ICANN86 Seville | PF – ALAC Open House
Tuesday, June 09, 2026 – 10:00 to 11:15 CEST

NATHALIE PEREGRINE

Hello and welcome to the ALAC Open House. My name is Nathalie Peregrine. I am the remote participation manager for this session. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior as well as the ICANN Community Anti-Harassment Policy.

During this session, questions and comments will be read aloud if submitted within the Q&A pod. Interpretation for this session will include English, French, and Spanish. If you would like to speak during this session, please raise your hand in Zoom. When called upon, virtual participants will be given permission to unmute in Zoom, on-site participants will use a physical microphone to speak.

Please state your name for the record, the language you will speak, if speaking a language other than English, and speak at a reasonable pace. I will now hand the floor over to Claire Craig, ALAC Vice Chair. Please go ahead, Claire.

CLAIRE CRAIG

Good morning to all of you in the room and good afternoon and good evening to those of you following this session online. Let me just first make an apology for Jonathan Zuck as he is unwell this morning and so I am in the hot seat. The objective of today's session is that we normally get requests from different

stakeholders to meet with us to share perspectives so that we can engage them on some of what is taking place.

And we will have that opportunity this morning as we hear from the RIPE NCC first, who will be speaking to us about their internet trust architecture. And we have with us Hisham Ibrahim. We then also have the Domain Name Registration for Cybercrime, and we have Greg Aaron and Karen Rose from Interisle.

And then finally we will have a conversation with Humberto Corrasco, who will be speaking to us about one of the grant projects, and that's Assistance for Domain Name Holders in the UDRP Proceedings. So, with that, I will turn the floor over to Hisham. Thank you.

HISHAM IBRAHIM: Good morning. Hello, everyone, and thank you for joining, whether on-site or online. My name is Hisham Ibrahim. I am the Chief Community Officer at the RIPE NCC. Can I please get the slides up? Oh, okay. It was a PDF, not a Word document. Sorry, just figuring out the slides for a second. Yes. Good morning again. Now with the slides on the screen. Well, they were.

Again, so while they're putting them up there, like I said, my name is Hisham Ibrahim and my title is Chief Community Officer, and a big part of the talk here is focused on that bit, community and what that actually means more than the RIPE NCC bit, which is, as many

of you might know, the RIR for Europe, Middle East and Central Asia. I'm honored to be invited to talk here to ALAC this morning.

This is an article that I wrote a while back titled The Internet's Trust Architecture. It's part of a series of articles that I was writing trying to examine what the internet actually means to have better understanding when there are policy discussions and such around that. So, what I usually start with is what is the internet. The internet is not social media. The internet is not the web. It's not applications that we use there.

It's not even digital economy or communication tools that we use on a daily basis. A lot of people use the internet as a shorthand for all of the above, but then that oversimplification of what the internet is collapses everything, every discussion into talking about how the internet works, rather than addressing the issue at the right level, be it platform, be it content or others.

What the internet really is, is something much deeper. It's a foundational network of distributed network of networks that are operated by separate and individual operators that have been interconnecting for the past 40 years. The internet is formed of, well, 80,000+ autonomous system numbers and networks that all interconnect to be able to push packets back and forth the globe. Next slide, please.

Now, with that in mind, the Internet basically was built on two core principles, the first being open standards and the use of open standards. Open standards allow us to use devices that come from

different manufacturers, different countries, and all be interoperable and allow us to be able to connect globally.

So, those open standards allow that interoperability on a global level. The second is the registration of internet identifiers, be it names, like what a lot of work here in ICANN and people do here, be it numbers, like what the five RIRs do in their communities, or ports.

Now, these registrations allow that uniqueness on the Internet. And those concepts of interoperability and global uniqueness are what makes the Internet what it is today. If you take one of these away from the Internet, it will no longer function. You cannot have two same IP addresses on the Internet. You cannot work with proprietary technologies and expect the rest of the world to seamlessly interoperate with you without having gateways and translators in the middle. Next slide, please.

And this is where talking about trust comes in play here, because, like I said, the Internet has 80,000 autonomous systems. There is no central command or control for the Internet. There is no entity that runs the Internet.

At one point in time, there are dependencies throughout how your packets travel around the world, which means you need to be able to trust that when you hand over your packet, when you hand over your traffic to another independently operating network, that they will follow certain norms and processes that you expect them to do.

And this definition of trust is one that I really like. It's from one of my favorite researchers on the topic, Rachel Buostman. She talks about trust being a confident relationship with the unknown. And basically, when we say the term, like, taking a leap of faith, what the image here illustrates is there's always going to be uncertainty underlying what you're trying to do, from what you know to what you don't know.

But then, as you build more trust capacity, that leap of faith becomes a lot more confident when you take that. Whereas, if that trust is not there, then you only perceive the risk of going from what you know to what you don't know. And that's very crucial to how the internet was built and designed from the beginning.

When the internet first took off 40-something years ago, everybody on the internet knew everyone. So, it was easier to have that trust. But whereas today, like I said, with 80-something thousand autonomous systems, with many actors with very different agendas on the internet, trust is something that is being challenged and we need to better understand that to be able to preserve what made the internet what it is today. Next slide please.

So yes, like I was saying, the internet's core has always depended on trust since the early days until today. It makes that coordination possible across these distributed actors, the different systems and such. You can see that in meetings like ICANN, for example, or the RIR meetings, where if you're a newcomer and you're first making your way around, you're still trying to see who shares similar

interests, aligns with what you're trying to do, or can help contribute to that.

You also see that, and that's more on the global level, you see that on regional and on national levels at network operator groups or IXP meetings, Internet Exchange Point meetings, or Internet Governance Forums, or others, where people come and exchange these thoughts and ideas for them to be able to come up with a shared understanding, shared way forward of what they consider to be the best thing they can do for keeping the Internet the way that it's currently operating.

So, bringing it back to the open standards and those uniquely identified networks and the community-led governance efforts around that, that's what builds that confidence in how the packets get exchanged around the world, how the Internet continues to work without a centralized command. Next slide, please.

So, again, I covered this a little bit when I was talking about trust. The Internet cannot develop without that trust. There is always going to be uncertainty. However, as we continue to build these shared norms and processes around it, there is less uncertainty and more certainty in how the process works, which makes this trust part of the actual Internet architecture that sustains it. Next slide.

So, yes, trust, confidence makes coordination possible even though uncertainty remains. And the point here being, what I mentioned, those national IGFs and NOGs and peering forums, those regional events, these global activities, these are all parts

that build these norms that create and generate more confidence. Next slide.

So, yes, you cannot take out community from the internet, from that kind of sustaining the commons of what the internet is, without compromising the architecture of what the internet is. Meetings like this, like the ALAC meeting, different forums, whether it brings together technical people, whether it brings together civil society, academia, media, others, all that have a vested interest in the internet, these are all part of that community that helps shape it and evolve it.

They develop the shared habits, norms, and leaderships that emerge. Then you begin to find, and we've all seen this before, where in different countries, you're usually looking for a champion to help move something forward, an agenda forward, be it technical, be it rights, be it something else, those local leaders emerge through stuff like this.

Again, ICANN has different programs like the fellowship program, like the NextGen program and others that allows for that kind of new blood to come into the community, for new leaders to come in and continue the efforts that are happening there.

Again, all tying it back to that concept of trust, if you take that away, if you stop, let's say, funding these fellows or stop doing these national activities or such, it does weaken the Internet, it does weaken the commons that sustain the Internet.

Next slide. Now, a lot of the work that my colleagues and I do ties back to development work. We serve a large part of the world in our service region where we have very different diverse communities. Some of the work that we do there is mostly on the engagement level and trying to understand what's happening, but big parts of our service region still require a lot of development work, and the next couple slides here map out some of the thinking and what we've seen over the past couple decades of how this works and how you can be very effective in making that impact that we would like to see in the world.

So, next slide, please. What I find over the years was that you can plot this very nicely across two different dimensions, one being that trust capacity, and that's the underlying confidence and knowledge and relationships and legitimacy that is built in these kinds of communities. It's the awareness, bringing new concepts forward, the technical know-how, training people on how to do something, local expertise, leadership and confidence.

The higher this is, the more you find that trust within that community and you get a sense of feel of it. If we had more people in the room here and maybe I just do this anyways, like how many of you are from a country or a region that does have well-organized structures around well technical civil um or any kind of groups that meet to talk about internet. How many of you have those in your countries?

Oh, I see some hands but not that many. But you do see that, right? You do see that countries, and the next slide is going to show a little bit more about that, you do see that that makes a big difference in the ability of a country, a region, a topic to move forward. The other dimension here is the execution conditions, right?

It's how welcoming the environment that you are operating is to adapting to new ideas and taking them on. So, institutional support, the prioritization of these topics, being able to self-organize infrastructure and such, all these resources, obviously, all these also impact the ability to affect that change. And if you can go to the next slide.

This is how you can easily illustrate that. So, starting from the bottom left quadrant, if the trust within the community, you don't have those connections within your local community or regional community, is low, and the execution conditions are quite low, then you find that you're dealing with an emerging community that still needs to better understand, have better awareness, have better technical know-how, but also needs work on those execution conditions to allow it to affect the change that it wants to do.

Now, if you move up vertically with the execution conditions, you would find different countries that are in the coalition phase of it, which is basically they have improved conditions, but the trust is still not there. You see these in countries that the government, for example, comes up and says, we want to move this agenda

forward. But then is there really in-country capacity and know-how to actually do this?

Do the operators trust each other to come together and make this happen? Does the community know each other well enough to effect that change? So, we do see these sometimes where you see these like big declarations of within the next, I don't know how many years we will be doing this. But when you go down to the ground and you talk to people, they have no idea how to get that done.

Now, if you go back to the bottom quadrant on the right, It's more constrained communities. It's the opposite of the one that we just described, where you do see a lot of people that have a lot of energy, a lot of know-how, a lot of willingness to make change. However, they do feel constrained because of regulations, because the conditions around them within their country or the region are just not there.

They don't have the funding, they don't have the resources, they don't have that. And then the top quadrant on the right there, which is the more mature communities, where you do see that strong capacity where people have that trust capacity, they know how to assemble, they know how to come together, and it's easy for them to effect change.

An example of that that comes to mind, a technical one with IPv6, a lot of countries have whether national IPv6 forums or platforms that they want to be talking about this, right? Belgium was a great

example of a community that knows each other. They came together, they sat down within a week or two, they enabled IPv6 and all of their stuff, and they just got it done. It didn't require a lot of noise or a lot of things.

It just made that happen because that maturity, that trust capacity was there and they were able to execute. Whereas others, like I said, you can have a big declaration that something's happening or people wanting to do something, but then restraints with resources or legislation or others.

So, mapping it around these elements allows my team and myself to actually work closer on understanding, do we need to be engaging sea level and talking to them about some of the constraints and what happens? Do we need to go with our technical training team to increase their awareness and the know-how? Do we need to find a mix of that?

Or do we need to just come in and begin to introduce topics? Or is it too elementary to a community that would then act, we know what we need to be doing, but we do not know how to move forward because we're stuck on a topic, right? Figuring that out makes the biggest difference if you want to make an impact in the world.

Next slide, please. So, sustaining the internet's trust architecture. Next slide. Again, all of this is those comments that I'm talking about. And by continuing to maintain open standards, the registration of the systems, the interoperability and uniqueness of

the internet is the key. This is the way forward for us to continue to do this.

Whether we're talking resilience, interconnections, routing, security, IPv6, any of the technical topics, that we mostly deal with RIPE NCC, but also this applies to internet governance topics, change that we want to see, rights, and others. Organizations like the RIRs, organizations like ICANN, do have a very narrow mandate, and they have to operate within that mandate.

Turning them into political tools would then jeopardize that trust if that were to happen. So, preserving that narrow and transparent roles of these institutions that support the technical coordination is really important and should not be compromised no matter what the surrounding circumstances is.

So, words like neutrality is used a lot and it's usually challenged but it is integral to how these organizations operate and not just a way to shy away from difficult discussions. Investing in the relationships, like I said, whether it be at Fellows, whether it be at NOGS, whether it be in these spaces, is a good way forward for us to continue to do that. Next slide.

The Internet was not built on control, and it's unlikely to be sustained on control. There's a lot of discussions, and I have a slide at the end there that I added, because we're hearing a lot about tech sovereignty these days and sovereign Internet and others.

There is nobody on the internet, there is no one organization that can claim it can reach everywhere through its own network.

You have to rely on others, you have to trust others, you have to be able to find a mechanism with working with others. It has to grow the trust, the coordination, those shared norms that get developed, like I said, in IG spaces and technical forums and stuff, they need to continue to evolve and build that confidence as we go. And if we continue to do this, well, then that trust architecture is more sustained and the Internet then becomes more interoperable, secure, and resilient. Next slide.

Sustaining the commons, as I keep on saying, and this is something that you're going to find even in my closing slide, that is something that we feel very strongly about, because it's those commons, it's those shared resources that the Internet is part of that makes the Internet that shared resource. And you cannot take away those characteristics and expect the Internet to continue to function.

I mentioned that I added something on digital sovereignty, and I do have a talk about this in the digital space on Thursday. But to kind of sum that up is, when you talk about digital sovereignty, because it means a lot of different things to a lot of different people and nations that talk about this, it's one of those terms that everybody thinks they're saying the same thing, but they really mean very different things from it.

But as recovering techie that understands a little bit about politics these days due to occupational hazards, digital sovereignty

actually means more choices. It means being able to decide and have more resilience. That actually means that you need to have a more capable community that actually understands how to deal with things so that they can be more resilient, less dependent, so the word dependence pops up a lot there, and the opposite of dependence is not isolation.

The opposite of dependence is actually choice, and the more you empower the communities, the commons with that knowledge with those trust capacity and those execution conditions, the better they are in figuring out these hidden dependencies and dealing with them. So, yes, as I put here in the slides, the opposite of dependency is absolutely not isolation.

Unfortunately, we are seeing some people that are using digital sovereignty as a means to advocate for isolation. That should not be it. It should be more about choice. The more choices you have, well, the more sovereign you can consider yourself to be. And actually, I would consider the more sovereign you consider yourself to be on the Internet, the more engaged you are on the global level, not less engaged. Next slide.

This is my last slide and I'm happy to take questions or comments afterwards. I mentioned there are two articles. The first one is the Internet Trust Architecture which was the main thesis of this presentation. But preparing for this meeting, I published yesterday an article on Sustaining the Commons in the Age of Digital Sovereignty.

So, if you're interested in any of these topics, here's the QR codes. Feel free to scan them. And I would love to hear feedback or comments from anybody on that work. Again, this is written from the perspective of somebody that's actually built networks and moved packets around the world that is now kind of forced because of his role to talk on a political level.

But I do think that it covers, in many senses, what the internet needs to continue to function and operate. So, happy to take feedback once people read them. Next slide. I think that's it. Yeah, happy for questions and answers, comments on any of them. I put here my contact details, email, and LinkedIn profile in case anybody wants to connect after this session. And basically, this is all, like I keep on saying, about sustaining those internet commons. Thank you very much.

CLAIRE CRIAG Thank you so much, Ibrahim. Sorry, Hamish.

HISHAM IBRAHIM Hisham.

CLAIRE CRAIG Hisham. I don't know why I keep calling you. Anyway, thanks. This was very enlightening. Particularly, I like the fact that you spoke about the digital sovereignty and the way some persons see it as more isolation, where it should provide more choice. I'm seeing one hand in the queue, but before -- I'm seeing two hands in the

queue, and I will close the queue because we only have a short time for questions, but I'm sure persons will meet with you after.

But let me just say, please speak slowly, and for those of you who may be speaking a different language, remember we do have interpretation, and put your headsets on so that we can keep this going. So, I will ask Aziz to speak, who I'm sure will be speaking in French.

AZIZ HILALI

Thank you. I will speak in French. Please take your headphones. Thank you very much, Hisham, for this presentation. You talked a lot about trust, and I really liked when you said that trust was at the heart of the Internet's architecture. I am someone who represents Africa within the At-Large community and within the AFRINIC board as well.

And in regions such as Africa or the Middle East today, some institutions have gone through very difficult times. I will not go into details, of course, but one question I have for you is this, what role can the RIRs play to sustainably strengthen this trust through community participation, and how can they build the resilience of our internet systems?

Of course, I don't want us to enter into the details of AFRINIC's problems, but we have gone through quite a difficult time and crisis, and I believe this reminds me of what you said about trust in your presentation. Thank you.

HISHAM IBRAHIM

Thank you for the question there, Aziz. As somebody that, well, full disclosure, I used to work for AFRINIC at one point in my life, and I did a lot of work in Africa as well, so I know the community there quite well. I do think that, indeed, trust is the major component moving forward for Africa in general to come together and collaborate and work. It's something that happened before and I'm sure can happen again, but it does need that careful attention.

Examples of this is, one that comes to mind is, in Africa, there's this big peering forum called the Africa Peering Forum. It's something that's been around for, I think, 15 years, maybe a little bit longer. And in that, it just comes in and tries to talk to people about how to better their networks, how to make them peer and interconnect better, how to come together, regardless of what part of Africa they are, what language they speak, what political agenda might people have.

Making it about how to make their networks operate better, that's what generates the trust, exchanging that information. So, I do think the biggest challenge, and that's not just unique for Africa, but like in any part, we have a very similar experience in Central Asia. A few years back, we went there, also we created a similar thing, a peering forum, because we considered that to be what they needed.

And we started raising that awareness, we started raising that know-how, and this is our fifth year of operating there. There is a

really good sense of community there, lovely community, they've come together, they've affected real change. They've interconnected amongst these, like, landlocked countries in Central Asia that have a lot of what you would expect to have in landlocked developing countries.

But they've really made strides in five years. And I'm pretty sure that would be the same case with AFRINIC and the organizations operating in Africa and other regions as well.

CLAIRE CRAIG: Great, thank you. Great question there, Aziz. I see, I recognize Satish and then Frederic.

SATISH BABU: Thanks very much, Claire. My name is Satish and I'm part of ALAC. I have two quick questions. The first is about a word that you've been using quite a bit, the community. Now, what precisely do you mean by community? Because for us it means maybe the entire population of a nation. It might mean technical community, civil society. What precisely do you mean by community?

The second question is, this phrase digital sovereignty is often abused in different contexts, especially when governments use it to impose top-down a certain kind of policy framework which says everything should be within the country or national jurisdiction, etc. So, how do you ensure that it's not kind of abused like this? Thank you.

HISHAM IBRAHIM

Thanks for the questions, and they're really good ones. When I say community, what I mean by it is a group of people that come together with a shared interest in something. It doesn't have to be just on a national level. Like, if you just consider it to be geography, that may or may not work, right?

What you're looking for is people that come together because they believe in certain things that they want to move forward, discuss, debate, share, disagree even. But as long as they have that basic common denominator, which is we want to work on this, that is what considers institutes as a community, right? Be it, again, technical, be it academic, be it governance are any of these issues.

And then what you end up finding is like-minded people in other parts of the world that are part of that extended community that you can draw from, learn experiences and such. That easy four-quadrant graph that I put up there, this is based on engaging with 70-something countries in my service region. Before that, I worked in Africa with 50-something countries there.

So, seeing different things and different progresses within different communities. And by the way, every topic has its own kind of development. So, in the same country, you can have an emerging community on one topic and a mature community on another. I see this in the Balkans a lot, where they have very mature internet governance meetings, for example, because of reasons.

But then the technical community coming together, it's there, but they can be doing more, right? So, it's not just a one-size-fits-all to a country. Now, to your second bit about digital sovereignty, indeed, like I was saying, different countries use that to mean different things. Some of them use that for more control, more keeping everything within the country, controlling it, everything needs to run by a state-owned or nationally-owned system.

That's one approach. The other, Europe, for example, just put out its Tech Sovereignty Act recently. It's talking more about capacity building and what they can do there., which aligns quite nicely with the trust capacity element that I was talking about. The Japanese, I love them, they're putting together very bold ideas about free data flow, right?

But then to do that, they're also using the same term, that we should enhance trust and figure out mechanisms of making that happen rather than kind of constituting everything. You see in the Arab world, countries working on, well, sovereign clouds and AI acts and stuff. Each one has a different definition, and this is where that discussion needs to properly define what we're talking about for us to be able to address that.

One last thing I'm going to say very quickly, just because I see Karen Rose sitting and being presenting us, I mentioned the Africa Peering Forum. She's one of the people that kicked that off in Africa. So, I just glanced over and saw her, so I wanted to recognize that. Thank you.

CLAIRE CRAIG Thank you so much. We are really out of time, but because Frederic had his hand up from the very beginning, I will allow this question. Everything else, I see there are persons in the queue, but please send your questions in, and we will try to deal with it offline, either through the mailing list or something.

HISHAM IBRAHIM My contacts are here.

CLAIRE CRAIG But we will allow Frederic, and if we could keep it just quickly, because we have to go on. Thank you.

FREDERIC TAES Thank you very much, Claire. Frederic speaking from EURALO. It's not a question, it's a small teaser. So, we have this afternoon EURALO General Assembly with the result of a survey we made with all our At-Large structure. And we have asked what are the top priorities for you. Is it privacy, human rights, artificial intelligence? And what came first is trust on the Internet. That's really the top one, just to mention that. So, well done. Thank you.

HISHAM IBRAHIM Thank you for that, Frederic.

CLAIRE CRAIG Let's just thank Hisham for being here with us this morning. Thank you. And you are free to stick around or, as I said, we will speak.

HISHAM IBRAHIM Yeah, thank you very much.

CLAIRE CRAIG Okay. Now, we move over to the Domain Name Registration for Cybercrime, and we have Greg Aaron and Karen Rose of Interisle, who will be speaking to us at this point in time. Again, we have 30 minutes for this session. And they are going to leave some time for some questions.

KAREN ROSE Great. Thank you very much for the opportunity to be with you here today. I'm Karen Rose, and this is my colleague, Greg Aaron. We're from Interisle, and we're very pleased to be able to present to you some of the findings of a recent study that we just released. a week ago, analyzing domain name registrations made in 2005 and cybercriminal demand in the market. Next slide, please.

So, a key purpose of our study was to put the issue of malicious registration and domain name abuse in context and to come up with some statistics and information that will help inform everyone's debate in queue, including here at ICANN. Our study set out to address four things, and I don't think our slides are rendering very well, but our study set out to address four things.

Number one, what percentage of new registrations in 2025 were sold to bad actors? Number two, where were those registrations concentrated? Number three, what can associated domain name checks reveal? And number four, what are the economic issues at play? Can I do it off of here?

GREG AARON

Okay, so while they're waiting on the slides, I'll go ahead. We put this data together using reputation block lists. These lists are protective lists that are in the background of a lot of internet services that protect us. They're basically lists of domain names that have been identified as problems. Domain names being used for phishing, to spread malware, and other kinds of problems.

There we go. We can go to the next slide, please. So, we collect those listings from a variety of sources that we list in our report. These are very commonly used block lists that are probably being used to protect your email and your network that you're on and maybe at your ISP and so forth. So, we also collected all of the associated data of all the domain names that were on these lists during 2025.

So, we got all of the registration data and so forth. We have a very large data set. All this information can be obtained publicly or commercially, so our results can be seen by other people. You could replicate it if you wanted to. Some of that data is also used by other entities who perform research. That includes ICANN itself.

The office of the Chief Technology Officer has a system called Metrica, which reports on abuse data, and they use some of the same sources that we do, NetBeacon as well. And academics also use block list data for the purposes of researching cybercrime. So, if you'd like to read the background, you can see it in our report. Next slide, please.

So, the first question. What our method is to say is that if it's been block listed, we're going to use that to represent a domain name that is a problem, is a threat of some sort. And we wanted to see, in 2025, how many domain names that were created in 2025 got block listed. In other words, we think that they were probably sold to someone who's going to commit abuse. Next slide.

So, in 2025, there were 85 million new domain names registered in the gTLDs. These are domains that were created and were in their first year of registration. These are the domain names that are important because these are the domain names that are being sold today. Other domain names exist. They're just being renewed from year to year. But these are the ones that are being sold.

And registrars and registries rely on this new business. Every year, registrars and registries have domain names that expire. So, they need to register new ones to fill the hole and also to grow. Now, 10% of those domain names were block listed, 8.5 million of them. So, that's our starting point. We know for sure that 10% of new domain names sold got block listed.

And that's not a very good thing. That is a significant portion already, but that's just the floor. We expect by the end of this year that will rise to 12% because domain names registered in the second half of last year are still in their first year of registration. They can be block listed through the end of this year. So, based on what's happened in the past, we think it's going to be 12%. But then we'll go on. So, next slide, please.

Okay. We know that the block list providers don't detect all of the domain names. So, we did some domain association, and ICANN has also done some work in the office of the CTO. They performed a study and said, let's look at the domain names that are block listed, and then let's see what domains are associated with those very closely.

Basically, domain names that were registered by the same party. And we can tell that through a variety of ways, like the same registrar registered at the same time using the same name servers and so forth. And they found that for every three names that got blocklisted, they could find at least two more that were probably registered by the same people, but were not blocklisted.

The blocklist providers are not able, frankly, to keep up with what's going on on the Internet. There's too many domain names being registered, too much crime, frankly. We did some similar domain name association studies, and the case studies we'll present in a minute, and basically found the same thing. So, we think that it's one in five new registrations. That would mean 20% of all new

registrations. And that's, frankly, a shocking and disturbing number. That's a lot. So, I'll hand it over to Karen.

KAREN ROSE

Okay. Next slide, please. We'll just skip over this one and go to the next one, please. Next slide, please. Okay. So, question number two, where is domain name abuse concentrated? Where in the market are we most likely to see it and find it? So, that was the second question that we asked.

Next slide, please. So, what we found was that domain name abuse is widespread, but it's also very highly concentrated in certain areas and with certain registries and registrars. It's kind of like looking at the Milky Way at night. You see kind of stars, a little bit of stars everywhere, but then you see really high concentrations in certain places. So, what we looked at is where these registrations, these block-listed registrations, could be found among registrars, TLDs, and then we also looked at something called registrar and registry families or corporate families.

So, for example, a domain name provider may operate a number of TLDs or a number of brands under a single corporate entity. So, for example, Identity Digital is one company that operates many TLDs. So, in addition to doing things like looking at single registrars and single TLDs, we then also looked at how those balled up into single entities under one sort of management control or corporate family. Next slide, please.

Okay. So, one of our findings, and I'll just make a note here, so the data that we're talking about are, again, are domain name registrations that were made, newly created in 2025, and this is data that we have on what was block listed as of April 30th of this year. So, we do know that more block listings will roll through as the year rolls through, but this data is, again, what was actually block listed as of the 30th of April this year.

And we found, for example, that new gTLDs, if you look at the bar in the back, .com of all domains registered accounts for about 49%. The legacy TLDs, those are things like .org, those count for about 8%. The new gTLDs, which are predominantly the new gTLDs that were released in the last round, account for 43% of the market.

However, the distribution of abuse is not evenly distributed according to that market share. You'll notice that while new gTLDs which, by and large, a lot of them are very low-cost gTLDs, a lot of them run on volume registrations, they only had 43% of the market, but they have 61% of the share of block-listed registrations that were created in 2025. Next slide, please.

We found that over eight registrars had over half of their registrations from 2025 block listed. So, this basically means that 50% or more of their domains that were registered were identified as malicious or otherwise dangerous domains. You'll notice at the top, the highest registrar had over 87% of its registrations from last year blocked listed. That obviously is nearly entirely the number of domains that it registered in the previous year.

So, we know that actors going through this registrar or these registrars are predominantly bad actors generally registering domains at scale for attacks. Next slide, please. So, then we also looked at registrar families. As I mentioned, there are companies that carry a number of accreditations. They do business under different brands, but they're all owned under the same operating company.

So, you can get an M&M candy bar and a Mars candy bar, but those are all owned by the M&M Mars company. It's the same concept. So, we found that five registrar families accounted for 53%, over half of all gTLD block-listed registrations. And we found that three of those registrar families had over 1 million block-listed domains each. And again, as a total, they came up to over 4 million domains. Next slide, please.

Then we also looked at TLDs, as I mentioned. We found that 13 TLDs had more than 50% of their registrations block listed. So, more than 50% of the registrations made last year were likely by bad guys. And some of the proportions are very high. One thing to note is that the total number of registrations in these domains can vary significantly.

Some of these domains are very small. They only have a handful, a few thousand domains. And then all of a sudden, you'll see the number of domains shoots up because they get hit and slammed by cybercriminal registrations. I'm going to note one thing here is .loan. Greg is going to talk about a .loan case study. But you'll see

that .loan has about 57.5% of registrations block listed that we can actually see.

And Greg will talk about what we can then find when we do things like associated domain names and how the number of registrations that are malicious that we find goes up. Next slide, please. And very quickly, four registry families had over 1 million block listed domains each.

And the top four accounted for about 76% of the market. So, Verisign there is 26%, about 2 million domains, then .top, Identity Digital, and ShortDot. Next slide, please.

GREG AARON

So, now we're going to talk about those domains that aren't getting block listed necessarily, but were probably registered by some of these bad actors.

Next slide, please. So, this is the tip of the iceberg, basically. So, we look for domains that are closely associated with the block listed domains. The block listed domains are basically the clues. They tell us, here are some domain names that are problems. Then we say, okay, are they in a batch? We go and look at zone files, for example. We find domain names that first were block listed, then we find the domains around them that were registered at the same registrar at the same time, they used the same hosting.

And then the domain names usually follow a very similar pattern. Criminals need lots of domain names. So, they generate them

using algorithms or scripts. And I'll show you some examples. So, we know that these domain names, even though we can't see the registrant information, we know that these domain names are related, probably registered by the same people.

Next slide, please. So, here's .loan. The blue line, dark blue line, represents the number of domain names in this registry. And it was a small registry. It was about 7,000 domains in it for a long time. Then in August 2024, the number of domain names started to rise radically. Lots of domain names being registered. And you see that it rises to over 120,000 over the next year and a half. So, a huge growth.

The red line beneath it shows the cumulative number of domain names that were getting blocklisted. And you see the number of block listed domains also starts to rise significantly and is a significant portion of the domains in this TLD. The green line with the scale on the right is the renewal rate. So, the percentage of domain names that are getting renewed each month.

This TLD had a renewal rate usually around between 50 to 60%. And that's kind of average for a new TLD. It's okay business-wise. But what you see is a year after, the TLD started to grow and the abuse started to grow, you see a year later the renewal rate plummets. It drops to only about 4.6%. So, what you see is lots of abusive domain names being registered, and then the criminals don't renew them. They've used them already. They're not going to renew these domain names.

They're bad business. And you see that basically the usage of the TLD plummets. Now, 77,000 of the domain names in this TLD got blocklisted. And we found 32,000 that were associated. So, that's over 100,000 domain names. Basically, almost all the domain names in this TLD. Who was registering these domain names? Turns out it was a major cybercriminal organization, which is known as Funnull.

This is the organization that handles the infrastructure for some of the major cybercrime operations that come out of Asia. You've probably heard about pig butchering farms. These are the scams that try to rope people in with romance scams and steals millions upon millions of dollars every year. And those compounds are actually places where people are enslaved and made to work.

Funnull also does malware, phishing, and cryptocurrency scams. These are some of the worst people that exist. And they got 100,000 domain names in this TLD. Now, just almost a year ago, in July of last year, the U.S. government sanctioned Funnull. That means they said no U.S. entity is allowed to interact with this group of people. And part of the reason is you don't want banks to process their transactions. We noticed that even after that happened, they continued to register domain names, including at U.S. registrars.

And at the time of the sanctions, the U.S. Federal Bureau of Investigation released a list of their domain names, 320,000 domain names that they had seen on Funnull's infrastructure, and

yet the registrations continued. So, this is the kind of thing we don't want to see happen. Next slide, please.

We saw in other case studies similar things. We looked at .pink, which is another TLD that started small and got very large. We found 38% more domain names. At least 76% were associated with cybercrime, basically. The renewal rate also plummeted. .gift was a small TLD that never had any abuse in it. We chose it because it hadn't been on the radar, basically.

This TLD stayed small. We did find some phishing domains in it. We found lots more when we started looking. But GIFT, things stayed somewhat quiet. Even in this quiet TLD, though, 15% of the registry was basically registered by criminals. The renewal rate, though, because there wasn't a lot of crime, stayed at 61%. And we also looked at .bond, which ended up having a renewal rate of 1 in 200 domains. Next slide.

So, you can see an example of the associated domains. These are actual phishing URLs, and you can see the domain names in the URLs in red. These were being used to phish the UK government services. There's an example of one of the text messages on the right. And you can see that once you see the pattern, it's really easy to recognize. Some of these got block listed and some didn't.

So, we went to look for other domain names in this pattern. And you'll see on the next slide, please, it's easy to find lots and lots and lots of them. We found literally thousands that were being used for this one campaign. So, these are things that registrars and

registries can find if they start looking. And the block listed information is your clue. So, next slide.

So, you can find these domains once you start to look for them. They're often obvious. They are often in very large batches. We found that the detection and the mitigation of these was really partial. Very few of these domain names that got block listed were suspended over time, which is unfortunate. Apparently, none of the associated domains were suspended at all in our case studies.

So, it doesn't look like registrars or registry operators were looking for additional domains and trying to shut down the bad customers, the bad registrants. And obviously, what's happening is that somehow the criminals are making the payments with money that's getting through. These are not stolen credit cards because those will often get caught in the fraud checks.

Somehow the money is getting through, so the criminals are using methods like maybe gift cards or cryptocurrency to pay for their domains, and that means the fraud checks are not catching these as bad transactions, the registrar gets the money, and then the registrar gets its payment as well. Next slide.

KAREN ROSE

Okay. So, what are some of the economic issues at play that we see in the market? Next slide, please. Well, one of the things that we know is that cyber criminals represent a very large and reliable source of repeat demand. They register domain names in massive

volumes, they use them for a short period of time, they discard them, and they have to come back and register more.

As we saw with the numbers, it seems, I'll be delicate, that some registry and registrar operators appear to gain some commercial benefit from taking these registrations. They seem to be apparently profitable in some areas, even if the costs are low, and sometimes the margins are even negative because they give them away in order to entice people to buy things like hosting packages.

And within the market, there's a lot of low-margin sales strategies and volume discount programs. The domain name market on the registrar and the registry level is very, very competitive. It has pushed prices down to below $2 in many cases, and you need to rely on volume, especially to drive growth. and market share.

But these high volume and volume discount programs also incentivize stales to high volume repeat customers, which is exactly the type of demand that cyber criminals provide. We also found and considered that even if you're not trying to gain or gaining commercial benefit off of these registrations, there are still incentives to at least tolerate abuse. So, tolerating abuse can be commercially rational, even when they generate little to no value, when the cost of carrying them is low, and the cost of deterrence to you is higher.

So, your commercial and economic incentive is to tolerate those registrations, especially if there is a risk or you perceive there's a

risk of any additional friction losing sales to other higher value customers. Next slide, please.

But the bottom line is that this creates something called a negative externality in economics. While cybercriminals and some registries and registrars may benefit from the situation, the reality is that the costs of cybercrime fall on the rest of us. The cost of cybercrime facilitated by abusive domains falls on victims, businesses, and society at large.

Again, in economic terms, this is called a negative externality, where the parties who benefit from a transaction pass the costs onto unrelated parties. And I think we have to be direct. Negative externalities are a form of market failure that undermine the benefits of competition that we want for this market. Next slide, please.

All right, so what do we need to do? Basically, policy in the area of domain name abuse needs to match the increasing scale and severity of the problem. Domain name abuse is industrialized and policy needs to respond to that reality. We also found, however, that abuse at this scale is not inevitable. Some registries and registrars grew without attracting outside levels of abuse.

And we saw that providers can make choices that affect whether the business is driven by legitimate demand or abusive demand. But absent change, the increase in the market by new gTLDs will

exacerbate this situation unless we have preventative measures to stop cybercriminals getting these domains in the first place.

GREG AARON

So, if you can put up the last slide. We can conclude at this point and take questions.

CLAIRE CRAIG

Thank you so much, Karen and Greg. We don't have much time for questions, but this is such an important topic, so I will allow just a couple of questions. Go ahead, Joanna, and I'm seeing Jonathan, and can we close the queue right after Jonathan, please, so that we have time for our next speaker. Joanna?

JOANNA KULESZA

Thank you. Just very briefly, an absolutely fascinating presentation. I'm assuming the report is available. I'm happy to follow up with you guys to read it in full. Two brief questions, if I may. First, what's the geopolitical impact of your analysis? I was reading between the lines. I know where the pig butchering farms are located.

I know the business model behind it. Nothing in that region happens without at least silent consent from, let's be very blunt, governments, authorities. I'm curious if there is a geopolitical implication to the data you're presenting. And I'm very much

looking forward to as diplomatic of a reply as you feel comfortable giving in this specific recorded setting.

But I'm glad to follow up off the record. And then subsequently, I think that's your last summary. What's the impact of this study on the next round? Because I think you said it very explicitly, the more domains we're going to have, the more difficult it is going to be for us to mitigate abuse. I feel very strongly about mitigating abuse.

I look at this in the work that I do from this geopolitical, international, legal angle. I see increased activity at the UN level. I don't want to say, although as an academic, I'm free to do that, we're abandoning the multi-stakeholder governance model, but I feel like it's leveraging very heavily on the work we're trying to do here.

So, is there an impact of the numbers you presented on the next round and the responsibilities of individual stakeholders in this model? I think that's a diplomatic question.

GREG AARON

Okay, thank you for the question. Well, the next round is going to happen. We have experience from two previous rounds, and we know that the introduction of new and open TLDs creates a green field. There are going to be some operators who are new at this and may not understand how their domain names are going to be potentially purchased by bad actors, for example.

There will also be new spaces, so there will be more TLDs that are available, and a lot of them will compete on price. We've seen that in the last two rounds. So, the open new TLDs are where the problems will arise. So the question is, for this community, what do you do about it? And do you have policies and procedures in place that tend towards prevention because mitigation happens after the damage has been done.

CLAIRE CRAIG

Thanks so much. I have to be the bad guy because we don't have extra time for interpretation and we still have one more presenter. So, at this stage, I just have to ask the persons with their hands up to please bear with us so that we move on to the other presenter. Thank you so much.

I know that a lot was covered in this presentation, and we need to probably invite you back at one of our CPWG meetings, where we could have a more substantive discussion on this. So, thanks again. And I invite Humberto to take the floor.

HUMBERTO CARRASCO

Oh yes, good morning. Thank you very much for accepting our presentation here. Thank you very much Frederic and Natalia and everybody here in ALAC. This is my house, as you know I've been a member of ALAC for a long time. Now I'm happy to be here with our team in the project here, Kathy Kleiman, Professor Chris Reed, and

Javier Maestro. Well, Margarita, I don't know if she's here, but she's also part of the team.

Now, we would like to talk a little bit about our project here, Helping Domain Bame Holders Defend Their Rights. Please, next slide. This is not going to be a long presentation. I just want to show you five slides. We have a lot more information about the project. And we start our clinic as we declare in other meetings before, 2018, in Chile.

So, we are part of a system in .cl domain name procedures, and there are a lot of conflicts related to the .cl domain names. We started in 2018, and until now we have been involved in more than 600 cases. And before that, the 80% owners of the domain name lose, only the 20% were successful because they didn't have enough help from the legal point of view.

After we introduced or we helped the users, we changed the balance. We took this statistic from WIPO, but in general it's similar, only 8% of the current owners win the cases. So, more than 90% are in favor of the trademark owners. So, we saw there is a pattern here. Well, some people could say that more of them could be cyber criminals, but we are not sure about that. We believe there are end users, good faith end users, who need help.

And this project that we are -- Next slide. It's trying to help them. Next one. The next one, please. Oh, yeah. What we offer. We have been working one year right now. We offer a free legal clinic. We have been training students, law students for one year right now.

We train more than 250 law students. Now we have eight current students in our legal clinic.

We have an online course. It lasts at least four weeks. And if you take the course, you can get a certificate. And after that, you can be part of our legal clinic. In the future, we hope in the next two months, we are going to provide artificial intelligence legal assistance. So if you have a doubt, a question, a problem with a domain name, or you have a conflict, you can ask to the assistant, the artificial intelligence legal assistant, and if you have more questions, you can require help from our legal clinic.

Please, the next one. So, you can see, now we have different platforms. We have our English website. It's udrpdefense.org, which is the English site. We have the same in Spanish. It's udrp.cl. And also, we have a legal blog. It's legalclinic.blog. And we are publishing information twice a week at least. With the last cases, we analyze strategies, questions, and most of our students are working on that as well.

Please, the next one. You can see some pictures. All of the team is there. On the left, you can see the members of the legal committee right now. But we are going to have members from different countries around the world. We have been training people in London, in Edinburgh, in Dublin as well, in Argentina, in Peru. We want to continue with Argentina during the next months.

And of course, we are accepting people from around the world because one of the goals of the project is involved, this is going to

be a global legal clinic. So, it doesn't matter if you don't speak English properly. We have people who can help because we have different kinds of teams. And they prepare the legal documents, and at the end, we check the final paper or the final legal response in order to help the person who is involved in a legal case. Sorry, in a UDRP case.

The next one. The next slide, please. And this is the last one. But we need your help. Why we need your help? Because the service is ready, the clinic is ready. We need your help in order to inform the end users that we have this legal help for them. So, please refer our websites, our different social networks, and if you want to be partnered with us, we are very happy to talk to you, to help you, and we hope you can help us as well.

At the end, you can see our websites and different ways of contacting us. And I think that's all. Thank you so much. If you have any questions, the team is here to answer.

CLAIRE CRAIG Thank you so much, Humberto and team. Does anyone have any questions? Go ahead, Amrita.

AMRITA CHOUDHURY Thank you, Humberto, for the presentation. Amrita, for the record. It's a great initiative. Do you have any, and this is not a question, just a common question, if you want, from the RALOs, to help to share this information to others, do you have some kind of a poster

which is smaller, which you have prepared, which we can then share it across our communities so that whoever is interested can go directly to the website or something? Either if they want to go in for the course or even if they want help, because that would be really helpful. That is how we can help pass on the initial information. Thank you.

HUMBERTO CARRASCO Would you like to? No? Oh, well, we don't have that right now, but we can work on that. And I think this is a great idea. Kathy, thank you for notes.

KATHY KLEIMAN But also, we'll have brochures tomorrow.

HUMBERTO CARRASCO Yes. Oh, yeah.

KATHY KLEIMAN We're going to bring the brochures back, but that's a great idea to create a small poster.

HUMBERTO CARRASCO Yeah. Go ahead.

AMRITA CHOUDHURY

Because what we see these days is, like, for example, if you even post it on LinkedIn, there are people who get interested. As in, we see that in APAC. It works a lot. If there's a poster, we share it with them. The community looks at it, goes there, and they can spread it across.

Like, for example, if you want to spread an information, we say, look at it, try, if there are people who need help, they can go into it, or even lawyers who work in different regions. So, we can perhaps spread the information. If they're interested, they can get connected to you.

HUMBERTO CARRASCO

Excellent idea. Thank you so much.

CLAIRE CRAIG

Thank you so much, everyone. Again, we've forgotten to say our names at the beginning of every time we speak. But I am Claire Craig. Thanks for being here, all of you. Thanks to our interpreters who have given us a few extra minutes so that we could conclude this discussion.

Just a reminder that we return in this room in half an hour for our CPWG session, and we look forward to seeing all of you back here. And remember those of you who were unable to have your questions answered, to please share it on the mailing list or send it to one of us, and we will send it out to our teams who participated.

We wish to thank all the members who participated this morning to bring such rich information to us, and we look forward to working with you again in the future. Thank you all.

[END OF TRANSCRIPTION]