BUENOS AIRES – Internet Security & Stability Challenges in Latin America & the Caribbean
Tuesday, November 19, 2013 – 08:30 to 10:00
ICANN – Buenos Aires, Argentina

CHAIR: Good morning to everyone. We are in Buenos Aires and we would like to greet you with some words in Spanish to welcome you to our session during this morning, about the Internet security and stability challenges in Latin America and the Caribbean region. I am from the Caribbean region where many other languages are spoken. Therefore now I will speak in English.

Thank you for coming to this session this morning about Internet security and stability challenges in Latin America and the Caribbean. This is an important session because it's a collaboration between LACNIC, LACTLD, ISOC and ICANN. We're working together to discuss some important issues, events and activities with regard to security and stability in the Caribbean and we are very distinguished panel of presenters.

We are still missing one presenter but we will get started. The presentations will be fairly short because we're hoping to have an interactive session, and our moderator will be one of the newest members of SSAC, Mr. Carlos Martinez. It is now my pleasure to hand over to Carlos, who will introduce the panel.

CARLOS MARTINEZ: Good morning everyone. It's a pleasure for me to be here with this panel in this session. I hope that all of us can have a very productive discussion regarding the security and stability activities we're carrying out in the region. Now we will start with our Agenda. I'll introduce our first panelist – someone who's a friend of mine, Gonzalo Romero.

Gonzalo is a Chief Security Officer of .com Internet, the registry operator for .com. Gonzalo regularly participates in Latin America and Caribbean activities, and communities related with Internet technology and cyber security issues. Gonzalo, you have the floor, go ahead please.

GONZALO ROMERO: Thank you very much Carlos. Good morning everyone. I will deliver my presentation in Spanish because I'm in my region. We have been working on a very interesting project for capacity building in DNS in aspects related to security, resiliency and stability, as Albert was saying before. We are trying to match the efforts among the different organizations that are part of this effort and part of this initiative; such as LACTLD, LACNIC, the Internet society and of course ICANN.

Now I will tell you about the project. This is the project umbrella, the strategic plan for Latin America and the Caribbean of ICANN between 2013 and 2016. This project covers the key interest areas, number two, which has to do with capacity building and outreach. The core objectives are to promote the technical capacity building on SSR issues, in particular in matters relating to the DNS.

The idea is to allocate resources to ensure these issues specifically for ccTLDs and to allow resiliency, security and stability in these infrastructures, which are considered to be critical within the Internet processes. Just a quick overview regarding the description of this project. This is a joint effort between the different RALOs to provide sustainable training cycles, which should be well defined in terms of capacity building, regarding the SSR.

When it comes to the scope and deliverables, the idea is for the deeper technical training and educational components at a technical level related to the DNS, and the stability, resiliency and security at different levels, and according to the different audiences. The targeted groups are the ccTLDs, the ISPs and any other entity or provider related to DNS services.

The project started in August 2013. We have defined some indicators, for example the number of trained or certified professionals in security, stability and resiliency, per year. We also defined the amount of events organized on a yearly basis and during the whole project.

We have identified some resources that are required; for example human and economic resources, for example budget, sponsorship, experts, fellowships, meeting rooms for these types of events, and platforms that are very important to develop, and the support by ICANN in terms of mailing lists or Adobe Connect services, etc.

Of course we've identified the relationship of this project to others, because we have five projects that are part of these great initiatives. One is the group of the Regional Emergency Response Teams for Latin America and the Caribbean region, and some other projects that are related to capacity building in the region.

What are the main activities? Well, we're not reinventing the will, we are working on what already exists. Each of the entities are working on this and offer workshops and events where we can deal with technical, commercial regulatory issues in relation to the TLDs or DNS issues.

Other activities are to identify and map out countries or regional agencies involved in the DNS, specifically in terms of security, stability and resiliency and related to the Latin America and the Caribbean regions, especially at a national or country, or local level.

We're now undergoing stage number two, and this is the identification and categorization of current activities and events aligned or related to a project. The following stage is to generate some commitment or contact with the entities, so as to be able to quantify or measure this project. Likewise, the other activity we're carrying out is to measure or identify specific needs in the region, to increase the awareness and tools to be used for these types of issue.

Likewise, we've identified certain activities and tasks to be developed. We have to develop complementary materials or activities to enhance these training cycles. Of course everything is focused on what's still missing, or on what is required by certain entities in this subject. Finally, to empower training cycles – basic as well as advanced – for all the DNS-related stakeholders.

We've identified training programs such as the SOAC program. We also have the managerial level [attack? 00:11:17] response planning. We have the trainers' processes so as to sustain and maintain the process. This is a kind of matrix we are now developing. On the first column we can see the activities that are now being identified. The second column has to do with how we can contribute to these activities; the budget, the outcome and the audience.

This is the first classification that was done. This is the summary of project number three. Thank you very much.

CARLOS MARTINEZ: Thank you very much. Later we'll have some time for questions but if you have any questions right now? Okay, we have some spare minutes, or else we can do it at the end of the session? Okay. Now the following speaker, according to the Agenda, will be me. My name is Carlos Martinez. I come from LACNIC, and although I'm changing my role in LACNIC, my participation here is wearing the hat of the Security and Stability Manager for LACNIC.

You all know LACNIC. It's the Latin America and the Caribbean address registry. Our main mission is the management and conservation of some Internet number resources. LACNIC is a non-profit organization based on members and in the region we have about 3,000 members. LACNIC has celebrated its 10th anniversary not long ago.

At the end of 2012 we carried out a strategic planning review and held some workshops where we could discuss and debate different issues. The security and the stability issues of the network arose in all of these workshops. We included that in our mission ambition, because we consider that one of our main working areas. The security and stability go together for us.

From our standpoint it's not convenient to separate stability and security. We need to prevent incidents or harmful attacks. We cannot separate that from the stability or the resiliency of the network, because the net is able to recover quickly. So we must include the resiliency in this concept. LACNIC, in the recent past has been working on different projects related to the stability and resiliency, perhaps not to well connected.

Perhaps you may know some of these concepts? For example, the Amparo project was a project that was carried out and funded by the International Corporation Agency from Canada. The creation of materials for training courses to develop emergency services was developed, and then all that material was translated into Spanish and Portuguese.

Then we have the [MASS RAISIS? 00:15:30] Program. We're working on the deployment of root servers in the region. That project started in 2008, if I'm not wrong, after an agreement with the SSA, and then copies of the servers were deployed in our region; six or seven. Now we're working together with ICANN to deploy the L-Root server and we have six deployments up until now.

They've founded their own servers and we only put them in contact, so we have six servers funded by LACNIC and nine that were funded by this [MASS RAISES? 00:16:29] efforts. Then we have training events. We are always carrying out training events in terms of security and stability. LACNIC is now carrying out two major events on a yearly basis. There's one in May, which is a LACNIC event, and in October there's another event shared with LACNOG.

We also provide tutorial activities and try to include in all of them three training activities related to security and stability. This is the instant response training and the wrote-in security training. We understand this is something important to take into account, because sometimes we think only about the DNS security, but there are some other aspects that should be taken in to account.

The other part of the Internet infrastructure has to do with the packages and the correct delivery of those packages. In terms of this we have been working for three years in the development and promotion of RPKI. This is a technology infrastructure and the ITF has been working to create a database with certain interesting parallels with the DNS.

But this is to allow and provide security to the wrote-in system in the Internet. We have deployed DNSSEC in the reverse space. LACNIC associated to its role – you know, LACNIC has a role to operate the reverse DNS directory for the IP's page in the LAC region. When I speak about reverse space I am talking about APA. When we perform the IP queries they're not by names to the DNS space.

We have DNS implemented. The reverse zones are signed and we are now able to accept the registry applications by some of our members. So if there's anyone here interested, just let me know. Something that we believe is a key point in terms of the network stability is the promotion of new IXPs. We have been working together with ISOC. We have delivered workshops. Christian and Sophia are from LACNIC staff and they've been travelling around the continent to deal with these issues.

Another activity we're carrying out is this. During the LACNIC events we try to invent the C-CERTs or the Emergency Teams to meet without any agenda, so that they can gather together and discuss. This might seem trivial but when they meet it's not so simple because the community is sometimes jealous, and it has certain ideas when they need to sit down to debate.

So we're now paving the way and these meetings are now more fluent than at the very beginning. Then we have the LACSEC. This is a security event that we carried out during the LACNIC event in May. This is devoted to security and this is the way in which I started to get engaged with LACNIC. I started in LACNIC by being a moderator, a facilitator. What are we doing right now? We're trying to provide a holistic, coordinated approach to all these initiatives.

These are initiatives that we're carrying out right now, and the idea is to incorporate new activities. We have four pillars – we have capacity building, we have the Internet infrastructure strengthening, outreach, corporation and dissemination, and we have one person devoted to the corporation for public policies and for the development of public policies with the law enforcement agencies and governmental agencies.

Here you will see there are certain concepts that are repeated. As I said before, the idea is to offer training. We've hired a person to offer online training, supplementing the existing training. We'll keep on working on secure routing training. We have also noticed and identified throughout our experience that our region is very different.

There are some places where we go and the technical people are very good – they're very well skilled. You can start talking with them about DNSSEC or about RKPI, but there are other places where some people don't know about basic concepts. So sometimes we need to deliver basic DNS training. We've started to supplement the RKPI training with some other concepts.

Otherwise it turns out to be complicated because not everyone knows everything about this. A very interesting aspect that I think we're not debating so much is the IPv6 concerns and the IPv4 exhaustion. Those who are not deploying IPv6 should be aware that the IPv4 exhaustion has some security issues implied. In the past event of LACNIC in [inaudible 00:23:22], I made my presentation about these issues.

Those operating a web page or an Internet service should take into account their initial ports and the IPs, because the IP will no longer be enough of an identifier to identify things. On the strengthening of the infrastructure the idea is to strengthen the deployment of server copies. We'll continue to work with ICANN [LL? 00:24:00]. It's been very effective to have this partnership with ICANN.

We've been able to deploy service very rapidly. The servers that ICANN uses are very easy to buy in the region, therefore it's something we were not aware of before, but looking back it's a very important asset. Also, the idea to incorporate [Ali? 00:24:24], Patrick was going to be here but we're going to include [Ali?] and we'd like to include some others. We still don't know which ones.

I expect to get together with some other people to discuss which other letters we can incorporate. DNSSEC, although implementation is almost completed, the reverse DNS resolution, we need to search towards scopes for collaboration. We will have to help other regions to sign their zones, etc. Among the functions of LACNIC we'll have an important aspect that we'll need to take care of, which is the register databases, which as you know is the WHOIS service for IP addresses.

One key aspect of this, the item relating to security, is that the WHOIS database is the first step of incident response to try to contact the source of an attack. For that it's essential to have this database updated, keeping it up to date, so as to have the validate contact details. That's an important effort we're trying to systematize, in order to maintain the value of that database.

We, in terms of cooperation, I already mentioned the agreement we have with ICANN for the [LL?] copies. We're working on standardization, especially in the IETF, relating to RPKI. We are trying to have a greater presence in security conferences specifically, because one of the things we've detected is that many times we go to conferences where there are more or less the same people.

It's something that we owe to ourselves to try to get out of our comfort zone. In fact, I attended the first conference, the International Forum of Incident Response, and I was the only person from [earlier? 00:26:36]. After many days I found one person from APNIC, but we didn't know each other, we were just lonely and it was quite an interesting experience. Going into an area where you have to explain where you're from, what it is that you do, what LACNIC is, what are the IPs, etc.

We have an agreement or cooperation with [OS? 00:27:00], which was signed in [inaudible 00:27:03] event, in Colombia and under which we've already conducted a series of interesting activities, such as participating in a DNSSEC workshop for law enforcement organizations in Costa Rica a couple of months ago, and at a public policy development activity in Montevideo last week.

Well, thank you very much. This was the presentation on the security initiatives by LACNIC. I think we have the panelist we were missing. Okay, as I was telling you we'll have space for questions at the end, but if you'd like to ask a question now you're more than welcome. I'd now like to introduce our third panelist, Christian O'Flaherty from the Internet Society.

Christian, you've made it hard for me, sending me the introductions by email in English. Christian is the Regional Internet Development Manager for the Internet Society for Latin America and the Caribbean. His job is to promote growth and sustainability of Internet access in the region, in areas such as capacity building, infrastructures, barriers to policies and quantity of traffic. Christian, another friend of mine, go ahead.

CHRISTIAN O'FLAHERTY: Thank you Carlos. I'm going to give my presentation in Spanish, even though the slides are in English. I see that the majority understand Spanish so it's easiest for everybody. Can we go to the first slide please? I don't know of another Internet organization which dates over 20 years. It turned 20 last year. It's an organization the objective of which is to keep this Internet model open. The motto or ISOC is that the Internet is for everybody.

But this Internet model, this ecosystem, is based on some pillars that have an impact on security issues, and during my presentation I'll try to describe the relationship between this Internet model we have and the impact on security. Then I'll try to see how leveraging this model we can tackle those issues from a global perspective, and then try to see how this impacts our countries and businesses.

Those pillars I described, which are very important to preserver, are in a way the ones that made the Internet so successful, so scalable. One of them is global connectivity. Every time you include one new device on the Internet it's visible by absolutely everybody – all the other Internet devices. This global connectivity, which is a characteristic of the Internet, is a fundamental pillar to the Internet, which we need to preserve.

Another important characteristic is that all new services, all new protocols, discoveries and applications developed on the Internet, are done by entrepreneurs who do not need to request authorization from agencies or institutions. We tend to say that this is information for anybody. Anybody can include things, services, new application on the Internet, test them, and some will be successful and others will not, but this makes the internet so dynamic and so changing in time.

Another important characteristic is this openness. It's very accessible. Anybody can contribute to the network. Anybody can be part of the organizations that are relevant on the Internet. This openness is one of the most important pillars for scalability. This is what has made it grow as much as it has done. It's important to maintain this so it can continue to grow.

Finally, collaboration. Although the Internet is a network where many suppliers compete, it's fundamental to have collaboration among all parties; not just businesses but all the organizations and all stakeholders, as we call them – all persons, institutions or governments and businesses involved in the Internet service.

Now, all these important pillars that the Internet Society wishes to preserve, has an impact on security aspects. For example, this global connectivity, this possibility of connecting any device having access to any other device connected to the Internet, causes the attacks and the incidents not to have borders. We no longer need to be prepared in our own environment, region or country, but threats come from all over.

So this is a very important feature and a very important threat. This other pillar, which relates to the possibility that any new service can be included in the network easily, is also leveraged by the creativity of hackers and those who benefit from this to develop new viruses, malware and applications that are really harmful from the point of view of security.

The fact that it's such and open platform and it's possible for software to be distributed so easily, is also an important vector for attacks. As we've seen, viruses and any malware is very easily distributed on the Internet because of this openness feature. On the other hand, this important feature, which is the multistakeholderism, the possibility that e can all cooperate and that it's all so open and voluntary, makes it very difficult to impose things.

In closed environments we can demand and impose authority, however on the Internet it's through cooperation that we have to solve our issues. So what are these characteristics of security, and how should we tackle them, considering this model we're defending? To begin with we must accept that it's an ongoing task. Absolute security does not exist, so it's a task that we must always be wary of and must always work on.

It's not a defect of the Internet, it's a characteristic that we must always take into consideration every time we make decisions. Then we are all responsible for security. It's a collective responsibility. This is important for suppliers. Suppliers and every network on the Internet we log onto are responsible for internal security.

We must protect ourselves from one that can come internally, and we also have to be responsible for the movements users make within out network, and the attacks that they may be generating outwards. So we must be good Internet citizens and be vigilant in both senses. This participation requires more collaboration in these respects to tackle problems together, to agree on diagnosis before acting and to create plans that are supported by all organizations.

In order to tackle these issues by preserving this model, which we believe is essential, we need to find a good balance between not expecting to have authority, not trying to restrict the geography of the networks and thinking of more global policies to tackle security issues, instead of regional or geographical-related policies; trying to preserve open standards.

One of the organizations that ISOC strongly supports is the IETF, which develops open standards, which are fundamental for the growth in the network. We will now see how with these features that we wish to preserve but have an impact on security, we can create some global activities to later implement them in the region and in the countries.

ISOC has some initiatives related to security. I'm going to mention the most important ones. I'm also encouraging you to go to the ISOC web page where you'll find further detail of each. First of all, trust an identity – more from the point of view of the user. What things affect users from the point of view of security and their privacy, and which authentication methods are being developed?

What is identity within the Internet? The concept of a credential identifying us, uniquely set as an ID number of a passport, no longer exists in the Internet. We have an identity that's built by different characteristics that we have as Internet users. When we use the Internet we have a profile – a series of attributes that define us in different environments, and you may have more than one identity, depending on that set of attributes.

There's a series of tools to preserve that identity, to prevent abuse from those identifiers that reference us when we use the Internet. The idea is to try to have that identity managed by attributes as simply as possible so that it only serves a purpose of the service we're using from the Internet, instead of having an absolute description of each and every one of us as individuals in everything we do on the Internet. This is going to enable us to have a certain level of privacy; at least privacy restricted to the service that we're using.

There are also problems in terms of technical aspects. I always describe problems in global terms. ISOC Internet Society with problems that affect the Internet as a whole. First, in terms of the promotion of IPv6, which Carlos was saying has an impact on security, which we need to be aware of, now DNSSEC is now a reality, we can say that it's being used more seriously. DNSSEC has been active for many years. It's a secure way to solve Internet names.

So far, every time we enter a name and the application receives an IP address, it's been using a mechanism that could have some issues. It could be interfered with and we could obtain results different than that we were seeking. With DNSSEC the resolution process may become more reliable. You may obtain responses from the DNS service, the resolution service that we can trust.

Besides this response, we may have additional information that may make the use of the Internet more secure. As I was saying, it's been going on for many years, it's matured technically speaking. However, in the operation we are a bit behind as a community. Currently we may say that there's a more serious use of DNSSEC.

We have 135 root domains, TLDs that have been signed. The new TLDs that are being launched will be signed also, and there's going to be a DNSSEC workshop tomorrow, Wednesday at 9:45 am, and you are invited to attend if you wish to know more about DNSSEC.

The next item is related to the stability of the routing table. The stability of the routing table is related to RPKI, as Carlos mentioned. RPKI is this mechanism to make a more reliable use of some resources; in particular the blocks of IP addresses when transferring them to the global routing table. The objective of this program is to use this and other tools so that the information in the routing table becomes more robust, more reliable, more secure.

These efforts have the objective that the service providers using PGP, the protocol to enter information in the routing table, to include networks in the Internet, follows some policies that have good practices and recommendations so that the Internet can be more robust in the routing infrastructure. You can find more information about this project of secure or reliable routing in the ISOC web page.

In a higher-level, but in relation to this, I can tell you about the promotion of current operational practices in the operation. There are many standards and many ways to implement these standards. When we configure a unit on the Internet, where there are multiple configuration options to obtain very similar results, this leads to a bit of a messy use of these standards and this unit and the deployment of these services.

The objective is to create recommendations so that this deployment that we make of these configurations in the units, on the Internet, has a better quality, a better security, a better reliability. This is why we're discussing among operators, which are the better ways to do things, the better practices.

The discussion groups normally are network operator groups, the NOGs, the persons among the operators who are part of these discussions, because they're the ones that will have to deploy this on their network. Or, the RIRs will hold meetings where members who are also operators, discuss policy and operation topics. This is another area where they can deal with those topics.

These recommendations will be recorded in recommendations for the community to follow those better practices in the configuration of their networks. There are some other initiatives, however I would like to show you how to implement and how to take these global initiatives to countries. There are certain mechanisms, as I said before.

We have the NOGs or the North American NOG, we have LACNOG and many other regions have their own groups where operators discuss and debate operational issues. Within those operator groups there are specific groups for specific issues. In our case, in our region, there is a group devoted to these best practices where operators debate about best practices to deploy services.

We would like to have local operator groups. For example in those countries where there is critical mass operator groups, well, we have to promote those activities so as to agree on best practices to debate on operational issues, connection issues, and to solve certain other problems relating to operations or security. It’s very important that operators gather together and debate to solve the problems arising in the region.

There are some other vital mechanisms that are important to carry out this policy, and this is collaboration with other organizations. As Carlos said before, LACNIC has been implementing many other projects to carry out the initiatives. The same applies for LACTLD, LACIPX – which is the Internet Exchange Points Association –they offer training courses.

Each of these groups embrace these initiatives to fulfill their projects. This was a regional level. Now we need to focus on the local level in each country how we can put all the initiatives into practice, and in that case it’s important to work with universities in the academia sector. So we are at your disposal if you know about any academic meeting or any university interesting in collaborating with these initiatives, we can keep in touch.

Then we have promotional organizations so that we can implement all these initiatives. We also have programs for people interested in the development of standards, for them to participate in the IETF. As Carlos said before, working with the IXPs is important because it's there where we can address the incidents and the security problems that appear.

Then we have governments and regulators. They're quite concerned about these issues. They need a different standpoint – they need a different approach because on the Internet things are not regulated, so there is not enough authority to solve problems. Another mechanism that we have to work at the local level, is the ISOC Chapters. I invite you to participate.

This is my last slide, so my request and my message is to try to see how these global initiatives can be taken to the countries and for that we need your help. Thank you very much.

CARLOS MARTINEZ: Thank you very much Christian. I was listening to you and it's very interesting to see the many activities we're carrying out, and this is something very important. Now I'll give the floor to Gonzalo. I won't introduce him again – I know that you know him. He will now speak about the security in the ccTLD .co.

GONZALO ROMERO: This presentation is within the framework of these initiatives because our ccTLD in Colombia is compliant with security, stability and resiliency. So this is a very quick agenda. I will explain first of all our motivation to develop these issues. Then I'll speak about some security policies, what we do in terms of knowledge transfer and corporation actions. We have a process for malicious activity monitoring that was implemented three years ago. Then I'll let you know about our main challenges in terms of cyber security.

To give you a context, .co is a private company created three years ago to manage the domain name .co, to promote it at a global level. We are a company dependent on the IT Services Ministry of Colombia. We see this from two perspectives. On one hand we're the managers of the ccTLD at a national level, and we're very committed to the protection of integrity, stability and reliability or resiliency of the TLD, as well as with the global remit of our registrants and all the registry chain.

As an agency managing the ccTLD, for us the security is added value for our registrants. Somehow we engage in those initiatives contributing to improving the resiliency and the security and stability of the network. This is a summary of the security policies that we have: first, it is price. We are not a cheap domain name. The domain name has a cost of $30 per year. We are not a $5 domain name.

We believe this is an important component avoiding the abusive use of the domain name. Then we have good practices on IT security and business continuity. We work with New Start – it's our partner – and then we use MAM – I will let you know about this later on. This works with security and global positioning for our ccTLD. In terms of security, we have agreements with our registrars and with our distribution channel.

Each registrar is assessed in terms of purposes and values, so that they can offer added value services to the users. We actively participate in all the national, regional and global efforts. This is a good opportunity for us. In terms of knowledge transfer and cooperation, we have our community, which is called CODNS. This is a kind of Facebook page. We have 50 members contributing very openly and actively in terms of DNS security.

That community holds an event on security and stability on a yearly basis. This event takes place thanks to the support of the ISOC, and the support of ICANN and LACNIC as well. They joined us in our effort. This is a good opportunity to thank those organizations for their support to strengthen our topics at the national level.

We're supporting the certification of our security centers. We have five certified centers and we're about to have our National Incident Center certified. This will happen at the beginning of December, and the secret for us is the cooperation. We have celebrated agreements with the law enforcement agencies, other ministries and incident centers; the academia amongst others.

In global terms we have entered into agreements with different organizations such as Microsoft. We have security agreements. We also have agreements for minor protection and we've celebrated agreements with the DNSORG. We also have agreements for security and stability and incident resolution. We have signed a resiliency agreement with the World Economic Forum and we're monitoring security.

This is our process. We have been working on it over three years. It is non-invasive monitoring to the DNS zone of .co. We validate [inaudible 00:57:36] domain names, most of them are [balinable? 00:57:41] but there is no bad intention, so what we do is a validation process by means of the Certification Center. This is New Start. We are focusing on those alerts, for example phishing, farming, hijacking, pornography, spoofing.

So we have a filtering process to avoid duplication and we eliminate false positives and filter that information and send that information to New Start for them to notify the registrars and registrants, because we work very closely with them. When we identify certain situations with terror, for example, with our domain name t.co, of course it is easier and better for us to work directly with those registrants.

However, the process is quite similar in terms of notification. So if the incident continues for a certain period of time we suspend the domain name to avoid any problem in the security, stability and resiliency of the domain name. There are certain special cases, such as [rockfarm? 00:59:18], piracy or spam, where we scale those issues to the law enforcement agencies.

We have celebrated agreements with different agencies and we work together so as to identify a way to address the issue and to take action. Any court decision, in the case of domain suspension, of course we take that into account. Our most important challenge is in terms of security cyber squatting, and any infringement or violation to the terms of conditions set forth with the registrants and registrars as well.

We have proactive monitoring of hourly domain name registrations, so as to avoid intellectual property issues. When we detect or identify critical situations in terms of cyber squatting, we send that information from our TLD manager and we remind them how to manage the security issues in our domain names. Thank you very much.

CARLOS MARTINEZ: Thank you very much Gonzalo. I will speak in English because I know it's his mother-tongue. It's a pleasure for me to introduce Patrick Jones from ICANN. Patrick is ICANN's Senior Director of Global Stakeholder Engagement, and he was previously with ICANN Security for four years. He's a regular speaker on security, stability and resiliency issues in the community. Patrick, the floor is yours.

PATRICK JONES: Thank you everyone. Good morning. As you note, I have a new role as of the last couple of weeks. I've recently joined Rodrigo and the rest of the Global Stakeholder Engagement Team. I had previously been with my colleagues John and Dave from the Security Team, but I'm continuing to work with them as a Liaison between the Security Team and our global stakeholder engagement efforts.

With that, ICANN Security has a long history of collaboration with the Latin America and the Caribbean region. We do this through history of training, engagement and awareness activities. All this builds from the requests that we receive from the region. We take in the interests from the community and match this up with ICANN's obligations under the AOC, and also the SSR Team's recommendations.

Then we match this up on an increasing basis with the new Latin America and the Caribbean strategy. We want to make sure that the activities that the Security Team and ICANN provide match up with the goals and objectives from the Latin America and the Caribbean strategy, as well as the goals and objectives of ICANN's partners in the regional TLD organizations, the organizations that are listed here, as well as the ccTLD community and the growing gTLD community from all the regions.

From a security perspective we build bridges. In the Security Team we connect people and stakeholders across diverse communities in the Internet ecosystem. Usually the Security Team acts as a conduit between either law enforcement or the ccTLD or TLD operators, in providing a contact point between those Teams – either in sharing of information of incidents and threats, or of providing training and awareness of best practices and new experiences.

The team can share and connect the registries and law enforcement to have basic DNS awareness, DNSSEC training, and also provide information on IPv6 and other capabilities. Our team has worked with the Commonwealth Cyber Crime Initiative, the Caribbean Telecommunications Union, [OAS Secte? 01:04:29] in a number of events, including this past Friday in Montevideo and also earlier in the week with the OAS Cyber Security event.

In the Washington DC area we participate in USTTI training. I know a lot of participants from the Latin America and the Caribbean region have taken advantage of that opportunity, to come to Washington and cover a variety of courses that touch on cyber security. We also work to share information and learn from TLD operators – particularly ccTLDs – to understand how you respond to threats.

I'm hoping to hear more about how operators have responded to hacking attempts and dealing with botnets and taking down malicious domain names. So I'm hoping that will be one of the topics of discussion in the remaining minutes or at least later in the week. As Carlos mentioned, we're also helping with deployment of L-Root nodes in the region, sharing our best practices and our experiences.

I'm conscious of the time. I know there's 15 minutes left, so I'm going to make sure there's enough time for questions.

CARLOS MARTINEZ: You were really quick. You still have four minutes if you want?

PATRICK JONES: Okay, well, I will say one of the things that we want, from the Security Team and also from the Global Stakeholder Engagement Team, is to hear from the region on what types of training and activities you're looking for. I know we've quite a bit of work to do to help with the current LAC strategy, but if there are other activities and other ways that we can share knowledge and information we want to do that, and do that in a way that meets the needs and requests from the region.

CARLOS MARTINEZ: Thank you very much. Now I would like to introduce our last panelist for the morning; Robert Martin-Legene. Did I get that right?

ROBERT MARTIN-LEGENE: More or less.

CARLOS MARTINEZ: Okay. Robert Martin-Legene has 20 years of experience working with the Internet. He started a commercialized [inaudible 01:06:42] back in the days when they had pools of dial-in modems, so I remember those times too. He was on the first row to witness the transition from one technology to the other.

Until now, when you have [themes?] being delivered [inaudible 01:07:00] at your home at the click of a button. I changed [inaudible 01:07:02] imagine 2 years ago. Robert now works for PCH, a non-profit organization, which specializes in Internet infrastructure. Robert?

ROBERT MARTIN-LEGENE: Thank you very much. If you want to know, it's Robert Martin-Legene, but I don't even care about my accent and the name actually. PCH focuses on strengthening the infrastructure of Internet and countries and in regions, and we do that by… Our main focus originally was to set up IXPs and we actually created the IXP in the world on the US west coast, I believe it was.

Since then we've been involved in the creation of one-third of the IXPs in the world. So we have quite a lot of experience in what to do and what not to do – good ideas and bad ideas on policy. We help governments form legislation, if that is needed, and we hope it's never needed but sometimes the market just won't come together by itself. We also do DNS Anycast for TLDs and some DNS hosters.

With that I'll continue. The main advantages of having an IXP is that it keeps your Internet local basically, it makes sure that your traffic doesn't have to go across, in this case, all the way up to Miami and back, which is usually the case in Latin America and Europe. It used to be that everything used to have to go to the US and back. That was 20 years ago.

There was a lot of effort on that in Europe because circuits back then were much more expensive than the expensive circuits that you see here today. The advantages of the IXP is that it keeps your traffic local, it stabilizes the Internet infrastructure because the longer you go the more likely it is that somebody trips on a cable or somebody in an other organizations that… You could have the traffic traverse six or seven organizations before you actually get to your neighbor.

So somebody in the middle of that would suddenly do maintenance and nobody knows, and if you have the IXP you usually just have two providers, maybe three, to go through. You have a lot lower latency. Basically it gives much better quality. You can use it for services that you wouldn't normally put on a high-latency link. If you ever try to watch live streaming TV from some TV station faraway, you will see that the quality is really bad when you have high-latency.

The low-latency enables that you do more real-time trafficking. You can use it for video surveillance, you can stream… Radio is not really a problem but video is usually a serious issue. Then it really lowers the price of every byte, which in turn means that the providers will usually…

Usually the international links will be the ones that are really expensive, that they will upgrade only when it's very saturated.

However, the local link that goes to the local exchange point is so cheap that it doesn't require a lot of talking from the local engineering guy to talk to the ISP's CEO to actually get more resources to upgrade those circuits. So basically you have a lot better quality when it's local traffic. The distance as a risk thing is a little bit also about when your traffic goes through other jurisdictions, physically, and you lose control.

I think lately we've seen that, there's been a lot of focus on that, especially with the US, but the US is not the only problem, where they actually go in and listen to your traffic. There are probably other countries that do the same, they just don't tell you. Countries that do not have an IXP seem to be suffering a little bit from content leaving their local area.

Usually you see it with a newspaper or… Somebody wants to provide content at a quite reasonable quality to the local community, but there is no exchange point so what they do is go to the closest point that gives reasonable quality to everybody – reasonably bad quality to everybody, but it's the same quality. So they can predict the behavior of the quality that the user gets. If you do not have an exchange point you would go to the exchange point or you would go to Miami with this.

The problem is that the hosting for popular sites, a [inaudible 01:13:23] will then leave your own country. It will take money out of your own economy and it will create jobs in another country instead of your own country. When you have the content leaving your own country you basically have no way of controlling what goes on.

The legislation thing is not something… People keep using the scare tactics of child pornography and everything – I think basically every country is against that so that's not really a problem, but there could be other things that were important for a country to focus on, like privacy. We see that once we have the IXP, even if it might have taken ten years to create it because of political blunders and ISPs not wanting to cooperate, once it's there it's usually very difficult for the ISPs connected to actually disconnect.

They don't want to because even if they try their users would get really upset, the regulators would get really upset, and you normally do not see the death of an IXP. So there must be a reason for… Once it exists, for it to keep existing, it must have a value that's very important, and when you don't have it you don't see it. I think that's probably some of the problem we're seeing right now.

In some of the countries in the region we're seeing that they're really trying, but some forces inside the country are fighting for the wrong motives. They think that it will give them less business, and experience shows that that's not the truth. Finally, for the e-government, you could consider Internet to be a vital part of your national telecommunications infrastructure, and I think almost all countries do that.

If that's the truth and you have organizations within the government, or even from citizens to government, who want to talk together, it doesn't make sense that if you build a road from one city or another and you want to pass it through a neighboring country first, you want to be independent, you want to be sovereign.

If you do not have an IXP you could consider a vital part of you infrastructure to be very vulnerable to let's say – maybe not external aggression; let's hope that doesn't happen – but there could be factors that are way beyond your control. What have we seen lately? We saw with the NSA a scandal that has appeared lately, that there's been a lot of international political backlash.

Especially in Brazil, that helped spark a privacy law that says that all data from users must stay inside the country, or something like that. That immediately caused some content providers to reconsider their plans. Google pulled out their public DNS services, and I don't now what else they pulled out, but it's interesting to think that something as simple as asking for the privacy of your citizens causes international companies to reconsider their plans for being in your country and providing content.

So other countries are fighting. We have seen Paraguay has a small, not very functional Internet exchange point that they're fighting to make work. I don't really know what's going to happen with that. It seems to be crawling. We have Bolivia that's now passed a law this year that should make an IXP appear – some time ago – and we have other countries that really want to do this.

It's not only engineers that can see that it's a practical thing to have a two-millisecond turnaround time on your packet – it's also the government that can see that you need to be able to have an infrastructure in your country that, when two of your organizations inside the country talk to each other, that it's a national thing – you don't need to export your traffic for this.

The minute you send your traffic outside your borders you lose complete control of it. You have no idea to see if anyone is wire-tapping it. Anyone can do route injection… Well, they can do that anyway but it's more difficult to hijack traffic. They can do DNS injection, there might be intelligence agencies that actually do that currently. They intercept a DNS request and they could forge a reply, because who says they can only read, right?

So they could be injected a fake UDP packet and giving a false reply to certain users that they might actually want to hijack DNS traffic from. After that it's very trivial to consider controlling what the user sees. IXPs are slowly becoming very efficient. They've been very efficient in Argentina and Brazil. What we're seeing now is that countries are starting to connect to each other.

I set this morning at my home to try to connect to… I think it was the L-Root server? I live here in Buenos Aires. I did a trace route and I went from Argentina to Peru, directly, through the IXP there and to the NIC that has a copy of the L-Root. So the traffic is regionalized. The need for going to the US every time you need to get content that's not on your own ISP doesn't happen anymore.

The situation is changing. The regionalization that Europe saw 10-15 years ago, with now the very big IXPs in Frankfurt, Amsterdam, London and Paris, it will happen here too. You need some cables but they're being dug down as we speak and it's just a question of maybe even subsidizing those. I shouldn't talk about economy probably.

So you could consider that getting the IXP up and working is the holy grail and everything is done. That's just not true at all. The Internet is very, very young and the threats we see today is just the tip of the iceberg. There will be new threats as technology becomes more and more advanced, and the IETF, one or two weeks ago, had a statement sparked by the NSA scandal also, that said that it's so easy for anyone to intercept traffic on the Internet because nothing is encrypted.

They probably have not been able to intercept and decrypt a lot of the encrypted traffic on the Internet, but it's not needed because most of the traffic on the Internet is not encrypted at all. I saw a tech talk the other day. I think it was [Yarri? 01:22:30] that was saying, "Most people say I have nothing to hide, so I don't care if NSA or anyone else listens to me, because I have no secrets," to which his reply was, "Well, then I cannot tell you any secrets."

That's kind of true. The outcome of the IETF Technical Plenary was that everything on the Internet should be encrypted, even if it's your cookbook recipes or whatever, encrypt it. There's no need not to. Encryption is easy. Basic encryption is easy. We have the DNSSEC, which is a little bit advanced, but with DNSSEC you can secure TLS certificates inside DNS. You can get your website encryption basically for free.

Now, the Internet drafts to TLS encrypt SMTP email, also by using DNSSEC encrypt certificates. I think the IXPs are a good start. I think everybody must have them, and within the next five to ten years I think we'll see that the landscape has changed, and I hope that DNSSEC will be more prevalent. We've all been here for many years and we all think that there's been so many changes and we cannot imagine what will be happening in the next 20 years, but I've been here 20 and I have no idea except that the internet is still young.

CARLOS MARTINEZ: Thank you so much Robert. This was our last presentation for the morning. We have about two minutes for questions, if you would like to ask any questions?

SALA TAMANIKAIWAIMARO: I'm from Fiji and I'm also on the ALAC, but my question is, I'm coming from… I chair the Legal Sub-Committee of the Cyber Security Working Group back home and I'm very much involved in this area. I was very impressed with .co's presentations and I hope it will be available on slides, particularly for countries like ours who are working on ours. So I'll just put that out there.

The next question is basically to all of you I suppose. It's a question and a comment. You know how recently there's been news reports questioning the integrity of NSIT's approved cryptographic algorithms, and that sort of thing? I note that there's been a recommendation from the Internet Architecture Board to reopen the comment period on SP 800 900 A, and that sort of things, particularly when we're talking about things like encryption.

I was very pleased at the IETF 88. I didn't attend by I was watching the video when they were talking about… Particularly Bruce Schneier, when he was talking about moving it to the fringes and that sort of thing, and decentralizing it. I think from a technical perspective – I'm not a technical person, I'm a legal person, but I have worked for TELCOs in the past, and ISPs and that sort of thing, and a corporation with the law enforcement – but I think the discussion has to take place, particularly in relation to strategies and that sort of thing.

Not so much regulatory control, but certainly discussions in terms of policies and considerations. So I'd very much be interested in what your take is on that particular process, in restoring integrity and faith in standard systems. Thank you.

CARLOS MARTINEZ: I'm going to answer regarding the IETF meeting you mentioned. I was there and it was very interesting how the technical community addressed the problem. One of the presenters did an approach which was agreed with by most – that this should be treated like an attack, as we address an attack. We should see what we can learn from it, what should be improved, and from there a whole discussion on focusing on the current security implications of most of the services we're currently using.

When most of them were deployed, the security was not a real concern that that time. For most of them it was optional to use encryption, for example. But now there's this and it's completely different, and it's not just because of that incident – it's in general; the privacy issues, the attacks are affecting many different areas on not just the infrastructure, so it should be addressed in a more holistic way.

This is not a real concern on the technical community, and it's addressed differently than it was in the past.

GONZALO ROMERO: I would like to make a comment on the cryptographic algorithm aspect of the argument. The current feeling or opposition of the community is that the fundamental mathematics behind the cryptographic algorithms is not compromised. The basic math behind the algorithms is sound. What have been supposedly altered by some efforts of some organizations are some components used when you implement those algorithms in software, or what are basically called the random number generators.

Those can be easily replaced, without altering the nature of the algorithms themselves. Cryptography continues to be a tool that we can use to protect privacy, even if we have to revisit some standards that were approved in the past.

YULIYA MORENETS: Thank you. Yuliya Morenets from TaC – Together against Cybercrime. I'm also with the Secretariat of EURALO. Practically what we do is… It's mainly a comment and not a question. We work on cyber security strategies advising entities and awareness-raising programs. I was actually involved of the harmonization of legislation in the Caribbean region, in mainly drafting the cyber crime interception of communications legislation for Haiti.

I wanted to just share a initiative that was born due to the consultation meetings in Haiti, which was at the Institute on Cyber Security for French-Speaking Countries, which will be based in Haiti. Mainly we will focus on capacity building programs and enforcement and awareness-raising practically. We would be happy to bring this to cooperate and to bring to the table. Thank you.

CARLOS MARTINEZ: Any more questions or comments?

MAURICIO OVIEDO: Hello, my name is Mauricio from Costa Rica. Basically we are actively promoting the use of DNSSEC, not just for the domains that we manage but also for the country itself. It was interesting to hear that there can be some cooperation to promote to provide training to the people, so that they can no better how to use it and why it's necessary. I'd like to know a little bit about what type of cooperation can be provided in order to integrate different entities in Costa Rica?

We've been doing different activities where we include DNSSEC, however it would be interesting to have a training workshop or something like that, specifically just for DNSSEC. Would that be possible? Thank you.

PATRICK JONES: We've done DNSSEC training with Colombia but we've also been talking with Rosalia from NIC Costa Rica about planning a DNSSEC training in Costa Rica, and open it up and invite participants from other experts within the region that are interested in receiving the same training.

So we're actively trying to find the right dates and also working with Rodrigo to make sure that this is an event that fits under the Latin America strategy under security and stability. So look for more information about upcoming trainings in DNSSEC. It's something that we're definitely doing.

CARLOS MARTINEZ: I want to add something very short. Four of us are working for organizations that are willing to help, and there might be specifics that we can discuss offline, and we're open to all of you, because each of us has different ways to support. Let's talk after this meeting.

SALA TAMANIKAIWAIMARO: Sorry, one last quick comment. In reference to Packet Clearinghouse, most of you will know that there are very few IXPs in the Pacific – I come from the Pacific, which is very much like the Caribbean. In fact, the highest cost of Internet access is from the Pacific, at least four of those countries are rocket-high costs and very poor resilience and that sort of thing.

But I'm very happy to say that Packet Clearinghouse was very much involved for the past three years, at least, in terms of strategy and just being open to answering questions. We rolled out an IXP executive briefing last year where we had somebody from the Caribbean visit Fiji from Packet Clearinghouse when we ran the executive briefing.

After eight months all the TELCOs were there and IXP was set up; although it's just two peering, technically there should be three good-case peering. But it has to start somewhere.

ROBERT MARTIN-LEGENE: Yes, that's exactly the thing. I don't know if you've actually seen traffic graphs from that IXP – I don't know which one you're actually talking about – but usually what you see is that the traffic does go very high up and people will really see that the Internet works a lot better in the local community. Especially in regions where you are, the traffic suddenly becomes something where you can actually put out a video of something that happens in the neighborhood, without considering that it needs to be downloaded from a satellite.

CARLOS MARTINEZ: With this last comment we'll conclude this session for the morning. Now we will adjourn this session. I'll give the floor to Albert and he can give the final words.

ALBERT SAMUELS: Thank you for these very informative and interest-generating presentations. As I said at the beginning this is really a collaboration. You can see from the slide the organizations that are working together in Internet security and stability in the region – LACNIC, LACTLD, ISOC and ICANN. I'm happy that the audience feels that there's some way that these organizations can work together to help you in all of your respective situations.

The last quick point is that all of the presentations are available on the schedule page for this session. You can download them in PDF format. Finally, I'd like to thank the moderator, Carlos, and I'd like to thank all of you for coming to this session. [Applause]

[END OF TRANSCRIPT]