TERRI AGNEW: I'll now go ahead and begin this conference. One moment please.

Good morning, good afternoon, and good evening. Welcome to the LACRALO GSE Capacity Building Webinar, Basic DNS teleconference, on the 16th of April, 2015 at 23:00 UTC.

We will not be doing a roll call, as it is a webinar. But if I could please remind everyone on the phone bridge, as well as computer, to mute your speakers and microphones, as well as state your name when speaking, not only for transcription purposes but to allow our interpreters to identify you on other language channels.

We have English and Portuguese interpretation.

Thank you for joining. I would now like to turn it over back to our moderator, Silvia Vivanco.

SILVIA VIVANCO: Silvia Vivanco from ICANN staff speaking. Thank you Terri. Welcome to the Basic DNS webinar, organized jointly by ICANN Global Stakeholder Engagement team, and the Latin American and Caribbean staff, and the LACRALO. This is part of the ICANN strategic plan for Latin America and the Caribbean for this year, 2015.

The objective of this webinar is to give fundamental knowledge so that you can gain a sound understanding of the DNS, domain names, domain name registrations, and domain name resolutions, both in physical TLDs and gTLDs. We will be speaking about security, stability, and resiliency.

And with that, I would like to introduce my colleague in ICANN. He is the Senior Manager for Security, Stability and Resiliency at ICANN.

He's a trained lawyer, and he is also a certified trainer. He focuses on collaboration on the [inaudible] cyber crime control activities and law enforcement agencies, at an international level. As part of his duties, he trained law enforcement agencies, ccTLD managers, and other stakeholders that are involved in Internet identifiers, operations, and security.

Carlos works on fundamental components for security, stability, and resiliency in the DNS. Alberto Soto will be giving a presentation devoted to explaining domain name registrations, both for ccTLDs and gTLDs. He will focus on domain name resolutions, and the DNS operations. He will be giving an example, and telling us how or what happens on the Internet when we want to read a newspaper online.

We will be having their presentations, followed by the questions and answers session. Please kindly type your questions in the Adobe Connect room, or else raise your hand, in order to take the floor. The floor will be given on a first come, first serve basis. With that, I welcome my colleague Carlos.

CARLOS ÁLVAREZ: This is Carlos speaking. Thank you Silvia, thank you for this kind introduction. We do not have plenty of time, so let's focus on our presentation. I will do my best to speak slowly, or slowly enough so that interpreters can work accurately, and can render accurate interpretation. But I will speak also quickly enough so that we are

within the allocated time for this webinar. We will be focusing first on unique Internet identifiers, what they are, what they are about, what their [AUDIO OUT] is.

And after that, Alberto will be speaking about domain name registration process, the domain name resolution process, and finally, I will be telling you a little bit about what we do in the security, stability, and resiliency department.

So, let us focus on unique Internet identifiers. All hardware, equipment, all the devices that can be connected, say a telephone, a printer, a fridge or refrigerator, now with the Internet of things even light bulbs, and phones that we have on our desk. Well, all of these devices have a specific address that is connected or related to them. And this is known as MAC, or MAC address.

These are unique addresses per device. So they are specific for each device, so this means that we have only one device in history, on the entire planet that can have these MAC address. Unfortunately, we do have fake MAD addresses, so some MAC addresses can be repeated. And this MAC address is allocated by the hardware manufacturer. That is a legitimate MAC address.

We will now focus on the relation between the MAC addresses, and routing. The first steps, routing steps, in a local network, and on an Internet protocol network. This brings us a little bit closer to the need of domain names, and domain name resolutions. MAC addresses are made up of a series of characters, as we can see on the slide.

They are separated by two dots or a colon, and here you can see different steps so that you can find the address of the device that you are using, depending on whether you use Windows, or Mac. For example, if you use Windows, you can type CMD dot EXE, and then you type get MAC. Now if you use Linux or Mac, if you use the corresponding term, then the user can have some kind of interaction with the device, by means of certain commands. So if you type I-F config, and then you search the results, and you look for one that begins with the word either.

The same applies to iPhone and Android cell phones. And here, on the slide, we see the correct routing, so that you can find the MAC address of your devices. Normally, users do not think it is very relevant to find these addresses, because users never want to know why things work, and how does the Internet of things work.

With a MAC address, a device is able to communicate, so to speak, with other devices, with other machines, with other computers that are on a network. But they cannot connect to the Internet, and what I mean is to get connected to a router, so that the router, in turn, and sorry if I am repetitive, so that the router can route that communication outward. So this device needs to have an IP, an Internet Protocol address to that end.

Surely, you must have heard about IP addresses, something at least. We have two kinds of IP addresses. We have IPv4 and IPv6, the different versions. Here we can see an example of an IP address, 192.168.2.1, that's the example of an IP address. In general, people are

not able to remember IP addresses as such, not IPv4 and let alone, IPv6, version six, typed in red on the screen.

As you can see, these are very long, very lengthy addresses, and it's very hard to remember them. These IP addresses are necessary so that routing can take place, so that communications can be routed and machines can be intercommunicated. Some decades ago, the Internet founding fathers had this idea, that is to have these IP addresses in formats that are easily remembered, and that can be related or linked to IP addresses.

It's far easier to remember ICANN dot org, then to remember a lot of numbers that make up an IP address, that can be used for a web server, for an email address, among many other things. As I was saying, devices need to be connected to a router, so we have different routers, and they need to connect the machine to a local area network, and in turn, to the Internet.

In the Adobe Connect chat room that we are using right now, we are unable to see the dialogue that would be taking place between that laptop computer and the router. The laptop computer would be sending a message to all of the internal networks, asking, "Can someone help me connect to a network, because I want to connect to the Internet?" And the router would be answering, "Yes of course, I can help you. I am your router. I am your gateway. And my address is a series of numbers. And your IP address is 1234.56, for example."

And we have entered an address to connect to the network, so these are just examples. Once the router and the gateway assigned an IP

address to this laptop computer, then the computer can connect to the Internet, and have some outward gateway, so to speak. So we can have communication under an Internet protocol.

Oh, here we go. Here we can see the dialogue on the screen between the laptop computer and the router. That's great. So, as you can see then, the laptop asks, "Can someone help me connect to a network?" And the router replies, "Welcome, I am your gateway. My address is such and such. Your IP address is such and such. And your sub network is such and such."

I will not go into any further detail about what a sub network is, but briefly, it's the name of the local network. That's the number that identifies the local network. So the computer receives that information, and the routing can take place. Now, in order to connect or link both addresses to MAC and the IP addresses, there has to be something that enables a machine to work with both addresses. So, the MAC address is hard coded.

It belongs to the hardware, but the IP address is at a different level, that is not associated to the hardware, and the machine, the computers, needs to be able to connect the hardware level with the IP level. So we have this address resolution protocol now, coming into play. This A-R-P connect MAC and IP addresses on a network.

Here we have an example where you can see that if I use A-R-P minus A, in a MAC session, I can find the IP addresses associated to MAC in that local network, and their corresponding MAC addresses for those devices. This way, my computer will know whether the computer has to

connect, or if it has to connect to another computer, my computer will know the right address corresponding to that device.

This is very interesting. I will briefly touch on this, before giving the floor to Alberto so that we can stick to the allocated time for this webinar. We have several types of IP addresses. Briefly, or in general, we can say that we have private and public IP addresses. Private address can exist, or must exist, in or within internal networks. If you pay attention to this slide, if you see the blue arrow, below that arrow, we have a link.

It says, "C-R-F-C, 33 zero, special use IP addresses." And if we click on that link, if we click on that link, you will reach, or you will access an IETF Internet standard. The IETF is the Internet Engineering Taskforce, the Internet Engineering Taskforce, that is the IETF, and that's the standard that deals, or addresses, special uses.

And you can find the ranges there, from this number to that number, the addresses are used for this focuses, from that number to the next number. The addresses are used for another purpose. When I connect to the Internet, my ISP assigns a number that is there within one of those ranges.

I pay a monthly fee to my ISP, and my ISP must assign an address that is within the corresponding route. It should be a public IP address. However, something, or there is a packet which is not quite welcome, and that is that some ISPs assign addresses that are within the private range of addresses. So it's carrier grade NAC.

So my ISP considers the following. Instead of considering all the customer's machines, or computers, as part of the Internet, what they say is, or what they consider is that the traffic within that ISP is not within the Internet, but within a local network that may encompass several districts or neighborhoods, depending on the configuration of that ISP.

This practice, the carrier grade NAT practice, is not really welcome, or appreciated. Why don't we like it, so to speak? Well, some of us want to have a secure and friendly Internet, so that our children can use the Internet in a safe way. So we don't like this because it makes it harder to identify people with a bad intention on the Internet.

There are some who claim that if they use the [tor] network, for example, they cannot be found, or located, well they're really wrong, they are mistaken. It is always possible to different extent, to find someone that is not acting correctly on the Internet, but this carrier grade NAT makes that a little bit more difficult, because each ISP has to store the corresponding data of their clients.

So of course, when we reach the Q&A session, we can address that question. We will be more than happy to do so. With that, I will now give the floor to Alberto. Alberto, go ahead please.

ALBERTO SOTO: Alberto Soto speaking. Thank you Carlos. Hello everyone. Good morning, good afternoon, good evening. Welcome everybody. When Carlos and I started coordinating the topics for this webinar, well we

realized, both of us are lawyers, and we thought, well, what is going to come out of two lawyers working together?

Well, I think this is coming out quite nicely, at least so far. Carlos already spoke about IP addresses. What goes on, as we will recall, as Carlos said, we need certain numbers, so to speak, to access Facebook, to access a website, and typing all of those numbers would be impossible, because the numbers are impossible to remember.

That's why we have the DNS. The DNS is a server, is a computer, that resolves domain names, but within ICANN, that is a system. It's a complete system that resolves domain names, and, as we will see, we have lots and lots of computers that can resolve this. Terri, if you could please go on to the next slide? Thank you.

So, I will try to speak clearly. Please tell me if you can understand what you see on the screen. Oh, I see nobody raising their hand, so everybody understands the screen. Okay Terri, please, next slide.

This is a little bit simpler. Please, if I know people, or several people here on this call, have knowledge of this topic. So please, if you don't understand or need an explanation, let me know. Feel free to let me know. Okay. We will focus on the domain name system, the DNS. We will be writing in the opposite direction.

So for example, United Kingdom, UK, is UK dot ORG, dot your domain, dot triple W. Okay, you will recall the issues we had with dot Patagonia, oh excuse me. That was not the example I wanted to mention. We had issues with two letter domain names, because normally these two letters are used for a ccTLD. The country code top level domain. So,

together with dot COM, dot ORG, and many other TLDs, these are what we call within ICANN, top level domains, TLDs.

The two letter TLDs that identify a country, as we know, that a group that is focusing on the country code top level domains, ccTLDs, and there is another group that is focusing on the gTLDs, the generic top level domains. So, as we can see that within ICANN, all the domain name policies are being specifically addressed by someone.

Carlos, yes, you're right. It's country code top level domain. I was not saying it correctly in Spanish. Thank you. So, in this example, we have your domain, that is a domain representing a person, an organization, or a company. So this gives us the domain name. So your domain dot ORG dot UK.

Please remember this because it will be part of our trivia questionnaire, how do we represent a domain name? The URL is the complete address that I have to type in order to reach a specific website. Terri, next slide please. Thank you.

So, if I ask someone from the technical community what the DNS is, he or she will say, it's a computer that resolves a domain name. But we, in our way of seeing this, have to consider this as a whole system, a comprehensive system, that ICANN has, that simply translates a domain name that is an alphanumeric address. Why alphanumeric? Well, it's alphanumeric because domain names can have letters and numbers as part of their characters, as is the case in some domain names.

So that alphanumeric domain name is transformed in an IP address. And that is what Carlos just explained. And vice versa. Why vice versa?

When I type something, the DNS translates that, searches the address of that site that I want to reach, and then sends that back to me. So, once that is completed, then the DNS, the domain name system, has resolved the domain name that I typed.

Terri, next slide please. Thank you. Let's talk on how the DNS resolves. When I type the address of any website, I type that in my browser. As Carlos said, I will have a router, a piece of equipment, a computer whose role is exactly to route that. That is to direct traffic to a certain location.

The Internet in this case, resembles an upside down tree, or an inverted tree. That is, if it doesn't find what I asked for initially, it will seek or search that at another level, until it finds a root name server. We have 13 root name servers, that are the main DNS servers. It will never read the root names initially, or from the start, when it activates the search. And this is because some domain name server resolves the name before we read this status.

This would be in case a domain name were not resolved, and we have to reach the root servers, which are breeched in very, very few cases. So as I said, from letters we go to numbers, then the domain name is resolved.

Normally we don't run into any issues. Why? Because there is a primary DNS server, and a secondary DNS server. These are computers that quickly resolve the names, so that the name doesn't have to travel for a long time within cyber space, before it is resolved.

So, I worked in a software development company. We had a data center. We had our own primary and secondary domain name servers there. So the level of redundancy is such, nowadays, so that things have improved considerably. Hello, can you still hear me? Yes.

So, once I obtain that information, well the information reaches my device, and I can access the information that I wanted to access.

SILVIA VIVANCO: Silvia Vivanco speaking. Yes, Alberto, go ahead, we can hear you.

ALBERTO SOTO: Alberto Soto speaking. Okay, I'll carry on then. Alberto Soto speaking. My apologies, I thought my line had dropped. So, that information reaches my device, but if we look at the slide, it says that if the information is not found in your computer, telephone, tablet, PlayStation, smart watch, fridge, etc., why have I included all of these devices?

Well, we, nowadays, have fridges or refrigerators that register, for example, the number of bottles that I have inside. And if the inventory is [empty], the refrigerator will call the supermarket so that I will get more bottles. So those would be internal or private IP addresses, as Carlos was explaining before.

As you can see, we have plenty of instances of communication, resulting in the DNS. As I said, many, many years ago, many years back, when I type an URL that stands for, Uniformed Resource Locator, well, back then, in the beginning of the Internet, we didn't have a domain name

server, at least in Buenos Aries, in Argentina. So the name was resolved in the United States.

Later on, a root server instance was formed in Argentina, and as time went by, the Argentine Internet chamber access, hosted that instance of the server. And in turn, placed more instances of DNS resolve servers in Argentina.

So people willing to resolve a domain name, obtained the information far faster than before, because the information didn't need to travel all the way to the DNS resolver in the United States or in Buenos Aries. And right now, Internet service providers have their own DNS. So this has improved performance significantly, because in the past, I used to click enter, then have a cup coffee, then come back and I was still waiting for the name to resolve.

Right now, the situation is a little bit better, but we need more, a broader band because of the social media that takes up a lot of space, so to speak. Here we can see a list of the root servers, and as I said, we have different organizations. For example, VeriSign is in charge of dot COM, then we have a university, then the third institution is Cogent Communications.

They have a root servers. They are in charge of domains. They are in charge of the maintenance of the root server, but on top of that, they are a very important carrier. Then we have the NASA. The we have RIPE NCC. And so on and so forth. So these root servers, and we're not going to go into that much detail right now, these root servers have different methods, and they are replicated in many places worldwide.

And Carlos, correct me if I am wrong, but we have between 450 and 500 replicated instances of the DNS. So if I'm not mistaken, we have between 430 and 500 replications of the DNS from the root servers. Am I right?

CARLOS ÁLVAREZ: Carlos Álvarez speaking. I will use this question, to compliment something that I said before, to supplement something that I said before. The DNS of a system is distributed database, that is not operated by ICANN, but by many organizations in many countries. The root is operated by VeriSign. VeriSign is in charge of maintaining the root in different servers.

And the instances of the root, the root server instances are managed by the different organizations that Alberto is showing us now on the slide. From then, downwards, the system is distributed at different levels of granularity. So that it is stable, resilient, and unlikely to be impacted or effected by interruptions or disruptions.

I started thinking about two processes that are similar but different. One of them is the domain resolution, and the other process is the domain registration. When the domain registration reaches the TLD manager. In terms of the resolution process and the replication process of the root servers, on the one hand, and on the recursive servers on the other hand, the root servers aim to end, well, each of these root servers is a cluster of computers, a cluster of machines.

It's not just one machine, but many, many, many machines that are geographically distributed. The L server that is operated by ICANN, has

or applies a very interesting concept, that is a root in the box. So basically that's an instance or a replication of the L server. And that box is a very small server that can be installed at a very low installation and administration cost.

So on top of resiliency, we can have a better management of the traffic, of the different queries reaching a server. And it's very important to mention the any cam protocols, or any cap. This means that servers are linked to a cluster of IP addresses, but within each cluster of this cluster submachine, corresponding to each of these servers, A to M, any machine associated to an IP address, will be able to resolve a query reaching that IP address.

Maybe I was not very clear. Normally, an IP address is an unique identifier corresponding to one machine only. That's the case of public addresses. In the case of root servers, an IP address can correspond to many machines. And this is because of geographic [inaudible] in order to reduce traffic time, and also, in order to achieve higher resiliency, and a wider band, and a lower response time as well.

If we go one level further down the root server, we will find the recursive servers, and we will focus on authoritative servers. VeriSign operates an authoritative server for dot COM. Then we have the BIR operating an authoritative server for dot ORG. This means that the information that we received is not arguable, not debatable, because those servers, in turn, have recursive servers that send the query, once and over, and over, and over again, all along the DNS chain.

Then they reach the authoritative server, and then they go to the authoritative server. And they are called recursive servers, because the query is processed over and over and over again, until the reply is reached.

These recursive servers, that are underneath, or one level below, the authoritative servers, well, I really, we cannot know for sure how many of them that are, I don't have the number for sure. And anyone can resolve the DNS server to resolve names. And that would lead us to the issue of open servers, but that's quite another story. So with that, Alberto, I give you back the floor.

ALBERTO SOTO: Alberto Soto speaking. When Carlos says that these servers can be installed quickly and safely, this is because of technology advances, because in the past, to do this safely, we needed a data center structure that was quite considerable, in order to achieve the desired or necessary security level.

Technology has advanced quite a lot, and we have improved quite a lot in terms of cost. So we will now focus on domain names. As I said, domains are made up of letters and numbers. And the hyphen is also accepted, in as much as it is not at the very beginning or at the very end of the domain name. Domains may not have or include these special characters that we see on the screen now.

Next slide, Terri, please. So, domains must be registered. I kind of said a registry is a central database where we have all of the domain name numbers. So the registrars have access to that database. A registrar is

an organization that has access to the registry, and therefore is in charge of domain name registration. And a registrant must be accredited by ICANN.

We will not focus on the registrar accreditation process, but here you have a link for further information. And let us focus now on the registrant. The registrant is a person that acquires, or purchases, a domain name, and therefore becomes the owner of that domain name. So the registrar introduces that name, domain name, and once that domain name is introduced, it will become operational.

Terri, if we can move to the next slide please. If you check the [Internet] dot NET side, operated by ICANN, you will access general information on domain name registrations. You will see an alphabetical list of registrars. You will also see a list of registrars on the basis on their geographic location, and also, on the basis of the languages in which they operate.

There is also a table with all ICANN accredited registrars, and their locations, and the different TLDs they operate. So, you can purchase a domain from VeriSign, from Go Daddy directly, but you can also contact a reseller here in Argentina. So if you look at the resellers, within ICANN you will not find that organization, because that reseller has a commercial agreement with a registrar.

And the reseller has no relation whatsoever with ICANN. Therefore, ICANN does not acknowledge the reseller due to the absence of a contractual relation. Now, we are going to read the newspaper from Argentina. I will give you an example now, if a couple of the newspaper

[Spanish], which have been resolved already. This is something used by technicians to solve certain problems, but ICANN uses to show you the example that I want to show you.

When I type WWW dot [inaudible] dot ES, there is a certain IP address, and that IP address is one of the [Spanish] dot ES website. So the domain name resolution is immediate. Please do not read everything, but just focus on [Spanish]. [Spanish] is my ISP. And with this, the time it takes, in second or milliseconds. That's the time it takes. Double crossing Argentina is the carrier that provides the most important broadband access in the country, and [Spanish] uses global crossing.

And then I see [Spanish]. That is the direct gateway out from Argentina. And then that goes to Los Angeles, then to Palo Alto, then to New York, etc. etc. Then we follow, or we reach the [inaudible] 23, 67, 250, 136, etc. So this shows that I have been using the fiber optic in the specific that goes out from Argentina, it reaches Chile, then it reaches Los Angeles, then Palo Alto, then New York, and then it reaches the fiber optic from the United States to Europe.

And you have the complete route. Terri, the next slide please. And we have the same case here, but in France. The domain name resolution was immediate. So I do the same thing, [inaudible], Argentina, Global Crossing, Miami. In this case, I also use the Pacific fiber optic, optic fiber, and I reached a root server, and a very important carrier, called [inaudible], that took me to France.

And there, I reached [inaudible]. Terri, next slide please. So that's the way we surf the Internet. That's the Internet traffic, routing, and the domain name resolution. Terri, next slide please.

With that, I will give the floor to Carlos again.

CARLOS ÁLVAREZ: Carlos Álvarez speaking. Thank you Alberto. Okay. I will now tell you about what we do in my department, but before going into that, Alberto mentioned the domain name resellers, and then we have privacy and proxy providers. Privacy and proxy service providers. These companies enable users to use third party contact information when they have a domain without using their own names.

So Carlos dot com would indicate that the domain was registered by privacy services limited, and the contact information would be the contact information of that company, instead of my own information. That has some benefits and some disadvantages, of course, but what I wanted to say about resellers is that while we have, here is professional, ethical, companies, we also have some other companies that are beyond our scope and reach, and pose a challenge so to speak.

Many ICANN accredited registrars work with resellers. And I don't want to speak about domain names sales, because there is no property right over a domain. A domain is an Internet resource, therefore we cannot have property or ownership rights over them in the same way as I have property or ownership rights on my car, my house, or my computer.

As I said, domain names are Internet resources. So I would rather say that they are registered. They are not sold. So we have information on the domain, information on the registrant, the server, the IP address, and the domain name is registered. About resellers, as I said, some registrars work with their own resellers, and that reseller, sorry that registrar has contract obligations with ICANN.

They have to guarantee that resellers observe or unearth the contract between the registrars and the reseller. And resellers are a little bit more trustworthy, but I don't want to make a sweeping generalization. So resellers have to be serious, responsible company. But the point is, if you're going to register a domain name, do all of your homework, so to speak. Work thoroughly. Check the registrar and the reseller's reputation, and track records, and understand, be aware of what you're going to do, how you are going to register that domain.

If it's going to be through a registrar, through a reseller, check or look up the names of these companies online. So do your homework, so to speak. Work thoroughly. It is unfortunately that bad things can happen. So in general, or generally speaking, these are the three most relevant areas in my department.

First of all, we focus on analytics. We analyze a lot of information on domain name registrations, and we try to find cases of misuse or abuse. So we focused on different domain names that were registered in the different industries sectors in the United States. And we found, or we reached, very good conclusions and also alarming conclusions, at the same time. And we shared that information. We shared that information with the corresponding companies, and we work under the

understanding that we cannot punish those conclusions because they would be detrimental to the company.

So that was the understanding, however, the corresponding industry sectors welcomed this information and the conclusions. And they agreed on implementing the necessary adjustments corresponding to the different conclusions. We are now working on another interesting project. We have an anti-phishing working group. It's a non-for-profit group.

So it's an organization, it's a non-for-profit organization that gathers companies, or brings together companies that work on this area. They are now focusing on the malware and bot list, and now they are focusing on e-crime. So they receive information about domain names that have been captured and are being used in phishing campaigns, so they analyze the domain name registration information, and they share that information with registrars, so that they can take the necessary steps and registrations can be blocked or suspended.

Then we also focus on capacity building, that's the second area. In that regard, ICANN does not operate Internet infrastructure, other than the L root, and of course, the IANA, the Internet Assigned Numbers Authority. The IANA functions are critical to the operation of the entire domain name system. It is critical because it's the management of traffic, and let's see how I can put this nicely.

It's the management of traffic that should be invisible, so to speak. If nobody knows that IANA exists, that is because things work smoothly. The moment something works wrongly, or there is something incorrect

and there is a mistake, and people start wondering what is happening? Who made a mistake? And they said, "Oh, yes, it came from the IANA. IANA made a mistake, that's why things are not working."

If everything works smoothly, correctly, and that is what people want, then this is working, so to speak, behind the scenes, and working well and working smoothly. But part of the servers used by IANA and the L root, is what we operate, but other than that, we do not operate Internet resources. That's why we train law enforcement agencies, units worldwide, ccTLD operators.

We train people in charge of the Internet infrastructure operation or security, and literally, that is worldwide. Our team can reach 20 countries, for example, as an example, quite easily. And this is so, on a monthly basis, we are all the time on the field, the more capacity building activities we can carry out, the better.

The more we can reach out to stakeholders in terms of DNS operations, and focusing on how to identify, contain, and mitigate threats on the Internet in terms of IP addresses, so much the better. Finally, we focus on trust based collaboration. And I don't have a very nice translation into Spanish for that.

It's not as descriptive in Spanish as it is in English. This means that we engage in the operational security community groups. Operational security means companies and people able to respond to threats that can affect users. And that can mean or a serious risk, for the DNS, that can endanger the DNS resolution, because if the DNS stops resolving

then it stops working, and certain regions of the world will no longer have Internet access. So if I type ICANN dot org, I will not reach the site.

So, when we engage in these groups, basically what we do is to monitor information. So we keep an eye on things to see what's going on. We monitor that intelligence. And when we see that there are threats that can pose a risk to the DNS, we take steps. We do not operate infrastructure, as I said. So that's why we help the community to face and reduce these possible threats.

So, briefly, this is what we do. And I believe now, Silvia, that we can move on to the question and answers part of this webinar call.

SILVIA VIVANCO: Silvia Vivanco speaking. Thank you Carlos. So, we are now going to open the questions and answers section of this webinar. And the first question, it's from Sylvia Herlein, "How can we remember and store our MAC number? What can we do, or how can we find out our MAC numbers?"

CARLOS ÁLVAREZ: Carlos Álvarez speaking. Well truth be told, the MAC number is irrelevant to the user. It is simply used for routing purposes, so that in an internal network, the router and the different machines can locate your device. But you as a person, as an individual, do not want to find the MAC number. Now if your cell phone is stolen, and the thief is arrested, and he or she has three phones that look exactly alike, if you were smart enough, so to speak, to write down your MAC address, your

cell phone MAC address, then you can see, or you can find your phone among those three cell phones that have been stolen.

But that it's, that's it. Other than that, I don't see the use in storing your MAC address.

SILVIA VIVANCO: Silvia Vivanco speaking. Thank you Carlos. Aida Noblia has a question on domain names. You mentioned there are no property or ownership rights over domain names, but what about the right to use, or a right of use over domain names?

CARLOS ÁLVAREZ: Carlos Álvarez speaking. Okay, I will tackle your question by saying that technically we're speaking about a domain, a registration. It's simply a registration. So you have the right of use when you are assigned, you are assigned the administration of a certain resource, but that's the way I want to put this in these terms.

When you register a domain name, you become the manager or administrator of that network resource in as much as that resource or that registration is valid. And you can use that in the following way. You can have a FTP, you can have an email address, you can have a website, you can have cryptographic information on the DNS.

So in as much as you're the registrant, that is the person that is identified as the one able to administer that network resource, than you can be in charge of that network resource administration or management.

SILVIA VIVANCO: Silvia Vivanco speaking. Okay, thank you. Aida Noblia adds, so this means that you have the right to administer the domains during a certain period of time. Then I have a question from Nascimento Falleiros. If technically a registry, what about trademark rights, or my trademark patent rights? What are the challenges for the market in Latin America?

ALBERTO SOTO: Alberto Soto speaking. When we speak about top level domains, that policy is clearly defined within ICANN. When we speak about a domain that represents a company or a person, an individual, or an organization, then that is totally different. There are disputes, litigation, controversies, and once again, we do not have plenty of legislation available on domain names.

In many countries, we know who can access those dot ORG. In Argentina, for example, if you want a dot ORG registration, you have to be a non-for-profit organization registered accordingly. And you can do that online. So we do not have big issues in terms of TLD. Now when it comes to domain names, there is a discussion about whether a, needs to consider that as a trademark or not.

Let us focus on Aida dot COM, for example. What if someone registered that first? We still have huge controversies on this matter. I remember now a surname used as a domain name. Somebody in Argentina had a shoe factory and there was a Spanish radio speaker, and they had the same surname. So the World Intellectual Property Organization gave

the domain name registration to the Spanish radio speaker, because he was more popular than the Argentine owner of the shoe factory.

And I don't agree with that. I think that it should be a first come, first serve basis. We still have plenty of thorny issues. For example, if I have registered a trademark, do I have the right to the domain name, or that depends on each country or national jurisdiction.

CARLOS ÁLVAREZ: Carlos Álvarez speaking. Within the ICANN world, we have the uniform domain name resolution policy, the UDRP. And in the new gTLD universe we have the URS, and please bear with me, I am looking up the acronym.

It's the Uniform Rapid Suspension system. Basically, the UDRP enables trademark holders to apply affordable, simple, and fast procedures when they see that somebody wants to register their trademark, but some requirements have to be met. And I am reading this online. The domain name has to be identified or confusingly similar. That is, that it can be confused to the trademark. So if that is the case, then you have the right, or else the domain name is registered or used in that phase.

So these are the requirements for cases. We see plenty of cases in which domain names have been registered only to use spam. And spam is used, or the sending of hundreds, and hundreds, and hundreds of irrelevant email messages. The spam is a tool used to access machines, just to capture computers and include them in bot nets, so as to get passwords, banking information, and this, many times, happens because people use trademark names that belong to third parties.

ALBERTO SOTO: Alberto Soto speaking. Carlos said that we need to be careful, or that we need to check the registrars background, and that we shouldn't focus on money only, or on cost only. In fact, we have reliable or trustworthy registrars, and if I reserve a domain name, and I use my own name, there is no issue about that, but if I hire web hosting service, and that organization reserves the domain name using their name, then that results in some issues, because the registrants wanted to get their domain name back.

And then, that was not possible. So, the end user, the individual user, can run into trouble when they reserve their domain name. So my advice would be for you to be in charge of all of the steps in the registration, and to do that personally, and to have the domain name registered in your name, to your name.

And not in the name of the ISP, or the designer, or the web hosting provider. That's it.

SILVIA VIVANCO: Silvia Vivanco speaking. Thank you Alberto. I see no further questions or comments, so I don't know if there are any further questions or comments. I don't see people asking for the floor.

ALBERTO SOTO: Alberto Soto speaking. This is not a question, but I see, [inaudible] webinar, and we spoke about security issues, about information security issues on the Internet. For those of you that did not attend yesterday's

webinar, what we discussed was the lack of legislation in our region, in the countries of our region. This IP addresses that are allocated are dynamic IP addresses. They may be the same, or they may be different. So that should be registered or recorded with the ISP somewhere.

However, this is not mandatory bylaw. There is no law mandating that that information should be stored for a certain period. So, when we reach, or when there is a crime, when a crime is committed, and I try to reach that registration, it is highly likely that we will not find that registration, because the service provider is not required by law to store that information for a certain period of time.

And it's called traffic data, not [inaudible] data. In Europe, most countries, have to store that information for a two year period, because normally because of the type of crime, the statutes of limitations is within a two year period. Thank you.

SILVIA VIVANCO: Silvia Vivanco speaking. Thank you Alberto. I have a question, if I may. Carlos, you mentioned a relationship between ICANN and law enforcement agencies. What is that relationship about?

CARLOS ÁLVAREZ: Carlos Álvarez speaking. First of all, as I said, we train law enforcement agencies. We engage in capacity building activities in Europe, Asia Pacific, America, Latin America, Europe. So, we, even in the most experienced unit in the law enforcement community, they find that this is like a sub-specialization within the [inaudible] crime field of expertise.

Investigating crimes that entail identifying people that misuse or abuse the DNS, is very, very specific. That's why recently we trained prosecutors, we trained the DEA staff, FBI staff, Interpol staff, and in Latin America, given the forthcoming meeting in Buenos Aries, we are focusing on training the Buenos Aries metropolitan police. We hope the federal police will also attend our training sessions. We will be in Chile in August, and in July we will be engaging in capacity building activities in Columbia.

Last year, we carried out some training activities in Bolivia. And this is just my realm of expertise, but I will be training the Zambia police, the cyber crime unit there in Africa, and our doors are always open to any law enforcement agency or unit that needs more information. Well, we don't give them the information, because ICANN is not a law enforcement agency.

But we explained to them how they can find the information they need, if they need to find a zone, find a system, if they need to find information about a domain name registrant. We take our time with it, done with them, we work together, we travel, we meet their team, their unit, so that they can successfully complete their investigations.

And also, their malware using algorithm for domain name automated generation. We have different viruses, game over, Suze, crypto-locker, and fiber criminals include algorithms in that malware, which are very sophisticated. So the infected, sorry. So the bot net can automatically register domains with certain characteristics.

And you can recognize those domains because they have the same number of characters. So they are easily recognizable, and they are automatically generated. As we say, sometimes in jest, when the good guys can decipher those algorithms, we can easily foresee which domains would be used in that bot net tomorrow, next week, next month, in 10 years time. Because it's an automatic generation.

And once you find the domain name lists that the bot net will be using, then you are a step ahead of the criminal, and you can capture their entire bot net structure, or most of that structure. And you just leave a very, very tiny part of that bot net operational, so as to monitor that traffic.

So, the law enforcement agencies need ICANN's support so that registries can block those domains that the criminals want to use, in advance. So Silvia, I think that's the reply to your question, generally speaking.

SILVIA VIVANCO: Silvia Vivanco speaking. Thank you, thank you very much. I think this also replies to Mr. Fernandes' questions. He wants to know if there are investigators that can identify a user that would be engaged in a cyber crime.

CARLOS ÁLVAREZ: Carlos Álvarez speaking. Definitely yes, of course, we have many very, very good investigators in many countries that find a lot of information, and I'm speaking about ethical people. People that are concerned

about protecting the users that work as volunteers on many occasions, that have, that are really, really knowledgeable in terms of programming, mathematics, etc.

And they devote their time, free of charge, or else they get a small salary, and they do that in order to protect people. So of course, yes, we do have these investigators. They are there devoting their time and reaching results.

SILVIA VIVANCO: Silvia Vivanco speaking. Thank you Carlos. Thank you for this thorough details presentation. We're reaching the end of this webinar. I would like to thank Carlos Álvarez and Alberto Soto for their presentations. I would like to thank my colleagues, Rodrigo Saucedo, for organizing this webinar.

And of course, thank you all for joining us. Thank you all very much. The presentations are available on our Wiki page, and the recordings will be ready in five days time, and the transcriptions in the three languages of this webinar will also be ready in a week's time, and they will be posted on this webinar's Wiki page. So Wiki space. So that we can go over the information and review it.

With that, I say goodbye. I bring this call to a close, with my warmest regards.

ALBERTO SOTO: Alberto Soto speaking. Thank you everyone. Thank you Carlos. Goodbye.

[END OF TRANSCRIPTION]