ICANN82 | CF – Joint Meeting: GAC and SSAC
Sunday, March 09, 2025 – 16:30 to 17:30 PST

NICOLAS CABALLERO: Ladies and gentlemen, welcome back. We're about to start. Please take your seats. Julia, please go ahead with the recording.

GULTEN TEPE: Hello, and welcome to the ICANN82 GAC meeting with the SSAC session on Sunday, 9th of March at 1630 local time. Please note that the session is being recorded and is governed by the ICANN Expected Standards of Behavior and The ICANN Community Anti-Harassment Policy.

During this session, questions or comments submitted in the chat will be read aloud if put in the proper form. Please remember to state your name and the language you will speak in case you will be speaking a language other than English. Please speak clearly and at a reasonable pace to allow for accurate interpretation, and make sure to mute all other devices when you are speaking. You may access all available features for this session in the Zoom toolbar. With that, I will leave the floor to Nicolas Caballero, GAC Chair. Thank you. Over to you, Nico.

NICOLAS CABALLERO: Thank you very much, Gulten. Welcome, everyone, to the last but most important session, I would say, in my humble opinion, at

least, with the SSAC, the Security and Stability Advisory Committee. Welcome, Ram. Welcome to your fantastic team. As a matter of fact, we were talking about some of the issues we'll be talking about today, yesterday, and the day before yesterday. And when I mentioned quantum computing and its potential effect on DNS and DNS stability and DNSSEC implementation and so on, and cryptography in general, symmetric and asymmetric, everybody looked at me as if I were crazy, which might be the case. But anyways, we'll be talking about that in depth with this team of experts. We'll touch upon quantum computing and its impact on encryption, as I mentioned yesterday.

Then we'll have a discussion on Infermal. For the benefit of the 60 new GAC members, I already explained what Infermal stands for. But we'll get to the details there. And then we'll discuss the next steps. So, welcome again, Ram, and your fantastic team. The floor is yours.

RAM MOHAN Nico, thank you so much. And on behalf of the SSAC, I really extend our sincere gratitude to the GAC for this invitation. This is the third time we've been with you. And each time, the interactions have become richer and really much more engaging between us. So, we really value this opportunity to strengthen our collaborative dialogue on critical internet security and stability matters.

For those of you who are new to the GAC and to the ICANN community, just briefly, the SSAC serves as ICANN's expert advisory body. It's dedicated to identifying and analyzing potential threats

to the internet's naming and addressing systems. The SSAC is comprised of seasoned technical professionals. And we provide objective, evidence-based recommendations to the ICANN community and Board.

There are times when we don't provide evidence-based recommendations. And in those cases, we do try to point out that those are expert opinions that we are presenting to the community and to the Board. Our focus spans a wide spectrum from DNS vulnerabilities and cybersecurity risks to the impact of new technologies on internet infrastructure to the security and stability and resiliency aspects of internet governance. So, we span that entire piece. But fundamentally, our remit is inside of the critical infrastructure area. And we are engaged in that area.

Now, we understand that the GAC's vital role in representing governmental perspectives on internet governance, among other things. And this interaction, Nico, this interaction really allows us from the SSAC to bridge the technical and policy domains and really our desire and our keenness to continue this engagement is to ensure that our recommendations are both robust and are aligned with public interest. So, that's a key focus of what we are doing. And we're eager to share our insights, to listen to your concerns, and together contribute to a secure, stable, and resilient internet.

So, that's really a key driver for what we do and why we really cherish this interaction with the GAC. So, thank you for that. As you'd already mentioned, we have really two key topics that we

wanted to discuss with you. Russ Housley is here on my right. And Russ has a long and distinguished career. And among other things, he has been spending quite a bit of time looking at quantum computing and its impact on encryption. So, we figured we'd have Russ here to share his thoughts on this topic. Our intention is not to lecture you. Our intention is to share really what our thinking is where we are, and then really ask you to engage with us, to come in and chat with us.

We try as much as we can to not make our presentations extremely technical, even though the material underneath is very technical. So, that's kind of our goal. So, if we veer into solely geek speak, just speak up and say, hey, what does that mean? We're happy to kind of translate that. So, with that, over to you, Russ.

RUSS HOUSLEY Thank you, Ram. So, I put the lead right on the title slide. Nobody knows the answer yet. Quantum computing has been coming along for a while. And the National Institute of Standards and Technology did a big competition. And the solution that came out of that is called ML-DSA. It's a lattice-based digital signature algorithm. And the solution just does not fit well with DNSSEC. It's just too bleeping big. It has very large public keys and very large signature values, and so if you're using DNS over UDP, it doesn't fit. It's just that simple.

And so, the good news about that is, though, that we have a good bit of time. Because the biggest concern with the quantum computer is what we call the harvest now, decrypt later attack. And

so, the concern there is, if you have a bunch of secrets and the attacker records them and saves them until they do have a cryptographically relevant quantum computer, then they can attack the key management with the quantum computer, get the keys, and decrypt the secrets. In the DNS, there are no secrets, so that's not a problem. What our concern is here is that we have a digital signature that cannot be forged in time when we get to needing to mitigate the existence of a quantum computer.

So, the second slide I have talks about maybe the things that we can do to apply these quantum digital signatures. So, this is the research that is underway. The Internet Research Task Force has a group looking at post-quantum DNSSEC. It has a side meeting next week. Merkle hash trees seem to be the basis of the answer. They're the answer to so many things, including blockchain and certificate transparency and a whole bunch of other technologies. So, maybe it's not a surprise that they're the basis here. But I put a couple links here on the slide.

One talks about how stateful hash-based signatures could be applicable, that those signatures also are large, and so they're looking at other techniques. Anyway, there's going to be a lot of discussion next week at IETF 122 to explore these further. But I don't expect an answer a year from now. But we have time. And so, if you have questions about this, or we hold them to the end, or you want to do them now? OK, if you have questions, I'd be thrilled to answer.

NICOLAS CABALLERO Thank you. Thank you so much. The floor is open for questions. I would like you to explain, for the benefit, again, of the full GAC, what digital signatures, the vanilla version, of what digital signatures are, please.

RUSS HOUSLEY Sure. A digital signature is the thing that DNSSEC rests on. And the idea is that when you get the response to your query, the digital signature is attached to it. And it means that it has not been changed since it was originally posted. So, it's the thing that provides the integrity and the authentication of the data itself.

NICOLAS CABALLERO Thank you so much. I have Netherlands.

MARCO HOGEWONING Thank you, Mr. Chairman. For the record, this is Marco from Netherlands. And thank you for this very brief but in-depth overview. I agree. There's still a long way to go. Yet, I am a government. And I know that a long span is often shorter than you think. Without going into too many technical details, is there any concrete advice you would give to us governments right now? And what can we do to prepare for what will probably be the inevitable point where we have to change the DNSSEC algorithm?

RUSS HOUSLEY It's too soon for DNSSEC. Other security protocols, we have solutions. We have work in other IETF Working Groups, such as

LAMPS, which is working on PKI and SMIME. We have TLS. And we have IPSEC in those three areas. I'm sorry, and Secure Shell. In those four areas, we have solutions where the infrastructure needs to be deployed now so that when we need it, it's there. Because it's going to take a few years.

If you look back at the transition from SHA-1 to SHA-256, I was the security area director of the IETF at that time, and I thought five years would be plenty of time. And it took more than twice that. So, start on the infrastructure so that the transition can happen, because a bunch of things later cannot happen if there's no infrastructure to tie them to. That's my advice.

NICOLAS CABALLERO Steve, go ahead, please.

STEVE CROCKER Thank you. Russ, it would probably be good to follow up on that question, which makes a lot of sense coming from a government saying, what are we going to do? You alluded to a prior transition from SHA-1 to SHA-256. Can you say something about what the transition will look like at the time when there is a decision about what the new algorithm will look like? Will switching to that new algorithm be qualitatively different from any of the algorithm shifts that we have already had and are going to have along the way, or is it sort of another algorithm shift for which we already have some practice and experience?

RUSS HOUSLEY So, thank you, Steve. We don't know for sure is the answer, but we do know that this one is more complicated, because we're not just changing one of the pieces in a gearbox. We're throwing the whole gearbox out and putting a new one in. So, I think in that situation, you've got to think of, if you were to think about a PKI, you're talking about building a new one from the root all the way down. You're not just changing parts of it. I hope that helped. No? Sorry.

NICOLAS CABALLERO Thank you, Steve, for the question. Thank you, Russ. Any other question or comment? I do have a question for you, Russ. Let's say government X has a very good implementation of DNSSEC and MANRS and RPKI and so on and so forth. Any combination of Blowfish and RSA and, I don't know, DES or whatever, SHA-256 or any combination, and then all of a sudden, there's a quantum computing breakthrough. Correct me if I'm wrong, but in that case, that government, the DNSSEC infrastructure would be automatically obsolete. Am I correct?

RUSS HOUSLEY Yes. However, it's not clear you'll know when that's going to happen. There's a lot of literature we're seeing about advances in the number of qubits and the size of a quantum computer. But so far, we're nowhere close to something that's cryptographically relevant. And these things are not linear.

Advances occur in leaps and spurts. And so, when it happens, we will not necessarily get a lot of warning, which is the point of starting now answer that I gave the earlier person. But RPKI and DNSSEC are unique in that they only have the need for integrity. There is no issue there where there's secrets to harvest. So, we have more time there because there's no record now, harvest later, or harvest now, decrypt later type concern.

NICOLAS CABALLERO: So, we should be fine with a nice combination of DNSSEC, RPKI, and MANRS

RUSS HOUSLEY: Right. We just have more time on those problems because they only deal with public data and providing integrity for it.

NICOLAS CABALLERO: Thank you, Russ. I have Australia and Netherlands. Australia, please go ahead.

INGRAM NIBLOCK: Hi there. Ingram Niblock for Australia. I know that they serve different purposes. But I was just wondering if you could comment on the role of DNS over HTTPS and DNS over TLS. Obviously, one's signing and one's transport security. But will it be easier to implement the post-quantum encryption, the new algorithms in the transport security things, and will that provide any of the

benefits we currently get from DNSSEC by virtue of it being encrypted in transport as well?

RUSS HOUSLEY

So, yes and no. Yes, they will protect the traffic between the point of encryption and the point of decryption. It's a hop-by-hop system when you apply it to the DNS like that. So, that will provide protection there. And as I said, the work on TLS is underway. We don't yet have the PKI for it to glue to. By the way, the CA browser forum is getting the week after the IETF in Tokyo to talk about that exact topic. So, I hope that helped.

NICOLAS CABALLERO

Thank you, Australia. Thank you, Russ, just again for the benefit of the newer members of the GAC, PKI stands for Public Key Infrastructure, and MANRS for Mutually Agreed Norms for Routing Security. Anyways, we can provide the links and everything. I have the Netherlands and then the gentleman over there. Sorry, I don't know your name, but Netherlands first.

MARCO HOGEWONING

Thank you, Mr. Chairman. It's Marco again. Taking a slight sidestep and well, maybe the devil's advert also trying to avoid this becoming too much of a technical discussion. But on your previous slide, you mentioned the challenges you have with UDP transport. And I recall this is not the first time within the DNS industry we run into particular limits with UDP as a transport.

	I believe it also plays a role in the current DNSSEC implementations with regard to key length. I wonder, and a bit in line with what my Australian colleague just asked, given that we are looking at the long-term horizon, would it be conceivable to consider different transport options for DNS other than UDP?
RUSS HOUSLEY	So, other transport options are well understood and specified, they just aren't well deployed. So, as part of this transition, maybe they will be.
MARCO HOGEWONING	That again borrows the question, we're the governments, how can we help?
RUSS HOUSLEY	Fair enough.
NICOLAS CABALLERO	Ross, on that point, could you give two or three examples?
RUSS HOUSLEY	Two or three examples?
NICOLAS CABALLERO	For substituting UDP, I mean.

RUSS HOUSLEY So, DNS over TCP, DNS over QUIC, these are DNS over TLS. These are examples of ones that do not have the same per-message limitations.

NICOLAS CABALLERO Thank you very much. Netherlands?

PETER THOMASSEN Please go ahead. Hello, this is Peter Thomassen. I'm also an SSAC member, and I felt like some of the things that have been said, I think, can be also restated a little less technical. So, that's what I'm trying to do. So, Ross said earlier that the signatures are attached to DNS responses, and they testify that the DNS information hasn't been changed since it was posted. Now, of course, if everybody could just attach a signature, that would not be very useful.

So, to attach a signature, you actually need to have control of a private key, and you need that to compute the signature. And so, the threat from quantum computers is about extracting that key somehow, even if you would not be authorized to have it, and then you could fake those signatures.

Now, another application of cryptography is encryption, which is protecting secret data and make it unreadable unless you have the decryption key. So, that is also an application of keys. And it's important to recognize that quantum computing threatens both applications, both the computation of signatures with the secret keys and also encryption decryption. But those are different use cases, and the DNS is not concerned with encryption and

decryption. It is concerned with checking at the time when you try to connect somewhere and make a DNS query, whether that signature that you get is currently valid.

So, if you would want to break that with a quantum computer, you would have to kind of do that in a very short amount of time, almost near real time, whereas if you have recorded encrypted information from like an HTTPS transfer in the past, you could take like five years to decrypt that if you want. So, if you have a useful but slow quantum computer, it'll threaten your encrypted data, but it will not be threatening at that time your DNSSEC information, because if it takes five years to fake the signature, by that time nobody's interested in the DNS response anymore, right? Because your connection takes only a few seconds.

So, the bottom line is that, like what governments could do now, which is I think the question the Netherlands asked, about the DNSSEC question, don't freak out. It's currently a research problem. It's a good idea to follow that, I suppose, if you're interested. But the more immediate problem is certainly protecting stored or in transit secret data, which has the same kind of key extraction problems, but it's much more urgent and there's also more progress there already than there is in the DNSSEC field. Yeah, so that was the summary that I wanted to make.

NICOLAS CABALLERO Thank you so much.

RUSS HOUSLEY And thank you for chairing the session next week.

RAM MOHAN Thank you, Nico. One thing that I'd like to offer to you, Nico, and the GAC, is if some kind of a ready reckoner, a primer of some sort, in this area would be useful, please write us and we can help provide some material for you that perhaps might be useful to your members when you work with your governments. That would be, because I think there is a useful distinction to understand and to transmit to others in your governments about what is the downside with quantum and DNSSEC versus the downside with quantum and shared secrets.

NICOLAS CABALLERO Thank you so much for that. Ram, and thank you, Russ. I'm not sure, I'm not entirely sure about that five-year timeframe you mentioned. I forgot his name. Peter, but thank you for the explanation. I really think we might, hopefully not, but we might have surprises in the near future. But anyways, before I give the floor to Jeff, do we have any other questions in the room or online? And I don't see any hand up. So, thank you so much, Russ. So, let's move on. And at this point, I'll give the floor to Jeff, all yours.

JEFF BEDSER Thank you, Nico. Jeff Bedser with SSAC. The question was posed to discuss the INFERMAL study, the INFERMAL Study. Next slide, please. Thank you. The INFERMAL Study is one put together by the OCTO, the Office of the CTO for ICANN, from their research

component. They have academic researchers who are really looking into malicious registrations when it came to domains used for online harms and abuses, primarily phishing.

And one of the first things to caution, and I put it in bold in the second paragraph there, is this is not a report that offers solutions, but it's a report that is designed to answer questions that have been asked by the community for quite some time about the influences of certain factors toward where the cyber criminals obtain their domains for these abusive purposes. The report highlights economic incentives, proactive verification, and some stringent restrictions in mitigating domain abuse as a state of the art as of the report's issuance last November.

So, some of the key findings, for those of you that haven't read the report, the economic incentives is that lower registration fees, each dollar in reduction in fees corresponded to a 49% increase in malicious domains, that free services or the availability of such, as such as web hosting, does drive up abuse rates by 88%. Discounts on domain registrations are associated with a significant increase in malicious registrations. And in regards to proactive measures, stringent restrictions on those buying domains can reduce abuse by 63%.

API access, which is the ability to do large volumes of bulk acquisitions of domain names at one time, can account for up to a 401% rise in malicious domains being registered, and of course, the verification practices, the proactive verification of registrant

information such as email and phone number validation significantly reduces malicious registrations. Next slide, please.

Reactive measures, mitigation times, the impact of mitigation times on reducing domain abuse is minimal. Even brief uptimes can provide attackers with valuable credentials and financial gain. And then registrar and TLD preferences, concentrations of abuse, malicious registrations are not uniformly distributed and tend to be concentrated in certain registrars and TLDs, and that registrar practices, such as those offering low prices and free services, are more likely to attract malicious registrations.

So, this is information that is validated, some well understood in the anti-abuse communities for quite some time. The issue simply is, is that it's calling out economics. Buyers go to the cheapest price. Buyers go to places where they can buy bulk. I think in most countries of the world right now, there are larger entities that sell in bulk for all types of products and goods and sell at the lowest price. So, while this is a legitimate read of the data, it's not necessarily implied a resolution to the problem, because if you bring the floor of the price up, you still have a lowest price. Unless you price fix across the planet with all the different economies and different currencies, you're not going to eliminate that problem.

Additionally, the cybercrime losses, I've seen numbers from $1 trillion annually in cybercrime losses to $10 trillion annually in cybercrime losses. And I do understand there's a zero missing in there between the two numbers, but I can't even conceive a trillion dollars. So, the difference between $1 trillion and $10 trillion, as far

as the losses, it's a very big number. Most of the studies show that globally, the average loss per phish per victim is $136 globally. However, in the United States, that number jumps up to the average loss per phish being $3,500.

I've seen variants of all those numbers, and I'm sure most people that are involved in anti-abuse work know these numbers vary depending on which study and such. But the reality simply is that if each loss at minimum represents $136, what price do you have to charge for a domain that makes it economically not viable to buy a domain to use it for harms when you're making significant amounts of money in cybercrime? So, it's something to consider, because we're looking at what policies, what changes to mitigate or to reduce the problem of malicious registrations to be used for cybercrime and for harming people and stealing money from them.

Is changing the price going to change the incentive of the criminal to make hundreds of thousands of dollars if the domain goes from $2 to $10 a year? So, I posed that as a question. So, the verification process, again, as I pointed out, the study was published in November, and it was based on data at the time. And AI issues, Artificial Intelligence issues, continue to accelerate at a pace that apparently is exceeding the pace that quantum is moving.

But the ability now to create digitally generated identities where you can take someone's real name, say to an AI algorithm, I need a driver's license from this particular region of this particular country, exact format, but I need a name from a real person there who's in this age demographic and has a photo that looks like mine,

or put my photo on it, to be able to digitally generate an identity that then can be used in a process to register a domain, this has really significantly impacted the ability to say, well, if they would just check the ID of every registrant, they could solve this problem.

The ability to detect a fake from a real, when it's a real person with the wrong photo or a similar photo, gets to be at a level that, well, you're going to be needing to use AI to fight, because a human can't do that at that level at the speed it's necessary. So, what better processes will assist in keeping domains from being registered fraudulently other than manual verification processes?

There's also the issue of the rates of detection from delegation to mitigation. Is that a valid measurement? And what I'm suggesting here is that most of the studies done use the publicly available sources on DNS Abuse volumes. And don't get me wrong, there's significant volumes of those volumes, and they are all shocking numbers. But I would pose that the biggest problem with DNS Abuse and phishing in particular is that it's reliant on entities to see it, be victimized by it or attempted to victimize them and report it.

So, we're looking at right now in most of the reports, the reports that are generated on this topic, we're looking at reported harms. How many of you in this room have received a phish or a smish on your phone or your email that you looked at it, said, you didn't get me this time, and you deleted it? If anyone in this room hasn't done that and always reports them, I commend you. But I don't expect a show of hands. A significant volume of these harms is unreported.

And if they're unreported, they're invisible to the industry to mitigate them.

So, changing the methodologies for registering is a potential solution or a path to follow, but also better opportunities for detection so they can be mitigated quickly so that a domain goes up for six, seven seconds, is caught and killed versus it goes up for two days, somebody reports it, it takes two days to validate, and it gets taken down. How many victims were there between that four-day period versus if we can do better detection to kill them a lot faster? And then, honestly, the other point for measurement, and it's something that's very difficult to measure, I'm not throwing this out there as well, we should be doing this already, but number of victims per domain, because you can have a hundred victims in a second for a well-done phish.

So, it's not necessarily the number of domains doing the phishing, it's the number of victims who are falling for it that really can measure the scale of the problem, because we already know that the volume, even at the top of the iceberg we're talking about, which is the publicly available source to tell us about phishing, has millions upon millions of domains being used, and we can all acknowledge there's plenty more that's not being reported so we don't see it, but we're also not looking at the true impact of how many victims per, and how really the impact of that is financially to the citizens of the planet.

So, I put those out as further discussion points and talking points, because what the INFERMAL report has given us is a good

validation that, yes, we've always known that low prices drive that type of business, we've known that bad validation and verification of your registrants drives that traffic. Echo added for effect. But now, how do we take the next steps? How do we take this and go better? What can we do to better measure the impact and also look to how can we better detect so that we can be more effective at stopping this problem?

Because I would venture that even if we start charging $1,000 per domain per year, what we're really doing is taking out most of people's around the planet's ability to register a domain because of the cost, but we haven't changed anything for the cyber criminals who are going to make $20,000 minimum per domain for the losses they're going to take on people, so they're not going to mind that cost increase. It's going to cut their margins slightly, so we have to find other solutions here. So, thank you.

NICOLAS CABALLERO Thank you, Jeff. Can we, all right, yeah, that was precisely my point. Next slide, yeah. The 400% increase, I would love to have that discussion now, and the API thing Application Programming Interface, what is your opinion in that regard? Is that really the problem, that the bad guys have access to the API, and by using, I don't know, artificial intelligence or whatever, they're more capable of causing damage and increase the phishing activities? Would that be the case?

JEFF BEDSER

So, Nico, I don't have a doubt for a moment that bulk registration is a bad vehicle for large acquisition of domains for abuse. However, the metric of the 400%, 401%, excuse me, one bad actor who's registering DGAs or domain generation algorithm domains for a botnet or for a malware campaign could be registering 10,000 domains at one time, and that doesn't make the API bad because the percentage based on the API could be one user out of all the users who use the API. On the other side of that, should there be a breaks, if you will, that once someone registers 50 domains, there's a pause to make sure, are those domains being registered, look like they're going to be used for something bad, and there's plenty of infrastructure information you can use to look and see if they're being set up to be used that way.

So, yeah, 10,000 domains at a time, I think the easy answer is, yeah, that should not be available, but the API itself should not be available, and that's not the problem. It's the unrestricted access to an API that's the problem.

NICOLAS CABALLERO

Thank you, Jeff. So, let me open the floor at this point for comments or questions from GAC members in the room or online. The floor is open, and I don't see any hand in the room. I'm sorry, sorry, sorry, yeah, there are two hands. I have India and Australia. Please go ahead, India. Thank you.

SUSHIL PAL

Thank you, Jeff. So, I think it's clear that the verification is an issue, right? I think if we have the verified credentials of the registrars, I think the likelihood of DNS Abuse or significance goes down, right? And that's also reflected in the use of the, I think, DGS algorithm wherein it's not AI which is the problem. It's because, you know, unverified credentials through these, you know, I mean, they get shared through the bulk APIs, right?

Somehow, I think maybe, although the problem is very clear, but still, we are weighing on with the GNSO as to how to define the accuracy of the data, what is the scope of the data, because once, if we do not freeze this scope of the, scoping of the, WHOIS data accuracy, I think you can never go to the verification aspect, right? So, can the GAC or the SSAC, I think, can you guys also impress upon the GNSO for expediting these things? I mean, because otherwise, you know, we're all discussing, we all know the problem, but we're not making any significant step forward, you know, to contain this.

JEFF BEDSER

So, one thing that I didn't say during the presentation, which I should probably make very clear, is that the people we're fighting in this, the people that are using domains for this purpose, are 10 steps ahead of us, 100 steps ahead of us. A recent trend has been that legitimate people with legitimate credentials will create an account and slowly over a couple of months, build up a portfolio of domains, and then they will simply sell that portfolio of domains

with the credentials to a criminal, who then uses those domains for a purpose.

So, while better frictions implied with better credential validation or verification is certainly helpful, my point is that leaning heavily on that as a solution is, right, is problematic. The other real concern is that this is a public session, and I guarantee that the people we're fighting against here are going to watch this recording and see, what do we know? What do we already know about what their tactics are and what they're doing, so they can decide what the next steps they're going to take.

So, your question about taking it to the right groups, what's next? I do believe it goes back to the point that I made earlier, which is, you know, I think go back to on the prior points, on the prior slide, which was, it needs to be about better detection. Better detection will, and acceleration of the mitigation processes is really where the focus has to go, because we're not going to remove the economic incentive to steal from people. People have been trying to move the economic incentives for crime for all of human history, and there's no success really in that yet.

Crime always exists, but if we can basically figure out a way that you do it, you get caught, it gets stopped before you can victimize, or at least minimize the victimization per the incentives to do the crime goes away, because there's better crimes that are more profitable. So, I don't know if that's a good point, either, that I'm saying, have them do some other type of crime, but the point being, of course,

that if you're looking to better detection and better mitigation rates will really help these problems.

SUSHIL PAL

I mean, not to take away the point that the better detection is definitely, you know, I mean, that's the end goal, I think, and when I say verification, I'm not saying that it's a be-all and end-all, but that's the first step, right? And I'm just, even we've not taken, I mean, we are talking and talking, but we're not taking an effective step, even to reach anywhere in the verification process as of now, especially in the gTLDs, right? We don't have any problem in the ccTLDs which we operate.

I think I can share from the experience of my own country that, you know, we have enforced in the two-factor verification process, and the number of abusers have significantly gone down, significantly gone down. I wish the same things can be replicated. It's a bit of cost, definitely, to the registrars, but then it's a huge cost, which we are paying because of these cyberattacks, which none of us realize because it doesn't tend to, you know, it doesn't pinch us. It does pinch our citizen, but, I mean, whom we represent, but it's important for us to recognize that that's the first step. Let's take the first step and not to undermine the importance of the detection and acquiring capabilities to monitor them.

NICOLAS CABALLERO Thank you very much. India, I have Australia, the European Commission, the United Kingdom, and the Netherlands. So, let's go ahead with Australia.

INGRAM NIBLOCK Hi, Ingram Niblock for Australia. I was just wondering about the sort of next steps with the INFERMAL research itself. There's the obvious limitation that's spelled out in the report that this isn't what criminals did. It's just the features of a registrar they were looking at. But I was wondering, is there any effort to, I guess, validate the hypotheses with the registrars and actually go and say, because you have particular domains that they had on their block list that they used for the research what did, like at scale to get some usable data, like what did the people doing the abuse in those particular instances actually use based on presumably the data that the registrar presumably has. Is that sort of, yeah, I was just wondering about the next steps for the actual research itself.

JEFF BEDSER Yeah, I'll have to refer you to the office of the CTO for those questions, as I know the authors of the report and their next steps. At best, I could give you hearsay from conversations. That's probably not the appropriate answer to give you. So, yeah.

NICOLAS CABALLERO Thank you, Australia. European Commission?

GEMMA CAROLILLO

Thank you very much, Nico. Gemma Carolillo for the European Commission. My colleague Martina Barbero is the topic lead on DNS Abuse, already referred to this in the chat. So, we are going to have a presentation of the report in the DNS Abuse session with OCTO also intervening, so we might just revert some of the questions to them. But I have two questions.

One more general is that since this INFERMAL report got a lot of echoes and we are hearing some of your remarks on some aspects, did you have some, like, statement of comments to the report, which we could access and see specifically what the abuse or certain points of the reports are, because this would also help us in the reading of the document. And second, I understand that, I mean, of course, API is not a problem per se, but this is for anything in technology. So, but then since bulk registration seems to be a problem, what is the takeaway for us is that there should be restrictions to the use of API, but is it possible that we entertain as a practice vis-a-vis the bulk registrations? Thank you.

JEFF BEDSER

So, to the answer to the first part, no, these talking points and comments do not come from a consensus document from SSAC at this point, though we can basically take it back as leadership to see if we can get consensus on a statement on a document that we can read on INFERMAL and what we think next steps should be, that certainly seems to be something worthy to follow up on. I'm sorry, the second question has now slipped out of my head.

So, personally, I think that I can envision opportunities where a corporation is establishing a new brand or a new company identity, and they might need to register that same identity across many TLDs, and it could be 2,000 registrations at that time, that those tools would be a valid purpose like that. But I have a hard time seeing anything higher than that as being a reasonable volume for bulk registrations. But there could be business cases I'm not aware of. But I think that, for example, to the gentleman from India's point, before you put a-, all right, I'm going to use it, there are rules to get a license to drive a motorcycle.

There are rules to get a license to drive an automobile, and there are different rules to drive a semi-truck. You've got to get different licensing based on your ability to hurt other people operating that vehicle poorly. If this vehicle needs to be utilized and available to people, then I would consider the API at volume to be a tool that is much more like a semi-truck or a train operator where you actually have to go through much more vigorous validation of who you are and your business purposes before you can have access to it. Then it's not a problem of the tool, it's a problem of who is licensed to use that type of tool.

NICOLAS CABALLERO Thank you very much. I have the U.K next.

NIGEL HICKSON Sorry, Nigel Hickson, UK. This has been incredibly interesting to put this important report in context, and thank the SSAC for looking

at this. We always knew you would. I just wondered whether, I mean, I know it's early days perhaps, but whether this might go on pursuant to your discussions to become some sort of recommendation or something given the importance of those recommendations that you issue from time to time. Thank you.

RAM MOHAN

Thank you, Nigel. We've not got to that point yet to define or decide whether we should make a recommendation on it. We've had OCTO present to the SSAC on this topic as well. But what we've not done is to look at this and say, is there something extra on top of it? Part of it comes from the fact that some of the work that may need to happen here may fall more in the policy development part of ICANN rather than the technical advice part of ICANN.

The INFERMAL report has provided quite a bit of technical advice. But those are just my thoughts, but we've not had a specific discussion inside of the SSAC. But thank you for the suggestion there, and we'll bring it up at our next conversation inside the SSAC to see, you know, what the mood of the members are.

NICOLAS CABALLERO

Thank you. Ram, I have the Netherlands next. Thank you.

MARCO HOGEWONING

Picking up on the Netherlands again. Marco for the record. Ram, you make an excellent point there. I do believe that in terms of mitigation, this is largely a policy problem. Yet I also hear Jeff

speak about improving detection and improving on, for instance, API. So, I wonder, outside of the policy discussions to have, is there a room, for instance, for technical standards to be improved on detection or on API behavior to solve part of this problem? Is there a space for technical solutions?

RAM MOHAN

Thanks. I'll speak briefly to it, and Jeff, perhaps you can also jump in. I don't know that there is a technical solution necessarily, but I think there is an education component of it. When you get phished, when you get smashed, do you know what to do? Not just do you know how to detect it, but do you know how to report it?

Because one of the problems at this point, certainly inside of our community, is if it is not reported, then you don't have enough data collected to say there were 1,000 cases that were reported, another 1,000 cases, 10% of it was not responded to in a certain way, and then let's look at that 10 percent, or whatever the percent, let's look at who is behind that and see what the patterns are to try and understand what some of the behavior and the characteristics might be inside of our ecosystem.

So, a practical thing to do is to really build a strong education campaign that says report the abuse, report the phishing, report those issues. Then once that is done, then let's go track what is happening downstream from that. We can then have data that can provide real focus on where the problem spaces might be, or who might be contributing to problems.

Right now, we are in, I think, a mode where we often are trying to apply a broad-brush approach to this and say let's create a new policy that applies to everybody, or let's paint all of a certain group of actors in a particular light, when you may have actors inside of that group who are doing a brilliant job and others who are doing an abysmal one.

And our focus, I think, ought to be on the ones who are not up to the mark. And once we have that data, then we can say here are best practices, here are the norms that ought to be followed, right? And I think the best practices can be done without Policy Development, because then you are saying this is just obviously a good thing for better hygiene, for a better ecosystem. Nothing to add.

NICOLAS CABALLERO Thank you. Ram, I have the Dominican Republic next.

AMPARO ARANGO Well, this is an important panel. The representative from the Dominican Republic is speaking. This is very technical, but I think it's the heart of what we're facing today in our countries. And I'd like to see here, as a government in a small country, as we are, which is the Dominican Republic, at the end, you did mention what we have to sue, what we have to do as a government.

First, we need to know what is the situation in our countries, in our own administrators of domains, the operators. I come as a regulator from telecommunications, from our operators, from all

our cybersecurity centers, our response centers with regards to the attacks, because in the last few years, Costa Rica, for example, two years ago, just went through a bad situation that cost them millions and millions of dollars until it disrupted their health system.

So, it's a little bit from a perspective as a government, and maybe on your behalf, you can't say it that clearly, but I think we need strategies. Some clear orientation as far as how to promote the DNSSEC in our countries. How many people know about this, whether it be our operators, our security centers, our own registries. I don't know if my country has it or not. But how can we attack this problem of insecurity and cybersecurity, which is something big for us? I'd like to hear maybe some kind of recommendation from you, but I think this has to be from SSAC and from GAC, because in the long run, this has to be turned into concrete tools, because it has to do with education.

It's costly to have a national strategy so that we can have all our systems regulated within the DNSSEC. I don't know if this is a question you can answer, but it's really frustrating. And I think we do have tools so that we can at least mitigate these impacts. Thank you.

RAM MOHAN One of the challenges that we have in the SSAC is that we can provide a great deal of technical expertise and technical information. What we do not understand fully well and do not have is what your needs are, and at what level do you need information to be provided, right? So, I think we need to collaborate, so that we

can understand what is the kind of information you would like for us to provide.

One of the things that we have started to do, it used to be that we would do the work and then we would publish reports, very technical reports that would go anywhere from 10 pages to 40 pages long. And one of the things that we've started to do is to distill those reports into 500,000-word summaries that provide kind of an executive briefing, if you will, of the crux of what we're trying to say in these papers. But that's still focused on our research areas, the things that we think are important needs.

So, what I encourage you to do, and you in specific, please come talk to us. We're happy to work directly with you. But the GAC in general, please work alongside us to provide us clarity on two things. One, the types of information that is useful for you. And then, two, the level of information you want, the level of technical detail you want. Because our default is to begin at a very deep technical level. So, that's what we are good at. But if you want us to go a level up or a couple levels up, speak with us and we can help you on that.

NICOLAS CABALLERO Thank you very much. Amparo, is that on all hand? Okay. So, we need to wrap up. We have one minute to go. Any final question or comment from the GAC? Japan. Go ahead, please.

UNKNOWN SPEAKER: Thank you very much for the presentation. I think that you've stressed the importance of collect the data about the phishing and some DNS Abuse. And I think that there is various type of DNS Abuse, not only the definition of ICANN, but also some other misuse like CSAM and maybe copyright infringement like in Japan, the manga piracy is a very big issue and very big economic growth. I think that the ground root problem is similar and I think that is it necessary to collect various type of abuse and abuse data and maybe there is some room to collaborate with the government to collect the data. But what do you think about it?

RAM MOHAN: I think it's an important topic and we are ready to stand alongside you to provide the technical details and the technical advice that can help on the collaboration side. But I think the eventual solution is probably going to be a combination of the governmental piece, the technical piece and the policy piece and finding a way to merge them together inside of this forum.

NICOLAS CABALLERO: Thank you so much, Ram. We need to wrap up. Thank you for your questions. It's been a fantastic session, Ram, as usual. It's a pleasure to have you here. Even though for some people these conversations are a little bit technical, but we try to convey the message. So, you do your best to give us some good advice on the one hand and on the other hand to help us fight the bad guys.

So, thank you again. Thank you so much. Thank you, Russ. Thank you. You have a fantastic team, Ram, and hopefully we'll be able to have another session in Prague. So, thank you so much. A big round of applause for our friends from the SSAC. Thank you very much. So, the session is adjourned. I'll see you tomorrow at 9 a.m. for the Welcome Ceremony and Community Excellence Award. Thank you so much. Have a good night.

[END OF TRANSCRIPTION]