting forward was that law enforcement might make use of portals that they could access at their job sites to authenticate into ICANN-operated request systems, whether it's RDRS or whether it's the SSAD in the future. Then use those tools as normal. Any request that comes out of that would then be paired with the authentication that's provided by those law enforcement agencies and passed along to the registrar so that they can have confidence that when someone purports to be law enforcement, that they actually are. Everything downstream would follow the process as normal, and disclosures would be routed back to the employee. Go ahead and click the next slide. So what we proposed to test was the actual connectivity piece then of how would the FBI's Law Enforcement Enterprise Portal in the US, which provides services to approximately 18, 000 law enforcement agencies there, or Interpol's aspirational GDPI, a Global Digital Police Identifier system, how would these connect to ICANN, make sure that they're talking the same language, that the appropriate certifications are checked, and et cetera. Next slide.

Now, before I hand over to Janelle of ICANN Org, catching up to where we are today, some of those initial conversations that we talked about had started off very informally. Members of the community that wanted to participate in them wanted to also

increase the transparency and the record keeping of these, and these are all valid requests, and so we're very grateful to ICANN Org having since stood up what is now called the Law Enforcement Input Group, which was created in July of this year, and which is now run by Janelle. And I am going to turn over the floor to her now to give an update from Org's perspective on how that's going.

JANELLE MCALISTER

Thanks, Gabe. So we did kick off the input group in July of this year. It is a slightly different process for ICANN, where this is not a policy development group. This isn't a working group. And we're using the term input group as a way to distinguish that we are looking for community input in the work that we are doing on this. And it is happening simultaneously as the policy development group, or the SSAD group that's looking at the policy for this. If we could go to the next slide, and one more. There we go.

So, to pick up on the background that Gabe started with, again, that started with the Public Safety Working Group and is now being taken over by ICANN, and this has allowed us to invite community members to participate in this conversation. We've done different meetings with this group. The first one we did created background information on the group, as well as a meeting to discuss how the FBI and how Interpol currently authenticate law enforcement agencies, and how that could be incorporated into a potential system with ICANN. Our next step that this group will be doing is a proof of concept test, and what this is, is looking at the technology

between ICANN's RDRS and the FBI system and the Interpol system, and how they can pass information to our system identifying an authenticated law enforcement request. I do want to distinguish, we're looking at how the technology works and how information can be passed into ICANN system. The actual definition of what information is passed is being decided by the SSAD. That's one of the big distinguishing characteristics of the two groups. And if we can go on to the next slide.

Yep. So the input group specifically is looking at four different areas. One is this proof of concept test between FBI system and Interpol system with ICANN's RDRS. We're also working with the input group to go through potential workflow design of how an authenticated agent or requester is authenticated, in this example, by Interpol or the FBI, and how that authenticated information is then passed on to ICANN as part of the RDRS, who can then submit a request for information to a registrar. So we're going through that potential workflow, and that workflow, again, within the input group is very much a hypothetical and is dependent on policy recommendations that come from the SSAD before they're finalized. We're also looking at technical requirements, specifically how the two systems communicate to each other and how information is passed back and forth between the systems. And the final process for the input group is developing a lessons learned document or a summary of findings, as we're calling it, that is passed on to the SSAD implementation to help inform what their work is. Next slide.

And last, I just want to distinguish the difference between the input group and the SSAD SRT. So the input group is very specifically looking at the technology that is used between currently the FBI and Interpol and ICANN's RDRS. This is very limited. It's two agencies right now. I think in order for this to move forward, we would need to look at more authentication providers. But for now, we're just looking at exploring this technology, and the policy development is really coming from the SSAD, which we'll discuss by one of my colleagues here. And again, we'll have a summary of findings that comes out around the same time that the policy recommendations are finalized, so that when it goes to implementation, we helped inform and hopefully move along implementation quickly. Next slide. I think this is just last. I'll say some of the deliverables are happening again at the same time. So the SSAD will have their public comment period around the same time that ICANN starts actually doing the technical testing between our RDRS system and Interpol and the FBI. And then we'll have our summary of findings published around the same time that the SSAD policy recommendations come at the same time. So with that, I'm happy to answer any questions about the input group. I also think the SSAD will be speaking as well, if we want to do those questions together. But Gabe, I'll turn it back to you.

GABRIEL ANDREWS Yeah. Do you have Q&A?

IAN SHELDON I don't see any hands yet. Any questions for Gabe or Janelle?

GABRIEL ANDREWS And importantly, we are going to be speaking about the SSAD directly next, so any questions can be incorporated jointly thereafter. All right.

JANELLE MCALISTER I think so.

IAN SHELDON Cool. Thank you. Well, if there are no questions, perhaps we can move on to the SSAD supplemental recommendations.

SUSHIL PAL Please, I just want-

IAN SHELDON Oh, sorry. India, please.

SUSHIL PAL Just a small clarification. So March timeline is only for, I think by March timeline, we'll have a proof of concept for its integration, one between Interpol and FBI, as well as for integration with ICANN RDRS or SSAD portal. Is that right? Or do we again hit the roadblock for its integration with ICANN portal?

JANELLE MCALISTER So by March, we'll have the proof of concept testing and information or lessons learned from that, but we will not move towards actual integration between the systems until policy recommendations are complete and we're ready to move forward with that. So that will definitely come at a later time.

SUSHIL PAL Do we have a policy recommendation holding it? Is that the reason? Or there is a-

JANELLE MCALISTER Yes.

SUSHIL PAL I don't see. I'm still not getting it. What is the policy recommendation holding it?

JANELLE MCALISTER Oh, the SSAD policy recommendations are what's holding it from actually being implemented into ICANN systems.

SUSHIL PAL But I think that actually the proof of concept is only between Interpol and the FBI. Is that right?

JANELLE MCALISTER The proof of concept is using FBI and Interpol as the two cases.

SUSHIL PAL Is that not an already established thing with regard to our normal law enforcement operations?

GABRIEL ANDREWS I think what you're asking is, it's Interpol connecting to ICANN, and it's FBI connecting to ICANN. And right now, the RDRS is something that exists, but we anticipate there being the SSAD as the more long-term permanent entity that we'd be connecting to. And so what we're testing now is just the connectivity to put us in a good spot so that as the SSAD is actually stood up, that we're able to be there as it comes into reality. Does that answer the question?

SUSHIL PAL No, it does not. I'm still not clear, I think.

IAN SHELDON Perhaps we can move through the SSAD update, and that might shed a little bit more light on where things are up to, and we can come back to this if you've still got questions. Would that work?

SUSHIL PAL If this pilot actually establishes a connectivity to the ICANN platform, then it's something worthwhile we should look forward

to. The rest of the things are already established at our normal daily operations. So I don't see what the proof of concept is heading at.

IAN SHELDON: Yeah. Let's come back to this point. With that, I might give the floor to David. Thank you.

DAVID BEDARD: Thanks, Ian. Next slide. Oh, great. So we have some background on the establishment of the SSAD supplemental recommendations and the supplemental recommendations team. I think Janelle and Gabe did a pretty good job with providing us with some of the background. So what I'll just point folks here to is that, specifically in March, after the Dublin meeting, the Board rejected the original SSAD recommendations. So this enabled the community to revisit the recommendations and revise them based primarily on the RDRS Standing Committee report and lessons learned from that process. So coming out of that, they established a supplemental recommendations team with representation from across the community. And for the GAC, we have two members, one representative, which is myself from Canada, and an alternate representative from the US. And so we're there to reflect and ensure that GAC priorities are reflected in the updated recommendations coming out of the SRT. Next slide, please.

Great. So here are some of the priorities that we, the GAC, have articulated through various communiqués, but most recently in the

communiqué coming out of Seville. So here, we wanted to ensure that the system is permanent. It was a big priority for the GAC. We wanted a permanent system to facilitate the request to gTLD registrars for disclosure of domain registration data. We wanted participation within it to be mandatory for all gTLD registrars, and we also really wanted the ability for the system to meaningfully support the integration of requests for underlying data that is held by privacy or proxy services. And, lastly, we really wanted the SSAD or the permanent system to be able to process urgent requests from a technical level, but also making sure that the recent updates to the urgent request policy that occurred last year are enabled to be operationalized as it would be contingent on the development of the work that the input group is doing, but then also of the SSAD policy process. So next slide, please.

So next steps. So the group actually met yesterday, and we've been able to get quite a bit of our priorities reflected in the initial recommendations. I'll just note that the recommendations still need to go out to public comment, so nothing is final until it's final. So, right now we do have confirmation that this is a formal policy process, so there will be required use after the recommendations are adopted by the Board and move through implementation. It will also offer the ability for ccTLD operators to have optional participation within the system and the technical integration needed for that. And we were also able, just recently yesterday, to move towards agreement within the group on language around how the system would handle privacy and proxy requests. So we

have it here at 5.7.3, which will be included within the recommendations for public comment. So that was a big priority for the GAC as well. And later this week, the GAC will be seeking confirmation from the Board that updates to the urgent request policy will be operationalized once the SSAD recommendations are approved and implemented. And we're also trying to embed that specific language and implementation guidance within the recommendation as well, since it's really quite important for the GAC that the urgent requests policy becomes operationalized as soon as practicable. Next slide, please. So I will hand it over to Marc Anderson from VeriSign, who is our trusty chair for the SSAD, and he'll just run you by some further details on how the group is progressing, and we'll be able to answer any questions that you guys might have. Thank you.

MARC ANDERSON Thank you, David. Thank you for the introduction. I'm Marc Anderson from VeriSign, and as David said, I'm the chair of the SSAD Supplemental Recommendations Team. Thank you for having me here today, and I'm happy to be able to provide an update on the progress and status of the SSAD Supplemental Recommendations Team. Before I get into that, just a little bit of background, if you will. Gabriel mentioned that there was an operational design assessment for the original SSAD recommendations, and that operational design assessment raised questions about the feasibility of the original SSAD recommendations. And based on the questions raised by the

operational design assessment, there were tri-party meetings between the GAC, the ICANN Board, and the GNSO. And as a result of those meetings, there was agreement to have a pilot, what you've heard mentioned as the RDRS or the Registration Data Request System. As David mentioned, it was a two-year pilot meant to inform future policy development. This, I think, was a really good example of collaboration between different groups within ICANN and some innovative policy work to help inform real practical policy development. Now we're at the phase where we're tasked within the supplemental recommendations team of taking the lessons learned from the RDRS pilot and applying them to updated supplemental recommendations for an SSAD system, a system for facilitating legitimate access to non-public gTLD registration data. If we can go to the next slide, please.

With that sort of background, I want to provide this slide. Some flavor of this slide is something that the supplemental recommendations team has in pretty much all our meetings. A fundamental principle for the supplemental recommendations team is to produce recommendations that balance the needs of data controllers, requesters, and data subjects. And so with those high-level principles in mind, we're trying to produce recommendations that meet those needs, are implementable, and are Board and GNSO Council ready. Next slide, please. The supplemental recommendations team first met on 12 May, earlier this year, and over the course of the following months, we've worked on refining the original SSAD recommendations. We

started with 18 supplemental recommendations. We started with 18 recommendations, and based on the lessons learned from the RDRS, we've pared them down to 12 recommendations. We've considered all the lessons learned from the RDRS, input from the ICANN Board, and the broader community, and we now have an updated set of recommendations which we're targeting to have out for public comment on 10 November, so shortly following the ICANN 87 meeting. Next slide, please.

We've had approximately 28 meetings so far, which it seems like a lot longer, but in those 28 meetings, we've made an awful lot of progress, and we're very close to finalizing the recommendations and getting them to public comment ready. To help get us there, we've had two full-day meetings. We had a full-day meeting before ICANN 86, and then the Thursday before ICANN 87, we had a full-day meeting as well. And if I could take a moment to thank ICANN Org and staff. A lot of work and planning and preparation went into that, but I think the Supplemental Recommendations Team really appreciates the support and commitment from ICANN Org in supporting this important policy initiative. Next slide, please. So I've already touched on this a little bit, but real quick, what we're trying to achieve. The goals of the SSAD are to produce a single standardized request system. We want reliable accountability, authentication, which we heard from Gabriel a little bit. We want a standard process for contracted party review and lawful disclosure, and we want a system that is able to take into account operational learnings as the system progresses. So the

supplemental recommendations aim to preserve the core values of the SSAD while reflecting lessons learned from the RDRS pilot and Board and community input. Next slide, please. And then just to wrap things up, you can see up in the slides, this is our overall timeline. Our focus right now is getting to public comment on 10 November. Assuming we stick to schedule, public comments will close on 12 December. We'll review the public comments, look to finalize our recommendations, and get the supplemental recommendations to GNSO Council in March 2027. And I think that covers my portion, and I believe I'm turning it back over to David.

DAVID BEDARD

Sure. Thanks, Marc, and thanks for your leadership throughout the SRT. I know it's been a lot of work and I think we've made significant progress. So I'm just going to touch very briefly on next steps for the SSAD in terms of GAC priorities. So we are meeting over the course of the week. I think we have three sessions in total, plus our, as Marc mentioned, the day minus one event that we had before ICANN officially kicked off. And as Marc said, the SSAD SRT is expected to publish its initial recommendations for public comment very shortly after the ICANN meeting. GAC representatives will be drafting and circulating GAC comment for that public comment, so we'll be making sure that the GAC is engaged throughout that process as well, and we'll be looking for feedback on that public comment. So, I think from there, we're

heading over to Owen to speak to the accreditation of privacy and proxy services. Thanks.

IAN SHELDON I might just pause there to see if there are any questions for David or Marc before I give the floor to Owen. I see no hands. Perhaps we can move on. Over to you, Owen. Thank you.

GABRIEL ANDREWS Next slide, I think Gabe-

IAN SHELDON Oh. Gabe first, then Owen.

GABRIEL ANDREWS Hello again. So this is Gabriel Andrews again speaking. Let's go ahead and go to the next slide. We're going to talk about the privacy and proxy services accreditation policy work. But before we dive into it, because there's been turnover of folks and because even though some of the old hands know this very well, I want to make sure that we all understand what we mean when we're talking about privacy services versus proxy services. There are some distinctions. When you talk about a privacy service, one of the key distinctions is the customer that's asking for the domain is still the registrant. They're going to be listed as such, and I'll show you some examples in a second. Whereas when a proxy service is used, the actual registrant is the proxy service, which has a lot of

repercussions on how you draft policy. So let's go to the next slide and let's look at what this data looks like in practice. Here's an example of a lookup of this data where there is no use of privacy nor proxy. I looked up CNN. Years ago, I did this search, and you can see in the red box, you get back the information of Turner Broadcasting Systems, their contact information. Importantly, if I was law enforcement and I wanted to reach out to them because something bad is going on and I need to let them know, there is a phone number I can use to do that. This is the kind of information that's very useful to public safety in a variety of contexts. But let's go next.

A more recent check of the very same domain name shows that it's more recently using a privacy service. You can tell that the registrant is still the same, it's still Turner. But instead of the contact information, it's now showing as redacted these days. There's no phone number listed. There is a functional email, thankfully, but it's obfuscated, so it's maybe an email provided by the privacy service that'll route to them. So it's still, just to repeat the point, it's still the same registrant. The data's obfuscated by privacy. Next. The final example is that when a proxy service is used, and this is a different domain lookup this time, you see that the registrant is actually the proxy service. It's typically provided by the registrar, affiliated with is the term, and any information there is not going to be about the customer anymore. It's going to be about the entity that's providing those services. And this can be very confusing to folks outside of our circle where we know and

understand this, but maybe folks that are just your day-to-day investigators might struggle with recognizing when a proxy service versus a privacy is used. Let's go next.

Another big open question is how often are these services actually used in the wild? And I don't have a good answer to that. I have this slide that I'm reusing from a 2020 presentation I gave to the GAC years ago when we were talking about law enforcement referrals of fraudulent domains, and we noted that when we were doing a particular program where we referred more than 1, 000 domains to various registrars and registries, we went back in an after-action and looked to see how many of them were using privacy or proxy and found that approximately two-thirds were. And I expect that this number's probably climbed since, due, if nothing else, to the increasing use of these services by the registrars, like turned on at the moment of registration. So where the customer doesn't do anything on their own, it's simply enabled by default unless they take action to not enable it. And so I think the general trend is that this goes up, but there is no perfect information that I found to tell you exactly how prevalent it is these days. But it has the important downstream repercussion, though, of when we talk about drafting any policy that is going to be speaking about the end customer who's actually making use of this, terms like registrant, we might be tempted to use, but it can be very ambiguous depending on which of these services are employed. Next. And here, I think I hand over to Owen.

OWEN FLETCHER

All right. Thank you, Gabe. So I'll highlight that's a useful introduction to the importance of this topic. David spoke a bit as well about how privacy and proxy services have come up as an issue or a topic in the SSAD Supplemental Recommendations Team. I will speak about the separate process that's ongoing that relates to privacy and proxy services. That process is the Implementation Review Team under the GNSO on Privacy and Proxy Service Accreditation Issues. This IRT is implementing policy recommendations accepted by the ICANN Board, actually, many years ago now. But we've made great progress in the last year or so in that IRT on this implementation work. So the idea behind this IRT or the original policy recommendations was to accredit all privacy and proxy service providers. So, you could ask, what does accredit mean? And the way people are thinking about that has shifted a little bit over time. I think years ago, probably some people envisioned a situation where all privacy and proxy providers became accredited, just like registrars are. They signed separate agreements with ICANN. There were challenges with that idea. So the IRT is looking at other ways of implementing the recommendations.

I put this quote in the second bullet from the PPSAI final report. It says, "Registrars are not to knowingly accept registrations from privacy or proxy service providers who are not accredited through the process developed by ICANN." I think this is a good high-level explanation of basically what's going on here, whether it's some

kind of standalone agreement that privacy proxy providers have or whether it's something else. The idea is that privacy and proxy service providers should be known and identified and subject to the requirements in the ICANN policy on privacy and proxy issues. Right now, Gabriel and I actually are both representing the GAC in this IRT, and the IRT is reviewing draft policy language on, or draft consensus policy language to implement these policy recommendations. So, in the coming slides, I'll highlight a few notable topics in that draft consensus policy text. But as David mentioned, importantly, also in the SSAD, privacy proxy is relevant. Specifically, the issue there is just to make sure that if you submit a privacy or proxy disclosure request through the SSAD, then it is given full consideration rather than somebody saying, "In response to your request, this is a privacy or proxy domain. You need to contact someone else to get that data." So that's the SSAD or RDRS piece of it. Now I'll give you the highlights from the IRT on the PPSAI. Next slide, please.

I've got three slides where I'll highlight a few things. So this first one is about the, you could call it the pass-through of policy requirements. Feel free to read this language, but generally, the idea in the current draft text of the consensus policy is that registrars must require all of their downstream partners, anyone between them and the person registering the domain, or the entity registering the domain. Registrars must require all those entities to comply with the requirements of the draft consensus policy. And one way that's done is, or that that would be done under the draft

policy language is through written agreements with each privacy or proxy, or with each entity, written agreements with each entity in that chain all the way until you get down to the last entity, which is the one working with a customer and providing them a privacy or proxy service. At the bottom, there's this important language about how registrar's agreements must require each service provider to impose equivalent obligations on further downstream providers. So the requirements in that way would pass through to each lower entity in the chain. Next slide, please.

Another item included in the draft consensus policy that is in line with what I think the GAC would hope to see is about disclosure requests. So the draft policy introduces language that is largely taken from the existing Registration Data Policy and applies that to privacy and proxy domain registrations. So based on the draft language, registrars would need to respond to disclosure requests or ensure that their service providers respond to disclosure requests within 30 days for a normal request and within 24 hours for urgent requests. Those are the same timelines used for non-privacy or proxy registration disclosure requests. The requests, again, based on the draft policy language, the requests must also be each considered on their own merits, considering the provided rationale and basis for each request. This is useful because you can imagine that without a requirement like this, it would be more difficult to seek information about the privacy or proxy customer in a case like Gabe was showing, where that information's not readily available in registration data records. Next slide, please.

The draft consensus policy language covers some other issues. Of course, I wanted to highlight the ones we just went through for your particular awareness. A couple of other things I'll just quickly mention are a requirement for privacy and proxy service providers to establish abuse reporting contacts to facilitate cases where somebody identifies abuse on a domain and wants to contact the provider about that. Other draft language covers what should happen when the registrar or their service provider is not complying with the requirements of the policy and what steps would be taken to address that. Then there are a range of other issues, such as some related to data escrow and how notifications are relayed on to privacy and proxy customers to make sure that they enjoy the same rights and protections that all non-privacy proxy registrants would also have. I might have one more slide, please. Right. Just on process and next steps. So the IRT has been meeting regularly. It has one in-person meeting this week on Wednesday. And based on IRT input on the current draft policy language, ICANN Org staff plan to propose revised draft text of the consensus policy. Discussion will then continue through the end of the year, and the goal is for the language to go to public comment in January 2027. The GAC will continue its engagement in the IRT during this process, and I'm sure we would like to consider a submission to the public comment. And I was going to mention one other thing, just in the sense that this is good timing, I think, because the public comment on the SSAD SRT is also happening in the next few months. It's a good opportunity for us to make sure that privacy and proxy issues in both of those processes are

addressed in a way that supports the GAC's interests. I think that's it, unless there are any questions. Thanks, Gabe. Gabe, go ahead.

GABRIEL ANDREWS

Yeah. I just wanted to really stress one important piece of this that Owen spoke to a moment ago. But speaking with my hat on as one of the public safety officials who have submitted requests for registration data using the RDRS and getting responses back from the registrars that in response to your request, here's information about our proxy provider, that's been a source of major frustration to a lot of my colleagues in the public safety arena. And the mere fact that we're getting to a point now where we're having this potential policy that would have a requirement for responses to actually address the underlying customer data, that's a really important advancement in this discussion, and that's something that I cannot stress enough how important that is, and I'm very grateful to see us getting to that point and the GAC being successful in bringing that forward.

OWEN FLETCHER

Sorry. I also wanted to just add one other very short note. So while I think a lot of the language in the draft consensus policy aligns with GAC interests and addresses our concerns, it is not final, just like David was saying about the SSAD language. So that's why we'll keep engaging in the process. Thanks.

IAN SHELDON: Thank you for the update. And before I open the floor, I would recommend GAC members take this update back and talk to your law enforcement agencies about this. This is quite an important step, and it's certainly something that we'll be doing in Australia, to let them know that one of these major barriers is being worked through. And like Gabe said, it's quite an important step, and I think it's really important that we let our colleagues outside of this room understand the progress being made here. So with that, I will give the floor to Sushil for a question.

SUSHIL PAL: Thank you, Chair. I'm Sushil from India. I must compliment the PPSAI IRT for the fantastic work they have done, and we are completely aligned with your draft recommendation for the must obligation on the urgent request, as well as for the obligation to provide such information for proxy and privacy service providers, because the ultimate contractual liability is with the registrars, and they have a fiduciary responsibility to provide this information to whosoever asks for it. And my only request is that we keep our efforts on so that we align it completely with SSAD recommendation or SSAD IRT, which is also shaping up in parallel, because its implementation will completely rest on that. Thank you.

IAN SHELDON: Thank you. Susan from the United States. Thanks.

SUSAN CHALMERS

Thank you, Chair. So in light of the fact that we have these two very important public comment processes coming up where the community can weigh in, I just wanted to make two very quick points. The PPSAI consensus policy, simply, we believe that registrars should ensure that all of their downstream service providers operate privacy and proxy services in compliance with ICANN policy. And on the SSAD supplemental recommendations, the policy language should support a straightforward process for privacy and proxy disclosure requests. So registrars and their downstream service providers should evaluate and respond to those disclosure requests based on the requirements finalized in the PPSAI consensus policy, even when those providers are not affiliated with the registrar. And that means that requesters will not have to send an additional disclosure request to the privacy or proxy provider, further to what my colleague Gabriel was saying. Thank you.

IAN SHELDON

Thank you. Next I have Giacomo from the WBU. Thank you.

GIACOMO MAZZONE

Thank you very much for these useful explanations. My question is in line with what has been just said. Are we sure that with this formulation, we will avoid the cascade of responsibility, that the provider will send you to the other provider and then to another

one? Because the wording doesn't seem to be cogent, no? Can you better argument that?

OWEN FLETCHER

Hi. Yes, I only put on the slides a couple of key parts of the draft language. It's much longer. I'm happy to talk, further look at it with you or anyone else who's interested. I think at least as currently drafted, again, it's not final, but as currently drafted, it, I think, does seem to avoid what you referred to as the cascading chain of maybe responsibility. So the registrar would need to have an agreement with a partner, such as a reseller, perhaps, and if that reseller had another reseller below them, then the first reseller would need to have a similar agreement with the second reseller, and the language would call for those requirements to get passed on further to each other entity. So that would seem to ensure that, whether it's the registrar or a service provider, somebody will be ensuring compliance with the policy requirements, and if there's non-compliance, then there's the language about how ICANN would handle it.

GIACOMO MAZZONE

Thank you for the precision. I will have a look at the draft with you later and with great pleasure. But the timeline will be cogent all along the line. So if the notification has been given 24 hours urgent request, this means that all along the chain applies the same 24

hours, or there will be 24 hours the first, 24 hours the second, et cetera.

OWEN FLETCHER: My reading, at least of the current draft language, is that it would just be 24 hours, and it wouldn't be 24 plus 24 plus 24.

IAN SHELDON: Thank you. Next I have Nigel from the CTU.

NIGEL CASSIMIRE: Thank you, Chair. Nigel Cassimire from the CTU, and my thanks to all the presenters for the useful information presented. Just a quick one, I think, to Gabe about your 2020 slide, which already makes the case for the value and urgency of dealing with this proxy and privacy services thing. Is there any challenge, though, with collecting the data to update this to give a more current view?

GABRIEL ANDREWS: I think you're right to highlight that. I did some searching online. The reason I ultimately went with this is because it's something I had direct experience with, and I felt more comfortable defending it. That's all. I recognize it's a little bit stale. The most recent public reports I've seen were from other folks in the industry space. I don't recall exactly who said what, but I will say that the general trend observation I read seemed to be that abusive registrations are still in the two-thirds general ballpark. Non-abusive registrations,

there's some disputed numbers for, generally lower. I think that the key point I'd like to leave you with is that we are increasingly in a world where registrars are enabling these privacy and proxy services by default at the point of registration. So my expectation is that this will just trend higher over time as more do this. If that changes, if for whatever reason the ecosystem changes and registrars stop turning that on by default, then maybe that'll change. But that's just what I've seen in the ecosystem since, and I think that this is still relatively representative of abusive registrations out there. But again, this is anecdotal. It's from my particular experience dealing with about 1, 000 domains. I don't think there's a perfect source of ground truth out there, unfortunately. If you find it, tell me. I'd be glad to use it. Over.

OWEN FLETCHER I was going to say something just like that. If you find it, please tell us. In particular, I think one challenge is that truly authoritative or representative data that would help us know the overall situation on this issue probably would need to come from registrars themselves, as they have access to the data of their customers. And we do not. So if any registrars are listening and are interested in sharing information about that at any point, I think that would be welcome. Thank you.

IAN SHELDON Thank you. Giacomo, is that an old hand? Nope. Great. So with that, perhaps we can move on to the next item. So I might pass the floor

to Martina to take us through a conversation on the 15-day verification timeline.

MARTINA BARBERO

Thank you very much, Ian, and I will try to speak slowly because I normally speak too fast, and also do a bit of a background on this topic. I understand we have a lot of new GAC colleagues, and this is a very long story. So bear with me for a couple of slides before we go to our speakers. The question of accuracy, registration data accuracy, has always been very important for the GAC. As you see, there is a long history of communiqué text and GAC participation into important policy processes, going back to EPDP Phase 2, where the GAC actually was in a minority position and made a minority statement on the importance of accuracy. Following the work on the EPDP Phase 2, the GAC took part in the Accuracy Scoping Team that was formed in October, but unfortunately paused in 2022. And then there was a gap of a few years where not much happened. But then, in 2025, the GNSO started resuming work on accuracy and asked the community input on a number of questions, to which the GAC provided input and launched the work of Accuracy Small Team, which released its final report in the summer 2025, and the recommendations from that report to the GNSO were all approved by the GNSO. Following which, in Dublin, the GAC said to the GNSO that they need indeed to implement those recommendations. And then we go to the next slide.

So we have reiterated the importance of this topic for the GAC in the Mumbai communiqué, but we have scoped it a bit further because accuracy is a pretty big topic. And in recent conversation, we have focused on one of the issues that was picked up by the INFERMAL study amongst others, which is the 15 days timeline for registrars to validate and verify registrant's contact information. What does it mean concretely is that if I today register a domain name, the registrars under the current ICANN policy has a 15 days window to verify and validate my contact details. This rule comes from 2013, if I recall correctly, so more than a decade ago. And there's been some studies, amongst which INFERMAL, but also other evidence, that this window can be problematic. So we're going to hear about that. We're going to hear about some practices of some ccTLDs that do otherwise. But this is what has been in the focus of the GAC as a potential problem to be addressed. It was also included in the DNS issue report. So following these developments in the spring 2026, we have asked to start a conversation with the GNSO and the ICANN Board to try to discuss this further. And if you go to the next slide.

We had a first informational exchange in Seville with the GNSO, where we stressed that it is particularly important to look at this potential policy gap before the delegation of the new strings in the context of the next round. That of course, we need to take into account the operational challenges for implementing a new window, or eventually even validation before delegation of the strings, sorry, of the domain names. And we also flagged back in

Seville that we would like to have the Board involved in this discussion. What followed from Seville was further correspondence between the GAC Chair and the Board, and we expressed openness to consider different approaches to approach this issue. And if we go to the next slide.

Which led to a more substantive, let's call it this way, call that we had with the GNSO and the registrars shortly before this ICANN 87 meeting. It was an interesting conversation because we did have a really evidence-based exchange. We heard a number of things that are of importance, amongst which the fact that there is no established position yet within the registrars group on what we could do, and if this is a problem, and what could be done to address it. We also discussed with the registrars what are the impacts of changing these 15 days validation windows and whether we need to distinguish different types of situations, for instance, new registration from transfers or registration data updates. We also learned from the registrars that there are a number of very different practices. Some of the registrars follow the 15 days window. Others verify immediately. Some have some fraud prevention measures, and especially in the ccTLD space, there are some stricter verification measures. We're going to hear about that from some of the colleagues in the GAC today and also from the ccNSO DASC leaders. So we agreed with the registrars that we need to continue the conversation, gather further evidence, and also, as you may have seen by emails, we have received a request from the GNSO to address a number of questions on this topic

during the GAC-GNSO bilateral. That will be this afternoon, if I recall correctly. So we will be providing some initial feedback and collecting more feedback from GAC colleagues in order to provide a written feedback in the next steps. So if we go to the final slide.

I'm going to now pass the word to our speakers, but before I do that, just a recap again for newcomers. So accuracy of registration data is a pretty broad topic. We have narrowed down to a policy issue that we have seen emerging from multiple sources of evidence, which is this 15 days verification window. Why it is a policy issue, because while abuse of the DNS can occur within these 15 days windows, and also because we don't really maybe see the rationale for these windows now 13 years after the world has changed. So maybe there's an update that could be made. But before we go into a GAC discussion, let me give the floor to Professor Maciej Korczyński, who is the main author of the INFERMAL report, which is one of our sources of evidence. The floor is yours, Maciej.

MACIEJ KORCZYŃSKI So hello everyone. My name is Maciej Korczyński. I am professor in Grenoble Alpes University, and also co-founder of Core Labs. And today I will discuss briefly one of the things that we investigated as part of a broader, bigger INFERMAL project, which is operational validation of registrant information. And this will be also a good opportunity to put the results into perspective a little bit. Next one, please.

So a little bit of context. So INFERMAL, Inferential Analysis of Maliciously Registered Domains. This is the study that we performed at Core Labs and Grenoble Alpes University. It was funded by ICANN and in close collaboration with OCTO Team. The goal was to investigate domain name abuse from the attacker's perspective, which is very important because there will be multiple other perspectives to take into account when looking at those practices. And the goal was to identify factors driving malicious domain registrations. So the scope of the study was on maliciously registered domain names, maliciously registered phishing domains. So our starting point were URL block lists. So we put a lot of effort to filter out all legitimate domains, so of shared infrastructure services, think about dynamic DNS services, subdomain providers, but also URL shorteners and also compromised websites where the domain names themselves are benign. So we selected 73 features that were divided into three latent factors. So registration attributes. So think about, for example, retail pricing, proactive verification. So for example, operational validation of email addresses or reactive security practices, for example, uptimes. So how fast TLD registries or registrars take down malicious domain names. So in our study, we used a GLM regression analysis, ideally with the aim of a causality, but we calculated correlations, and the goal was to study relationship between features and concentration of phishing domains at the registrar TLD level. And this is because some

practices, some policies might come directly from registrars, while some from the TLD itself. Next slide, please.

Okay, so one of the features that we studied was operational validation of registrant information. And here we tested 38 registrars, whether they verify operational contact email addresses and phone numbers during account creation or before the purchase. So we did not really evaluate the 15 days period. And the conclusion was, when the validation of registrant information takes place during the account creation or before domain purchase, it has significant negative coefficient, indicating that it is associated with 70% decrease in malicious registrations. So how to interpret all of this? Next one, please.

So two very important points, not only related to this particular feature, but all of them, is that all the results of the INFERMAL should be interpreted with caution. They may or may not be generalized into actions by registrars or TLDs. And second very important point is we take the perspective of the attackers, but it's also essential to consider economic implications, the impact on legitimate users, and also it's not the question whether the attackers will respond to some changes in practices or eventually policies, but also how they're going to adjust. Will it be difficult, easy for them? And this is something that me personally am missing a lot in discussions about common practices and so on. And also the result of partial and full implementation. So I would

like to give three examples to cover those two points. One of them will be operational validation of email addresses.

So first example, the INFERMAL study shows a high correlation between bundled services that come with domain registration. So for example, expected increase in abusive domains when the DNS service is bundled with the domain registrations is by 200%. Attackers also very much appreciate bundled hosting service. But the problem here is enforcing or asking registrars to just sell the domains without bundled services wouldn't really make sense because we would be asking 60, 70, maybe 90% of registrars to change their business model. Another example within the INFERMAL study, we also selected two labels of most attacked brands at that time, which was Facebook and Office 365. And we tried to register domains with different registrars, with different TLDs, and two registrars actually blocked it. But now, once more, if we take one step back, what would be the complexity of implementing this and how would attackers adjust to such a change? So first I will have a question. Who among you knows the brand that is called Allegro? Please hands up. Okay, there is no one. So Allegro is a Polish equivalent of Amazon. So you know it either because you're Polish or because you analyze abuse data on a regular basis because Allegro is one of the most attacked brands in Poland. So my point here is, if you would like to introduce something like this, we would need to very carefully select brands that are being attacked. We would need to go to Indonesia, Poland, France, Canada, and so on, select local banks, try to get the labels

that we would like to block. What about also ING Bank, for example, with very short names, labels? Also what about inclusions? So it does not need to be Facebook, right? Or we can replace by double zero, zero inclusions, bit swaps. Conceptually, it would not be trivial, and it would not be trivial also to implement. And what would be the response of the attackers if we finally managed to have such a practice or such policy? The attackers would simply start registering domains without those keywords, and then they would start putting deceptive keywords as subdomains. And then we could go a little bit further, and then registrars potentially could also check subdomains, right? But then the attackers could make delegation to their own authoritative name servers, and technically all of it, it's not very difficult. So we need to take into account if we introduce some practices by how we will raise barriers for abuse.

And the third example is directly related to operational validation of email addresses. So this is also very similar example. If there are attackers that exploit this, then adjusting to such a change in policy would be really easy in the sense that they would use disposable email addresses, phone numbers, so raising abuse would be minimal. Now, the final point I would like to make is the more data-driven analysis we have, the better. So the INFERMAL study is very comprehensive, but it also has its own limitations. And when it comes to this operational validation of email addresses, in my opinion, the intermediaries that are best equipped to discuss this subject are registrars because they do have ground truth data. They can see how many abusive domain names were validated before

they were detected and taken down. So that's why I think WhoGoHost, Namecheap, the statistical analysis provided by them is valuable, and the more data we have, the better. So thank you very much. And if you have any questions, I'm open. Thank you.

MARTINA BARBERO Thank you, Maciej. Before we go to Janos, I see his hand's up. Maybe we wrap up all the presentation because then we will have a bit of discussion, if that's fine. Janos, hold on one second. We have Barb Pearse from the ccNSO DASC. They have done a very nice survey of ccTLD practices. So Barb, the floor is yours.

BARBARA PEARSE Thank you very much. The ccNSO DNS Abuse Standing Committee has now just completed its third survey of ccTLDs. The previous two were done in 2022, 2024. I want to just start by giving you some brief context on the ccTLD landscape. There are 309 delegated ccTLDs. They're very diverse geographically, culturally, their size, their policies, and their models. For example, they range from nonprofits to university-run to government-run, et cetera. In respect of this survey, it includes responses from 65 of the ccTLDs or 21% of the population. This is not a scientific survey. It is self-reporting by those ccTLDs that participated. Next slide, please.

I'm just going to talk to you about one question. It's a big question with a few components to it. I've just brought up how the question was framed to the respondents, and it's essentially around do you

verify registrant data? And if so, at what point in the life cycle of the domain name does that occur? And does the ccTLD do that, or is there a requirement for the registrar to do that? Next slide, please. I'm just going to focus on the first three columns to the left, and this is around the timing of validation and who does it and how. So in the first column, you can see registrars are the green, the highest at about 44%. CcTLDs require registrars to verify registrant data. CcTLDs will do it to a lesser degree, and it's a manual exercise. Much less are doing it automatically with automation. And one of the barriers to automation is that databases for company or business registrations might not exist in all jurisdictions, or they might be cost-prohibitive. So an opportunity there is to facilitate that more and for free, and you may have more registries and registrants verifying data through those automated databases.

The second column, also in the first column, that relates to registration validation prior to registration, so before they are released to the zone. In the middle, the second column there is post-registration, and there you can see that registrars are required to do that less, and ccTLDs are doing that more and a lot more manually. The third column there is upon renewal. So registrars a little bit higher on renewal and ccTLDs not very often at that time. The last column on the far right is a slightly different topic, and it's around the point in time or do you do screening for suspicious registrations and how is that done. So significantly more ccTLDs are doing that manually and less requirement on registrars to be screening for suspicious registrations. And again, across all of the

columns, you can see automation is very low. So, some of the reasons why there is some manual verification happening is ccTLDs are different sizes, so they may not get very many registrations every day, and it's easier for them to undertake that manually. But if registration's scaled, you're going to need more resources and time to do that. That's all I had. The next slide there is just a bit of a shout-out to a webinar that we will have for the wider survey question results if anyone was interested to come along to that.

MARTINA BARBERO Thank you very much, Barb. It was very interesting and to see the diversity of ccTLDs practices, but also highlighting that some, they do verification before delegation. I think Finn will speak a bit about the experience from. Dk, and then we open the floor. I see there are already a lot of hands. So Finn, the floor is yours.

FINN PETERSEN Thank you. Finn Petersen from Denmark. I hope that the staff can put some slides up. The first one is number three. I will just give the result of effective validation procedure. I have stolen some slides from. Dk. They gave a presentation in Kobe. I think they have a one-hour presentation there and discussions, and I think that staff will put the link to that presentation so everybody can look at the Zoom and what was discussed there. I don't think it's the right slide. Number three. It's core problem, yes. In 2017,. Dk experienced an increase of intellectual property right abuse on websites, and also in 2018, they could see that it is rising. Already within the first two

and a half months, there were many of them, and they could see that this would increase. So they had a problem. So they thought about a solution, and if you go to the next slide, that is slide number seven. If you calculate it in the same way that I do, I will just... Further? Yeah. That's the right.

They had already a procedure on Danish customers and companies with our company registry and also personal number and the addresses. It was not so effective. It was troublesome for foreign companies and persons. There was some check, but not very effective. It was actually ineffective. What they did was that all Danes in 2018 were demanded to use MitID or NemID, which is a Danish electronic ID system. And it was mandatory for everybody, for companies, and for private citizens to use it. By using this, you have 100% guarantee on the identity of the person and the address and so on. For foreigners, they can also, if they have a relationship with Denmark, have the electronic signature, but if they don't have it,. Dk introduced a risk-based assessment. They have a kind of engine function looking through, and if the risk was too high, they make an identity check on it, and they have improved the identity check through the years, and they are considering to do more, especially on businesses.

The result of this exercise is shown in slide 14. I think it's called result. Yes. There have already been some studies in Europe on abuse on websites, on intellectual property violation. And you can see the statistics for certain countries and also from Denmark in November 2017. After introducing this, you can see a significant

drop in March 2018. The procedure was not fully implemented because all the existing domain names were running through the new procedure, and I think staff will be able to circulate a one-pager also showing the result measured in June 2018. And I can see the first row here. It is zero for Denmark, or approximately zero, and the last one is 0.12%, which is very low. And by introducing this, the reductions on expected violation was 50 times, which is significant by introducing new procedure. And if you look on different websites on the result on abuse, you can see. Dk on the top of it. If not really on the top, they are doing a lot to do that, and the result is good. Of course, they validate the data before they put it into the zone. All other will be nonsense to do it afterwards, and they haven't experienced any major problems. I don't think they had any problems when they introduced this for many years ago. Not today, which technology is even more advanced, but for 10 years ago or eight years ago, there was no problem. So a good, effective validation procedure and checking before putting into the zone, the result is good. Thank you.

MARTINA BARBERO Thank you very much, Finn. I think it was very helpful to have your experience, and back to you, Ian, to manage the queue, which is quite long.

IAN SHELDON Thank you. We have about seven minutes left in this session, and I've got three in the queue, and then I want to leave a little bit of

time to touch on communiqué, as well. So with that, perhaps I can give the floor to Janos for his first question. Thanks.

JANOS DUJAKOVSZKY Thank you very much, Ian. This is Janos Dujakovszky, other co-chair of the Public Safety Working Group, for the record. I would like to ask a question to Maciej, because if you work in the area of law enforcement and fighting crime, you will realize very soon that whatever you do, the malicious actors will adjust no matter what measures you take. So it's a core reality. And in this regard, I really appreciated your aspect on saying it does matter which measures are harder to adjust to, which ones are easier, which ones are harder. So I just wanted to ask you in that regard, in your experience, based on the data that you had looked at, what type or nature of measure would be harder to adjust to for an attacker, in your opinion?

MACIEJ KORCZYŃSKI So hi, Janos, and thanks for a great question. So I think that our study, INFERMAL study, shows, for example, huge correlation with the possibility of having access to API without restrictions. So this is quite important because imagine the situation when you have access to API, and with API you can, for example, create registrant accounts fully so you can streamline your operations. So this, I would say, is one of the most important results from INFERMAL itself, and also from our daily analysis of the data, we see huge campaigns. So that only supports this anecdotal evidence, but still

analysis of those campaigns clearly shows that this is important. That being said, also from our experience, I would say that attackers, it's not one thing, but it can be, I would say, a variety of things. So imagine I'm the attacker, I have unlimited access to stolen credit cards or let's say Bitcoin wallets. So for example, I will care much less about pricing itself, right? But I will care much more about having a possibility of a payment with Bitcoin, for example. And on the top of this, I'm very interested as an attacker to make big campaigns. So something like having access to API without too much verification would actually do the job for my particular case. And this is also something we show in INFERMAL. We show on one hand that, yes, pricing matters, discounts matter, but we also show the cases where domains are much more expensive, but they have very deceptive keywords in registered domain names. So this clearly shows anecdotally, but shows that there are attackers behind that care less about pricing, but they're willing to pay more to have deceptive keywords in their domain names. Thank you.

IAN SHELDON Thank you. In the interest of time, I might take the next two questions together and see if we can get a consolidated answer as well. So, with that, I might give the floor to Wang Lang, and then Sushil.

WANG LANG Thank you, Ian. I have a question to ask Maciej. Forgive me for the poor pronunciation, the author of INFERMAL study. Before we take

some measures, do we need to distinguish the difference between the malicious domain and the compromised domain? And how do we address them differently? Thank you.

IAN SHELDON: Thank you. Sushil.

SUSHIL PAL: Sushil from India for record. I don't have a question. I'll just have a couple of points to make. First of all, I think it's important to distinguish between reducing the timeline and making it simultaneous or concurrent, and therefore we would support and repeat the GAC communiqué which was made during Seville, Dublin, and Mumbai. That's one, and I tell you why it is. It's also important in view, as was mentioned by our China colleague, we need to examine the malicious domains, right? And recently, GAC Secretariat has also shared a report which has been published in the Oxford Journal of Cybersecurity, which has examined only malicious domains, and the data it throws, it completely supports this logic. The Oxford study has actually examined about 1, 600-odd domains from 190 top TLDs for more than 200 registrars and found that 90% of those malicious domains, they survived only for two days. The median life of such malicious domains is one day, and we on our own did independent research as well, and we have also found a similar number. So I think it's important to note that.

And therefore, the second thing, I think I completely take the point from our INFERMAL colleague who made this study. First of all, no study will be comprehensive because we don't have complete DNS abuse data. The DNS abuse is not mandatory for registrars to report that, right? So whatever study you do, it would only give you any analysis based upon the sample set. Right? And therefore, however, it's important to note the negative correlation which has been inferred by INFERMAL studies and multiple ICANN research studies have shown that. So, I think we completely, negative study of about 70%, negative correlation and leading up to about 70% reduction in the DNS abuse, that should give us enough confidence that the rationale exists. However, it might have some difficulty for registrars to adjust the process. We completely appreciate that point, right? And as regards to the concerns of the users, which some of users might have a difficulty, we haven't heard this from the users per se. I think we are hearing it more from the registrars than the users. And business community group or the brand owners or community at large, I think they have never raised any such concerns. And although with the GAC interaction with the RrSG, Registrar Stakeholder Group, we thought we have some positive things to look at. It might be that registrars might agree for new TLDs, keeping in view the new round coming up and the potential it has for rampant DNS abuse. I think we continue to look forward to the Registrar Stakeholder Group consensus at least for the new TLDs. Thank you.

IAN SHELDON: Thank you. Could I beg two additional minutes for our translators' time just to wrap up? Would that be acceptable? Okay. Thank you. Would you like to touch on very briefly and then we'll need to wrap up? Thanks.

MACIEJ KORCZYŃSKI: Yeah, I would love to. Thank you so much for two questions. I will maybe start with the second one, or comment. I'm not sure which ICANN research you're referring to. I think because the INFERMAL was with OCTO, so there is, I think, one, there is this study that looked into-

SUSHIL PAL: This was Oxford study reported in the Journal of Cybersecurity.

MACIEJ KORCZYŃSKI: Sure. So you mentioned there that the lifetime of domain names is two days, right?

SUSHIL PAL: 90% of domains, they were live only for two days, and the median life of such, and mind you, this is the study only about the malicious domains, not in general.

MACIEJ KORCZYŃSKI: Ah, okay.

SUSHIL PAL So we need to examine only the malicious domains and nothing else.

IAN SHELDON Sorry. If there's an exchange, we can take that after this session, and we can talk about journal studies and-

MACIEJ KORCZYŃSKI Just one comment on this.

IAN SHELDON Yeah, please.

MACIEJ KORCZYŃSKI Just one comment. So we see a lot of domains that are used straight after registration. We see a lot of domains that are aged to get their reputation. We also see campaigns that keep domains registered for one year, and they start using them just before expiration. So there is a great variety of results, and definitely, the lifetime can be two days. But when the attack starts, the attack can start straight after registration. It can start after two months, three months, five months. So this is slightly, I'm not sure if this is exactly the argument for 15 days verification. But definitely, the study, the two days activity, perhaps, but it depends when the attack starts. It can start after two months, three months, six months, and so on.

Thank you so much. But we can definitely discuss it further. Thank you.

IAN SHELDON: Thank you. That's all we have time for this session. Look, it does sound like this is something the committee may want to touch on in the communiqué. So what I will suggest is finding other GAC members who had made interventions and start having a discussion. Start that conversation now, work out what you're interested in, and start working out what that text looks like. And then we can touch on the communiqué drafting in sessions to come. So with that, thank you very much. Please join me in thanking our speakers today. Please be back in this room at 01:15 PM. Is that? I think that's about right. And I just also wanted to note that there is an African GAC coordination session on right now in the Lily meeting room. So, if you're interested in that, please head there as well. Thanks all.

[END OF TRANSCRIPTION]