COPENHAGEN – NextGen Presentations
Monday, March 13, 2017 – 11:00 to 15:00 CET
ICANN58 | Copenhagen, Denmark

DEBORAH ESCALERA: Okay. Next Gen while you're presenting, we're going to actually be, unfortunately, timing you. So, keep an eye when you see the signal. This signal. That means you have one minute left. This signal. Like, I'll give you a signal that means one minute left. Okay.

[SPEAKER OFF MICROPHONE]

This one minute. I mean, your slides shouldn't take more… I mean, you knew that you had 10 minutes. There is 15 of you, so it's going to take quite a while to get through 15. So, we'll give you a minute warning. If you run one or two minutes over, it's not the end of the world. Just relax.

Just go over your names quickly.

[Inaudible] or Fellow? Carolina Matamoros, should I say Matamoros or [inaudible]? Matamoros. Should I say Ferrari? Ferrari and I don't know how to say your last name. Oh, [inaudible] is the last name. Yeah, I know it's [inaudible], but do you want me to say Ferrari or [inaudible]?

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

But how do I say your last name. Come over here. It's a really long last name.

Okay, and Sara Dushi. Should I say Sara? Sara, should I say Sara? Okay. Jacqueline [inaudible]. Oh, Jackie? Is it [inaudible], or how do you say your last name? Just say Jacqueline? Jackie. Okay, Jackie.

Katharin Tai, Krishna Kumar, Luã do you want me to say your entire last name?

LUÃ FERGUS: No, no, Luã Fergus.

DEBORAH ESCALERA: Okay. Matthias. Would you like me to say your whole name? Matthais? Nertil Berdufi? Is that last name correct?

NERTIL BERDUFI: Yeah, it's Berdufi.

DEBORAH ESCALERA: Berdufi.

NERTIL BERDUFI: It's a little bit difficult.

DEBORAH ESCALERA: Olga. How do you say your last name, Olga? Kyryluk? Kyryluk. Okay, I'll try. Peter Chon. Is it Chon?

PETER CHON: Chon.

DEBORAH ESCALERA: Chon. Chon. Valerie Filnovych. Yeah, I can say that one. Yousra, how do you say Yosra's last name? Yosra, how do you say your last name, Yousra? I can't… Put your microphone on.

YOUSRA HSINA: Hsina.

DEBORAH ESCALERA: Yeah. Okay. So, I want to remind you all that you're being recorded. So, when you do introduce yourself, speak slowly. Introduce yourself. Let the audience know where you're from, because we have interpreters that are interpreting at the back of the room, so we want to keep that in mind. And we're going to go ahead and start. We're running a little bit late.

So, thank you to the audience…

Okay, let's try this again. Thank you to the audience members for joining us today for the ICANN 58 Next Gen presentations. First up we have Abderrahman Ali, with his presentation. And Abderrahman, do you want to come and get the mic?

ABDERRAHMAN AIT-ALI: Hi everybody. So, today I'm going to talk about block chain. I'm going to be there. All right, apparently it's not working. Yup.

No? Yeah.

All right, it's working now. So, first of all, I'm going to introduce what's block chain, some characteristics, and then talk a little bit about the history, it's not a long history actually. And I'm going to let some of the applications, which is very interesting, and one of them is a project I'm working on.

And another one is an idea for ICANN to work on that as well. And then some conclusions. All right. What's block chain? Block chain is basically a peer to peer public ledger that a distributed network of users are maintaining. So, the idea is to make a transaction and to have a recorder ledger for it, and then we have a system for verification and storage.

It's always like some kind of cryptographical tool. And the idea is to have a [chain?] list or record, or orders. Okay, here are some of the characteristics of block chain, which are very, very appealing when it comes to internet services. So, one of them is openness, it's basically open to everybody to edit, and contribute to the blog, to the ledger.

Also, decentralization, which is a key characteristic, no one controls the ledger. It's basically decentralized. Also security, this is also a very important characteristic. The ledger, the storage system and the verification system used cryptography, which is going on in terms of research and development.

Also, resilience, there are lock, it's a distributed system, so we have a replication process going on. And many other characteristics like immutability, that was is in the ledger, what has been written cannot be modified, consensus. It's basically about trust. And example is Bitcoin. Traceability, so it's a chain block, so you're basically crack down all of the transactions.

Here is an example, Bitcoin is a pretty famous example of block chain application. It's basically a crypto-currency and also a payment system. It's basically based on block chain, and this is just one application that launched a list of other applications. Yup.

Here is some history. So, it all started in early 90s, so it's not that old. It started with research work, going on about cryptography, and then there has been like a mechanism, a concept introduced by Nick [inaudible]. It's not… It's just a concept. It's called Bit Gold, but then the execution of this concept was later on done by [inaudible], in terms of Bitcoin.

And then there is another wave of application which is referred to as block chain, 2.0, which goes beyond the crypto-currency and the financial applications. And I'm going to talk about some of those applications later. So, those are basically like a spectrum of, this is a spectrum of the different application of block chain. It's basically a basket that reveals every day new kind of application, but it basically spans digital currency, it also started with digital currency, now are going to smart contracts, and then security, record keeping.

And there are many, many applications. It's just, feel free to imagine some kind of application that can use the concept, and then you have an application. So, the most famous application is the financial sector. So, we have crypto-currencies, as I mentioned, Bitcoin. We have another crypto-currencies which is [inaudible], they started as crypto-currency, but now they move to smart contracts, which is basically a way to use computer protocols to facilitate transactions and contracts.

A very famous product is the [Dow?] project. They are basically working on smart contracts and how to apply block chain for smart contracts. There is also like funding, which is also one part of a project I'm working on. And this is like the, a map of the different companies and projects they're working on, financial applications.

It's basically a lot of companies, because there are a lot of financial incentives and potential there.

Okay, now internet of things. This is another application, or another sphere of applications that block chain can be applied to. One important application that will basically change somehow the internet service in the future is digital identity, so there are a lot of projects going on in order to use block chain to identify people digitally basically.

And also a lot of projects going on in internet of things, security to reduce vulnerabilities. Yeah, and some other applications, one of them is an application we thought about, which ICANN can actually use. Yesterday, we attended ICANN DNSSEC, and one way actually to further increase the security of the DNS system, is probably to use distributed system architecture, using a block chain.

So, that's one interesting application for ICANN. And another interest in application is a project that I'm working on, which has to do with founder NGOs match making. So, the idea is to use block chain as a decentralized transactional system, so that NGOs and philanthropists or funders can basically exchange money without need for a third party, or central authority like banks.

So, that's one project. And you can all visit the website, [inaudible] dot org for more information.

All right. There are a lot of communities, actually. Many communities are working on this block chain applications, and different projects an initiatives. Two of them, [inaudible] block tree summit, if you're interested in joining, or ISOC block chain special interest group. So, in case you're interested in this concept of block chain, different application, just get involved in one of those two, or hopefully two, all of them.

Yeah, okay, those are some conclusions. So, block chain is a very, very new technology. It's relatively new. It's just early 90s, and it has a lot of desirable characteristics that we all want in an internet service, and it has a wide range of applications. But there are a lot of issues that hopefully are a lot of other communities will work on, which they have to do in regulation, a lot of problems with regulation, privacy, integration, and scalability, and there are a lot of other issues coming along the way.

So, that's it, thank you.

[APPLAUSE]

DEBORAH ESCALERA: Thank you. I'm going to ask for any questions between the Next Gen to be held until the end of the entire session, but if there is any questions from the audience, we'll take them now.

UNKNOWN SPEAKER: Hi. I'm wondering if you can talk a little bit more about how you think block chain technology can contribute to the DNSSEC and the security of the overall system?

ABDERRAHMAN AIT-ALI: Should I answer the question now? All right. So, DNSSEC, as you have seen in this slide about the characteristics of the block chain, there is one characteristic which is basically the resilience. So, the fact that a distributed system that increases the resilience of the DNS system. The thing is that there is an issue with scalability, so this should be worked on.

And I think one of the applications that will push research and development in terms of scalability of block applications, will be this application to DNS.

DEBORAH ESCALERA: Any more questions? Okay. Thank you. Next we have Carolina Matamoros.

CAROLINA MATAMOROS: [Inaudible] everybody. Carolina Matamoros. I'm here to talk about the defense and security perspective. The need to have a safe internet versus the need to have an open internet.

So, to do this, I will talk about this, troublesome triple intersection, it includes defense and security, but it's difference of security on a [inaudible] perspective, on a perspective of what is defense and security and not just security as it's usually considered within these debates.

So, let's start just simple kind of introduction of what this refers, defense and security is much more related to both states and individuals. How to protect them, where the concept of protection is much more important than what would everybody think. We must think also about the sovereignty of every state, how to defend that, how to protect that.

And especially how to do that on every domain. Every domain must be protected of every state, and that's the perspective every nation has, and it must be done. Also, from the perspective of security, especially here in Europe, it's the concept of human concept. It's like, how do we protect individuals from every possible sphere?

How can we allow them to be completely fulfilled to make them feel free? To make them protect their lives? And that's what security means in general terms. In this, to do this, well, you have the armed forces, and the national police, and these agencies are the enforcers. And also, the ones that can, in theory, guarantee those rights.

They are there in order to protect us, in theory at least. Now again, in general terms, this is one I cannot, I shouldn't spend so much time in it, the internet, it's open and global. It's a platform. It's really open. It allows to innovate, to create, to connect. We're all here because how broad internet is, and how it can affect us on every level. Let's move along.

Governance, well it's the ability to govern properly something, a state, an individual, the entire organization. So, it needs the definition of what it is. It can be local, national, global. It can be anything. But it requires someone to cover and something [inaudible]. So, it needs those things to be clear. So, let's go back to the intersection. Let's talk about the intersection between security and governance.

For this to work, you need to know who you're governing, who you're protecting. So, it's interesting to know who that is, and that's actually usually defined the law, according to every constitution, or treaty, or whatever it is that we're looking at, to define who you are defending, according to the different laws on governance.

There is also something very important note, that there is no global defense and security forces, there is simply coordination between the states. The states coordinate one another in order to provide global security, but it's a very difficult process, that it's done on coordination and consensus, and it's very difficult to obtain.

So, there is something to note, no governance without defense and security. So, the global defense on security depends on this coordination of the states. According to that, how incredible is enforcement of any kind of defense. If it depends on coordination on a global level, can we enforce something? Really? It's very difficult to do. So, now, when we go back and talk about governance on the internet, we have a lot of things that are difficult, beginning with the national laws.

These are not aligned. You can have very different approaches from different states on what is legal and what's not legal. What's a crime and what's not. At least among us, we agree that the internet must remain open, neural, and interoperable. But it's difficult because of somethings. First of all, anonymity. Everybody can say everything, nobody is accountable of anything that they do within the cyberspace domain.

So, this led to exponential growth of [inaudible]. We are, especially now, effected by it. We can even say that we're in the de-information era, because there is so much fake information on the web, but it's very difficult to manage because we don't know what's true anymore.

So, it is really unclear what and who the policies of the internet are directed to, for now. Let's go to defense and security and the internet. Between this, the first issue comes by, we don't who the perpetrator of the cyberattack is. It's really difficult to pinpoint them.

At the most, we can identify the IP address, and even that can be wrong. So, it's really difficult to know anything, and it's also very difficult to actually focus what the attack is about. You can attack an identity, you can steal my bank account, but you can also hack the training systems in Germany, and according to what you're attacking, the difficulty and focus of the states, changes.

If you're attacking a state, then it becomes something of national defense and sovereignty. So, it's something that every country is really concerned about. Because everybody is under threat, we are only here, but they are not real differences in security measures that can allows us to be safe within this [inaudible]. And it's something very different of how I'm talking, I'm talking about a domain.

I'm talking about a domain. So, think about land, sea, air, and space. Those are the traditional domains in the defense sector. Well, the internet is another domain, it's what we are moving. We are also have a [inaudible], and in there, we must be protected, as well as the states. But the jurisdictions are not clear, so how can we defend ourselves in those conditions? It's very, very difficult.

And when this is so difficult, you can see all of the different nations, you can see the treaty now recently done in Munich, in defense, you can see all of the white [inaudible] of all of the different nations. And cybersecurity, cyber [inaudible] are a top priority. It's the most interesting, and easy even, way to attack another country. And you cannot even know if another country is attacking you.

You can be a civilian. So, a top priority for every state, and what does this do? Well, it has a very, very ugly implication for the openness of internet. As long as the countries are concerned with their own defense, with their own states, if they cannot perform properly, they're going to be concerned about it, and the openness of internet is under threat.

If we don't address this issue, eventually the internet is going to be fragmented. We are already seeing movements about stats regarding this. In different countries in different levels, China, Korea, Venezuela, even Germany, how do you, if you can't even download something, it can be legal.

It cannot be legal. You don't know. But it's very difficult, and every stage is trying to pull, in a way, to defend itself. So, it's something that we, here, must be concerned about. So, wrapping up. First, countries may be interested in fragmenting the internet and protecting their own state, and their own civilians.

Second, there is no global, credible enforcement. And this creates a very difficult coordination issue among the states, because even if we're all agreeing that this is an issue, we cannot agree on how to deal with it. And third, global governance on the internet, as you see here in ICANN, it's much more of an advisory level.

We can make recommendations, but it ends there. They are just recommendations. And we keep on living with this threat for the internet from now on. And it's… What I want to do with this, is to create a sense of urgency here, in ICANN, that something must be done about it.

So, wrapping up, as long as we don’t know what our jurisdictions, and what our [population?] that’s being affected by every attack, well, the defense in the cyberspace domain is not real. And as long as it’s not real, we are under threat on the openness and interoperability of the internet. So, we must be concerned about it.

So, here are some options. Things that we can do. We can be able to recognize fiction from reality in the internet, like in a library. There is a history section, and this is [inaudible]. We should be able to know that. You should also end the [inaudible] of users, if a user has an ID, national ID, they are going to behave in a really different way then criminals.

And we must look for a way to make enforceable regulations on a global level. So, that’s about it. And I close up.

DEBORAH ESCALERA: Thank you Carolina.

[APPLAUSE]

Questions from the audience?

UNKNOWN SPEAKER: Hi. Do you think, in those strategies for defense and security, could cyber peace be a possible strategy to help out with communications with other countries and so forth?

CAROLINA MATAMOROS: By cyber peace, you're talking about like peacefulness? Okay. That's regarding how much trust we gave to civilians. Like, can we be certain that everybody is going to be peaceful just by agreeing to it? It's not likely, but it can be a principle. Like the principle in law that we are, in principle, innocent. Yes. On principle, we're going to behave peacefully.

But still, we need measures that guarantee that when somebody doesn't align with this trust, and attack us, we are able to prosecute and actually treat the attack. So, even with a peace principle guiding the internet, measures must be made in order to prosecute and deal with any kind of attack.

So, even with the principle, this is a matter of concern.

UNKNOWN SPEAKER: Anymore questions?

UNKNOWN SPEAKER: Yes, that's like a way to balance all the stuff, and internet user anonymity, how will that balance with the privacy?

CAROLINA MATAMOROS: Okay. So, there is different ways to go around it, because of course, privacy is a concern of every internet user, and according to the country, some may be more concerned of not knowing who is the user than giving the information. So, the way to implement this, change from country to country, you can go up and say, you can do this in a voluntary way, give your identity and be able to do it.

And those who will do it on different, let's say, kind of domains. You may be interested to not be anonymous if you're going to go to your bank account, because everybody that goes to a bank domain, is going to be there to do a transaction, at least in theory.

So, as long as all of the persons that go into the bank account are identified, you may feel safe. But if you just are going to, let's say, browse Wikipedia, okay, you can remain anonymous. So, maybe certain sites can remain anonymous, and some other not. But the concern of privacy is more related in the trust of government, like, who is going to use this information, right?

Like, if I give my ID, is somebody going to be able to use it? Well, it depends on how often they are, but as long as the information is there, it's a threat. But on our realistic point of view, I would say that, right now, there is no privacy whatsoever either. So, if you give your ID and you trust your government that it's going to protect you with it, maybe you can even gain more privacy from other entities.

But it's, of course, a debate that we must have, because it's on contradiction with it and I agree.

DEBORAH ESCALERA: Okay, thank you. Hold one minute, we're experiencing some technical difficulties, and then Chawana will go on.

CHAWANA HUANGSUTOMACHAI: So, okay….

DEBORAH ESCALERA: Okay, our next presenter, Chawana Huangsutomachai.

CHAWANA HUANGSUTOMACHAI: Thank you. You did well, Deborah. Ladies and gentlemen, may I have your attention for maybe like, not even 10 minutes? Don't worry. Are there any Danish people around here? No. Oh yeah, hi. [Foreign language]

Okay. Good morning ladies and gentlemen. My name is Chawana Hugansutomachai. Please call me Ferrari, it's my nickname, and I suppose it's easier for you. Okay. I am an LLM master student in [inaudible] University, the Netherlands. And today, let's talk about this.

We're going to have IP version six, which is going to be plenty for years to come. So, I came with up an idea, it's a very imaginative idea. What if, what if what, you may ask? What might happen if you have a personal IP address, like a static IP address for all of us?

Like, it sounds like identification numbers for everyone around the world, yeah. Like, pressing, typing IP address, and then [inaudible] that's some individual. So yes, as the previous presenter has talked about, there is one essential part of being in internet, it's anonymity.

Okay. Anonymity [inaudible], will be absent. Some people say, anonymity in the world of internet, no one knows if you're a dork, with due respect. I didn't mean that. It essentially means that no one knows who you are. But hey, but if IP address references someone, it's going to be you, you loss anonymity.

And what will happen in illegal context? And let me make a reservation, it's kind of bread and butter in legal professional field is highly subjective, and it depends on which, if it's good or bad, it depends on which way you're looking from.

Efforts on government, surveillance becomes easier, because normally, normally, IP address are collected from ISP. But then, it's possible that the governments will have the database to say, oh, this guy is this IP address. So, if they want to single out someone, it's going to be much easier. So, law enforcement, investigation, especially for cybercrime, let me explain it briefly.

If someone is going to commit some cybercrimes [inaudible], the governments, like the law enforcement authorities, will work on IP address in the first place. And then, because they don't have idea who is behind the IP address, but now, maybe they have.

So, if you have a personal IP address, it would bypass some [inaudible], they would get to you easier before the, cyber forensics have gone cold. But hey, there is some good stuff in it, which I possibly believe, because it will enhance citizen's protections unlawful procedures, because if they know who we are, if they know where we are, there can be our armor to say, hey, hey, I'm here. Don't try to mess with me.

Data protection issues. Okay. We talk about, we are going to talk about data protections now. IP address will become personal data, and personal data that means data that can identify persons. Well, it sounds… Especially in the era of internet of things, like okay, now we have smart phone, now we have [inaudible], now we have smart wash, and we charge all of them.

And you don’t want, maybe next thing we charge is rechargeable shoes, but the thing is, they would gather data through the connections of internet, and then, yeah, viola. With only one identification number, they would have almost everything that you would connect your internet. But hey, there is also a tradeoff.

This may enhance ability to manage online privacy because of the identification numbers, this was centralized all of every information regarding to one person in one place. So, in order to make compliance of data protections compliance in law, we should be much easier. Further implementation is required.

Peaceful internet. I personally believe that internet is nice, but behind the screen, behind the keyboard, it’s still blood, it’s still flesh, and humankind’s mind. If you go out of your house and everyone knows who you are, because you identified yourself because they know, because they might know you by IP address, you’ll rethink.

And maybe the third time thinking before you’re pressing enter. That’s the thing, because now here comes cyberbullying and some kind of other bad stuff coming on because of anonymity. And this might help. But also, please, that keep make a [inaudible] effect, it's yourself. If you go out of the home, and know everyone is watching you, whatever you're going to do maybe it will effect on freedom of expressions.

It also depends. Near opportunity, I just like one key, so please ignore it. New opportunities and difficulties. The thing is, conflict of interest, oh sorry. IP address might supersede any other numbers. Think about your telephone numbers, or maybe citizen's identification numbers, like in Thailand, we have 13 digits. It might supersede all of them.

It might become a new business opportunity, but then, what will telephone comments company think of it, that will bring to a conflict of interest, of course. Yes, thank you for your attention.

[APPLAUSE]

DEBORAH ESCALERA: Do we have any questions from the audience?

UNKNOWN SPEAKER: So, I agree with difficulties…

CHAWANA HUANGSUNTOMACHAI: Excuse me, who are you? Oh, thank you.

UNKNOWN SPEAKER: You pointed out about how to make anonymity. I'm a little bit concerned on how to put it into place, because right now, all the providers of the internet actually rely on the flexibility of IP addresses to be able to set up new connections.

So, to create just one IP for every person, it creates like [inaudible] and that [inaudible] are going to be something to think about, but you need to coordinate all of this information in one central database. And all of these companies are going to be in conflict with one another, on what is the right information.

You may get several equal IP addresses with the amount of people we're dealing with you. So, the actual procedure to make it happen, at least in my perspective, seems too difficult to actually be able to do it.

CHAWANA HUANGSUNTOMACHAI: I personally agree with you, because this is somewhat imaginative idea, but who knows? Things seem to be impossible until it really happens. So, I just want to say that implementation will be somewhat horrible for techy guys, I'm sorry to you guys for this, but it's just the possibilities. And I haven't think about on how to implement it.

It would be a conflict of interest, of course. Thank you.

DEBORAH ESCALERA: Thank you Chawana. Okay. Our next presenter is Clement Genty.

CLEMENT GENTY: Hi everybody. So, I'm French. My name is Clement Genty. I'm an engineering… I am an engineer in industry engineering. Nothing relating to accountability, nothing related to lower diplomacy. No. I just want to talk about naming policy. Maybe you have noticed I am French, so I am going to talk about France.

Yes, here is a wonderful plane. Yeah, it's a French plane, okay? Now, it's an American plane, okay? Okay. What's the [inaudible]? Maybe you have noticed that on the tail, if it works, yes. On the tail, there is an identification code. In fact, in 1944, [inaudible] in order to create this civil convention on aviation, and this code has been launched.

Next, let's talk about radio [inaudible]. In 1927, we created the telecommunication code, as you may noticed on this, sorry. I cannot go back. Yeah. So, in 1927, we launched this code. And for example, you can see that on this QSL card on the MIT radio club.

So, W is for US, and F is for France. Let's go onto new. When scientists created the domain name system, they had this same idea. So for example, for the dot FL, which is a French ccTLD, the scientist of [inaudible], which is a French lab, created a naming policy for the FR with subdomains.

For example, at the top, you have the [inaudible], which depends on the Ministry of the Interior, and you know that you're on a governmental website, because you have a dot gov dot FR. Next, for [inaudible], which is the French Army School, it is a French Army belonging to the family of [inaudible], Ministry of Defense, and the government of France, and so on.

Okay, you get the, first the US, same thing. Jon Postel, which is, who was, unfortunately, the manager of the dot US, create the same thing. So, on the top right, you can see [inaudible] school, because K12 is for school, depending, locating in California and then in US.

Okay? Just after you have the city of [inaudible] in California, and in US. Okay, you see, the deal. So they tried to launch the kids dot US, but it didn't work, unfortunately. Here you have a wonderful collage in Canada, in California, sorry. Is the city of [inaudible]. Please notice that you can read the domain name and trust the domain name.

It means that you know that it's [inaudible] State, California of US. Next, if you are looking for the police of New York, you just have to go on police of the city of New York in the state of New

York in the United States. But a registry understood that they could make a lot of money by delegating all of these subdomains.

So, yes, they earn a lot of money, but yeah. But the belated, this identification tool that is, which is the domain name. Now, you can be everybody. ICANN register dot [inaudible] domain name. I can register for example, Clement lawyer dot US, if I want. Nothing is forbidden.

Companies try to create some navigation bar in order to help the final user to trust the information on the internet, but it doesn't work. It's really, it doesn't work. That's a fact. And then, we created the SSN security or SSL, a nice story too.

Please, you have to pay for website, and as you can see, they both have FFL. But, because there is always a but in the life, on the left, it is the paper website which has SSL security. On the right, it is summary support dot com, which has the SSL security. And you can notice that the domain on the right has SSL too, but the first level of SSL because SSL level, I mean, there are three levels of SSL.

So, you cannot trust an information on internet, that's a reality. Today, you cannot say, oh, I know the website of the French government. You cannot say, oh, this is a really website. I'm personally concerned because I'm French, and in May, we have the presidential elections, and when I saw what happened in some other countries because of fake news, I feel upset.

Okay. So, here is the deal. Nothing is present in order to gain trust on the internet. Personally, I'm a university lecturer, so I ask a student to give me the way for them to have trust in our webpage. It concerns about [inaudible], the [inaudible] is a political subject, is a religious subject.

So, when you type [inaudible] on Google, because you know that 76% of youth in France are looking for medical information through Google. So, you have a lot of webpage, but you have some webpage which are managed by religious person or associations. So, it's a big problem.

As you can see [inaudible], I asked the students, there were 137, to rank these four subdomains to escape from zero to three. Three is I can trust it and zero is I cannot trust it. So, you can see that dot gov, dot FR, is the highest domain for the trust. [Inaudible], org, and net, nothing.

So what I want to create and what I want to present, is a free tool for French user. I said French because I'm using a ccTLD, which is not used, as you know, France is [inaudible] so [inaudible] in South America, you have a ccTLD, you have a ccTLD for [inaudible], you have a ccTLD for [inaudible] territories and so on.

We don't use two ccTLDs. The first is [inaudible], here at the west of Mexico. And the other is the ccTLD for metropolitan France, which is that dot FX. And I want to use this dot FX to recreate trust on the internet.

Okay. Here is the deal. Let's create a trusted space with subdomain managed by authorities. And ask to some authorities, I mean, for example, lawyer association, I mean the profession of lawyer in France is managed by a lawyer association, called CNB.

I purposed, I suggest that the CNB manage the dot lawyer dot FX, in order to recreate the trust link. And so, concerning the airport, concerning the embassies, the trademark, or the medical doctor. Currently, France use [inaudible] France dash country dot org for the embassy, but anybody can register a dot org domain name.

So, you can easily understand that France haven't registered all of the ccTLD domain for the embassy. And you can find a lot of fake news on the internet.

So, here is it. It's not, how could I say? You cannot use subdomain, I mean, I suggest that we use subdomains, encouraging to the [inaudible] certification. Maybe you don't remember, it was three years ago, and [inaudible] thought that we could divide information through memory, reason, and imagination. But I will talk this just after the presentation.

So, I suggest to create a [inaudible] structure [inaudible] with a registry, with a registrar, sorry, accreditation. Here is it. So, that [inaudible] point, you can't trust anything on the internet through domain names or other tools, we have to find another way to help people to access this information. Thank you.

[APPLAUSE]

DEBORAH ESCALERA: Thank you very much. Again, for NextGen, hold questions until the end, but if we have any audience members that have questions.

UNKNOWN SPEAKER: Well, I have question to presenter. About [inaudible] trust. Do you know and consider it in your work, another project run by France researcher, and inventor of packet, connections [inaudible], which is called open root, which is, could be used for such purposes for everyone who don't trust ICANN, for example.

CLEMENT GENTY: Yeah, yeah, absolutely. I have a meeting with [inaudible] next week, for the little story. [Inaudible] is the inventor of open root, and it created a Europe alternative to [inaudible], some decades ago. Thank you.

DEBORAH ESCALERA: Sara, hold on one moment. We're having difficulties with the computer again. One moment.

Okay, so our next presenter is Sara Dushi. Sara?

SARA DUSHI: Hello. I'm from Albania. And I'm doing a PhD in science and technology at University of [inaudible]…

DEBORAH ESCALERA: I'm sorry Sara, I hate to interrupt you, we're going to change the computer out. [CROSSTALK]

I apologize to the audience, one moment.

So, for our audience members, we're going to break about 12:30 for lunch, and resume again about 1:00.

We have quite a few presentations to get through, so we're going to take a very short break for lunch.

All right, I apologize. Our presenter, Sara Dushi.

SARA DUSHI: So, as a PhD candidate, I'm researching on sexual abuse and sexual exploitation of children on the internet. I like to start my presentation with this expression which dates back to '95, just as the computer has begun to revolutionize social life, it will revolutionize crime and deviance, especially the parameters, deviance, sexual behavior. In fact, this already doing so.

It shows that since those years, cybercrime has already started happening. Next slide, please. These are some facts. For the last two years, currently we have 2.4 billion web users, but as far as I remember, from today's presentation of Göran, it has already gone 3.9 billion users.

In 2016, Internet Watch Foundation has identified over 68,000 webpages of child sexual abuse images, which shows an increase of 417% over the last two years, which is a huge increase. 69% of the children in these images are eight years, 10 years old or younger, and most of them are girls.

According to the researches, what adult perceive as online risk taking behavior, such as providing personal information to strangers or agreeing to meet with them with [inaudible] France, are perceived as young people as normal social networking site behaviors.

These are the forum of online sexual abuse. So, it's a kind of a child sexual abuse, which before happened only rarely through images, which were not transmitted, which were not so global. Now, with the internet, everything is made easier, it becomes a global issue. And [inaudible] are sexual harassment, sexual solicitation, sexual grooming, and commercial sexual exploitation, which is in different ways, like child prostitution, child trafficking for sexual purposes, production and consumption of child pornography, and child sex tourism.

So, let's start with an illustration of the problem in real life, in 2007, there was a case in UK, when they found, they detected images of sexual abuse of children, girls, which were from Southeast Asia. But they couldn't detect the abuser. They had a suspect, because he was frequently traveling to Southeast Asia, but they couldn't prove, it wasn't enough to prove that he was the one who committed the crime, because in the images, it was shown only his hand and the children who were being abused.

So, they asked for help. A research center for the… Which we're using very special techniques for forensic, measuring of skin type patterns. And they could identify the skin pattern of the suspect was the same as the skin pattern shown in those pictures. So, this example shows the connection between the online images that circulate on the internet, and the real abuse that is happening.

Those images are real, and those children are being abused in real. And it also shows that in order to investigate this crime, only law enforcement is not enough. They need special technology, and cooperation with different stakeholders. And it also shows the international scale of the problem, because criminals usually tend to find countries, which don't have strong legislation for cybercrime.

Like in this case, that a person from UK went to Southeast Asia, and it also shows that there is a need for a cooperation among different institutions. Another example is in November 2015, when [inaudible], it's a famous company in Hong Kong, which provides, sells technology used for educational purposes by children. It suffered a data breech, which compromised 6.4 million children's account.

And those accounts, from those accounts [inaudible] images of children, and they could relate to the name of children and find their addresses. So, according to global statistics, the child abuse images are mostly hosted in North America and in Europe.

This is a graph that shows the number of domains hosting child sexual abuse, counted by year. It is… The highest level was in 2007, but then it was, even though it has decreased, it shows that it is increasing. In 2015, it was 1,900 domains who were hosting child sexual abuse.

So, my research questions of my thesis are, what are the most effective legal steps to tackle online sexual abuse of children, and what is the scope and nature of international capabilities like legal, law enforcement, and technological capabilities needed to implement any approach for the prevention of online sexual abuse and sexual exploitation of children.

And so, in order to answer this questions, I have planned to follow forming directions, which are the causes of the crime prevention, identification, and those are response.

Methodology, what they follow so far is nominative analysis of international standards, case load analysis, and qualitative interviews with different stakeholders from government, academia, law enforcement, and tech community.

The critical points that I've gleaned through so far is that there is no singular uniform definition of child and child sexual abuse content. And the age of children, the approval for engaging in sexual activities. There is also no standard definition of child sexual abuse. And we all know that the technology develops faster than the law.

It is also a borderless crime, which causes many jurisdictional problems, communication between different countries, and there is a very low rate of crime reporting. Usually these crimes, the children don't report the crimes and they only get detected occasionally. And in most of the countries, there is a lack of special investigation department for online sexual abuse.

It usually follows under the Department of Cybercrime and economy crime, that those investigators are not so experienced with investigating child sexual abuse. And it is… There is a high [inaudible] for common universal age of consent for engaging in these child sexual abuse activities, which causes very big problems when the crime is borderless, and it can be, the crime, the child can be considered an adult in one country, and the criminal doesn't, cannot be prosecuted.

There is also a multistakeholder approach, [inaudible] as I mentioned before. So, my conclusions, so far, are that there is a need of new technologies for investigation process. One of those new technologies was introduced in the recent years, late years, in US by [thorn?]. They have spotlight technology for, which most of the countries now are using for the investigation purposes, and it's easier to detect child abuse images.

There is a need for multistakeholder cooperation and prevention and identification process of online child sexual abuse. And I think that there should be, remove the possibility of opting out from international, from provisions of international documents about child sexual abuse, like the case when you can opt out from criminalizing simulated child pornography.

And the number, and the quality of human resources for the investigation of these kinds of crimes are very low. And I also suggest the need to create an international, or at least regional, commissioner for the online child rights. Thank you.

[Applause]

DEBORAH ESCALERA: Thank you Sara. Do we have any questions from the audience?

Okay, so at this time we're going to take a short break for lunch. I think we can reconvene about, let's say 12:40. Okay? Thank you for coming.

NextGen, we have lunch here, so we're going to go ahead and take our lunch here and then we'll start again.

Okay. NextGen, get ready because we're going to be starting again very soon.

Okay. I want to remind everybody, computers and phones down during presentations, and during any of our sessions this week. You're not allowed to have your computers and phones open. If some of you are using computers for your presentations today, like Jackie, just let me know, and that way I won't bother you during the session.

Okay. So, if you're taking notes, that's fine. That's another reason why we gave you the notebooks at newcomer so that you wouldn't be using your computer.

I'm sure audience members will return, but for the sake of time, since we have so many presentations to get through, we will resume. Our next presenter is Jackie Eggernschwiler.

JACQUELINE EGGENSCHWILER: Well done. Thank you. Hi everyone. It's very hard to come back after lunch, I know, and we can see that. So as Deborah said, my name is Jacqueline Eggenschwiler. I'm a researcher at the University of Oxford. The topic of my focus is actually cyberspace and the regulation there of. So, what I'm going to present to you today is a side project of that. And it focuses mainly on accountability, a buzzword that I think we've heard quite a number of times, already, these two days, and multistakeholder model and multistakeholderism would be the second buzzword that will also figure in this presentation.

So, let me give you a little bit of background what motivated this project in the first place. What we see happening and emerging in this space that we're talking about, in this ecosystem of digital technologies, and in this environment, we see different stakeholders, different spheres of regulation coming together.

And also, of course, different issue areas. We're not just talking about the management of the DNS, for example, we are also talking about privacy and data protection related issues. We're talking about cybercrime. We're talking about how to manage, for example, a digital IP for everyone.

As we've heard Chawana talking. So, there is a lot of issues that come together. And really what it does to this space is, it muddles structures of accountability. So, given the multitude of actors and the issue areas we're talking about, and also, of course, the different forums that engage in this type of regulatory steering, we really can't say easily well, this body is accountable for that, and this body is accountable for that.

We see conflicting structures emerging. One of the leading questions that guided this project was from a conceptual perspective, what challenges are confronting the accountability of cyberspace governance. And in a second step also, given the prevalence of all those different actors coming together and really the importance of those actors shaping this environment. What types of accountability can we see emerge in this context?

Is it just one type of accountability? Is it multiple times accountability? And if so, what are these? With regards to the first question, the answer, really say part of an answer is that, I came up with as part of this project was, the challenges that this environment is confronted with, basically emerges from the foundational issues of the concept itself.

So, we have an issue with many hands contributing to this environment. We see the profusion of different issue areas, and we see a certain degree of hybridity with regards to the institutional arrangements. Now, with regards to the problem of many hands. As I said, it's not just one stakeholder, for example, governments contributing to it. It's the private sector, it's individual constitutions. It's Civil Society organizations.

So, one really has difficulties trying to identify who is accountable for what, given that complexity. The profusion of issue areas, similarly, we see that suddenly issue areas can convert, if you think about naming and numbering, for example. There might suddenly be issues popping up related to IP.

So, then again, you need to ask yourselves, well, how can we handle that, and address that, and who can be held accountable for that? The hybridity of institutional arrangements, refers to a situation where we have different institutions, arguably, and more and more of those institutions being engaged in the regulation of cyberspace popping up. But sometimes, they only show transitory natures, so they emerge, resurface, at times again, vanish, reemerge again.

So, we are confronted with that challenge as well. Now, with regards to the second question. Given the prevalence those different actors, what kinds of accountability structures do we see? And I would argue we see three not exclusively three structures, those can merge, interact, they can even form new structures.

But these argue typical types are hierarchal accountability, which refers to probably a situation, for example, classic state accountability. So, you follow strict and vertical lines of commands, trickling down from the top. Whoever is at the top, almost has individual accountability for what happens below the level.

That kind of structure might emerge, for example, in cybersecurity related areas, where you can try to hold individuals accountable for failings to provide necessary security provisions. We can also see corporate and private sector types of accountability. These let you actually pierce through the veil of the individual and look at the cooperation and hold the cooperation accountable for that.

Given the prevalence of those big internet players that we hear and talk about, a number of times, think of the big ones, Googles, the Amazons, the Microsofts of this world, this is an important type of accountability, because it lets you at least conceptually hold those needs to account, and we see where those companies have been held to account in this environment.

And the last one, and probably, well, one could argue the most important one, is collective accountability. Because given, again, the fact that stakeholders contribute to policy outcomes, also to technical outcomes, and to economic outcomes together, and when you think about well, if we can't hold them to account individually because it's not just one entity deciding, then we need to have some sort of instrumental that lets hold to account, for example, a community.

So, this concept would be based on the idea that everyone contributing to an outcome, a policy outcome, or a technical outcome, and where you can determine a certain level of engagement, would be held to account. And accountability in this sense is really a relational concept, because it talks about the duty of an actor to render account for contact to another actor.

Now, the project didn't provide any answers in terms of how to resolve those issues that I've just been mentioning on the go. But I just wanted to look at well, what are possibilities? So, it didn't make any recommendations or hard recommendations, but generally, what we can say is that cyberspace governance presents both researchers and policy makers with those critical questions that I just talked about.

And that you see this tangled web of interrelations. And also, what is quite fascinating is that accountability is actually contested by the very constitutional and fundamental elements of this concept of cyberspace. So, again, the many stakeholders contributing to the many issues that arise, and the policy areas that we see.

So, what might be required, and where ICANN has actually done a great job and can be applauded for is the explicit rehashing of accountability structures. So, to really think about how can we rehash these structures and make them as transparent as possible, and as highly accountable as possible, as well, so that we can see well, this is the process that we line up in order to determine accountability.

And that was the conclusion with this project. I'm happy to receive questions from the audience, from you guys later on. Thank you for that.

[Applause]

DEBORAH ESCALERA: Thank you Jackie. Do we have any questions from the audience?

Okay. We're going to take… We have one question from the audience.

UNKNOWN SPEAKER: For the record, [inaudible] from Pakistan. I am a NextGen ambassador of your ambassadors. This is not actually a question, so you can sit down. It's actually a quick couple of comments. So firstly, to my NextGen, to staff, to [inaudible], to Andre, to Lauren, congratulations. I'm really proud of you that you made it to the ambassador within a year.

And secondly, to [inaudible] and Janice, thank you for everything that you are doing for us, because I'm a NextGen, I'm a Fellow, and now I have to run from a Fellowship session. I just came here to thank both of you, and all of you, in particular, thank you for everything.

And now, of course, the most important thing, to my NextGen that are sitting here. You know, at ICANN everything is being transcribed, so whenever you go to speaker, first you say your name and your affiliation, then you comment. For example, I'm Carolina from Mexico with NextGen, now here is my question.

Just don't go up to the mic and say, hi, this is my question. And NextGen and Fellowship, they are both different programs. I have heard a lot of NextGen saying, hi, I'm from NextGen

Fellowship. They are both different. Either you are NextGen, or you a Fellow, you cannot be both.

And finally, the most important thing, please do come back. No, it's not the end of your journey. It's just now beginning. Once a NextGen, always a NextGen. I am here for you, you will be here in next meeting. Thank you.

DEBORAH ESCALERA: We're experiencing some technical difficulties, so we're going to resume the presentations in just a couple of minutes.

Okay. Our next presenter is Katharin Tai. Katharin?

KATHARIN TAI: Okay. So, my name is Katharin. I study international relations at the University of Oxford. And my thesis project focuses on the question of cyber sovereignty as a narrative in Chinese foreign policy. So, the main question that underlies this whole project is kind of like, what is cyber sovereignty? And first, I think, it makes sense to briefly talk about my background, also talk about IRs, International Relations as a discipline and what it tends to do.

So, sorry. So my background for my undergraduate in area studies. So, I focused on Asian politics, like societies and history. And my master's degree is in international relations.

International relations tends to concern itself less with the question of what should be done to reach certain goals.

It's much less policy focused, and it tends to be much more in love with theory, and tends to focus much more on trying to provide concepts that help us understand the world, and that can help us understand the things that are happening in politics.

So, is this working?

Perfect. So, the aim of this presentation is first to give you a quick overview of cyber sovereignty, and what it seems to be, and why it is a problem, or like, a problem for IR as a discipline. And then secondly, look at whether IR theory has, gives us any tools that we can use to conceptualize the state in cyberspace.

So, that was quite interesting, because Carolina in her earlier presentation had, oh the state, and then she had a footnote, and it just said, oh jurisdiction within territory. So, I'm going to try to break that down. So, first what is cyber sovereignty and the challenges that it opens up, right?

So, it's something that has been central to Chinese government scores on international internet governance, since around mid-2014, which was also around the time the Chinese government created a small leading group on cybersecurity issues, and when it created the cyberspace administration of China, which is essentially a whole entity within the government that is solely devoted to tackling these questions of cyberspace, like on a variety of levels.

So, there tends to be a much more domestic focus, but they also deal with these issues of international internet governance. Cyber sovereignty has been central to what this agency has been saying for the past three years. However, lots of people are very unclear as to what this means.

So, it’s also, while it is central to government discourse in China, it has become a buzzword when IR academics write about what China does in terms of international cyber policy. So, let’s say, this is the Chinese, this is what the Chinese say, we’ll stop them and move on to the next thing.

However, nobody has ever actually tried to look into what this, like what this means as a concept of what this means as a word. Secondly, it also forces us to tackle head on the question of what the state is in cyberspace and how we, as IR scholars can conceptualize this state. I recognize that especially ICANN, lots of people may say, well, the future is multistakeholder, we don’t need states anymore.

But at least us now as a discipline, IR focuses quite a lot on the state as an actor, and additionally we can see that the state is going to be relevant, and still acts within cyberspace. So, for us, the question is, how do we conceptualize sovereignty when we are in cyberspace?

So, to answer that question, it's important to answer the question of what sovereignty is in the first place. There is the common assumption that cyberspace undermines the state, right? People say, oh, like cyberspace transcends borders, and because it transcends borders, like it's suddenly under minds the state.

Inherent in it, is this assumption that the state is inextricably linked to particular territory, and that it cannot be a link from the territory, and once the territory becomes more difficult to determine the state and state sovereignty are under mind and somehow taken away. However, if you look historically at where sovereignty comes from, it started off essentially as more of a bundle of rights.

It was not so much associated with the state as an entity initially, but it was associated with, for example, a king. Right? Or like the sovereign. The sovereign were not initially the people. That is a concept that developed over time into something that was afforded to the people. So, rather than an original person being sovereign, there was this idea of like country, the state, is sovereign as an entity, as a political entity.

This was then around the 15th century really like much more closely linked to this idea of a territory. So, rather of an abstract entity, of abstract entity being a sovereign, suddenly people started thinking of it, like this entity being sovereign with reference to a particular territory.

So, kind of like, let's, like you can think about it as a loop on the map, right? Like, we draw lines, and someone is sovereign with regards to everything within the lines of this particular map. This is a concept… Like, this was an idea that was further entrenched in the late 19th century, for example, Latin America during decolonization there. Lots of the states demanded the right to particular territories.

So, there was this idea that a state in Latin America wants, became independent from colonization, with the right to sovereignty and self-governance came the right to the territory, like that had been colonized before. So, it's not only self-governance of a certain group, or like a nation, but it's like it's also self-governance over this particular territory.

So, suddenly this notion of sovereignty, despite it only being about rights of a certain entity, becomes linked to this territorial idea. And so, this one scholar who is briefly tackled this, like the way he framed it was, the way he framed it was the spatial, the territorial state has colonized our imagination, so we can't think of the state as anything different then this, then these lines on a map.

So, we think of the state as long as on a two-dimensional map. This brings a variety of problems with it, for example, if we think of cyberspace, it's often difficult to say where something is. Our maps, the way we imagine them in two dimensionality often don't apply anymore.

And one particular problem is, for example, the question of authority, which kind of ties into the question of accountability as well, right? Because if you have a map, and you draw a line through a circle, you can say one part of the circle is mine, and another part of the circle is yours.

It can't be both at the same time. That's the fascinating feature of two dimensionality. But, the problem with cyberspace is that this exclusivity of authority, is not something that can be applied anymore. Suddenly, we can't think of space anymore in a way that like divides things, and divides space immediately into different parts that are accorded to different states, and what different states clearly have authority without anyone else being able to impinge on that.

DEBORAH ESCALERA: Katharin? Slow down a little bit for our interpreters.

KATHARIN TAI: Okay. Is it fast?

DEBORAH ESCALERA: It's very fast.

KATHARIN TAI: So, two… Now, I want to talk about two approaches to the theory of sovereignty that might help us, or might be able to give us an idea of how we can approach the state in cyberspace. One, is the idea that was introduced by Stephen [inaudible], who said, actually sovereignty is not one thing that you can have. It's not like a piece, like it's not a whole keg.

It's something that can be divided into different parts. Some parts of it are about control. It's about control over things within your territory, but some parts of sovereignty are about, for example, authority. You have a part of sovereignty that consists of being recognized as a legitimate state, by other states. So, that's something that can exist without control.

As a conclusion, [inaudible] also says then, well, if that's the case, then states can be sovereign in different ways. Some states are sovereign in like, for example, in the way that they are recognized. This is a part of sovereignty that other states may be lacking, but that doesn't mean that sovereignty in these states doesn't exist.

So, this is already important approach when it comes to cyberspace, because just because the territorial and the spatial part of sovereignty that we've been used to before, does not necessarily apply anymore, does not mean, in itself, that sovereignty is under mind, if we think about it as a [inaudible] of different aspects.

Secondly, one thing that's particularly interesting, is something that's come out of people who deals with globalism and globalization. Some of you may have heard of Anne Marie Slaughter. So, she works on international networks of professionals. And for her, sovereignty in the time of globalization has transformed. Rather than thinking about sovereignty as different attributes, as saying a state has X, a state has a territory, a state has authority.

She says, states need to be able to protect their citizens. And if, for example, the capacity to engage in international organizations, serves that purpose, then that means sovereignty is present. So, sovereignty becomes suddenly instrumental and less something that is an attribute that exists right away.

And so, just to draw back the… To go full circle and go back to China, this is, for example, something that is also very much present in the government narrative, on how they understand cyber sovereignty. Right? So, for example, they say sovereignty is really important because the main thing that it's for is like economic development.

And this is the aim that we want to reach, and this is how we know that sovereignty exists. Thank you.

[Applause]

DEBORAH ESCALERA: Thank you Katharin. Is there…? Are there any questions from the audience?

Okay, our next presenter is Krishna Kumar.

Krishna, hold on for one moment.

Okay, go ahead.

KRISHNA KUMAR: Yeah…

Okay. Great. Okay, so, I'm Krishna Kumar. As you all know, but before I start my presentation, feel free to add me on LinkedIn, Twitter, Facebook. I use the same handle everywhere. But, yeah.

So, I'm going to talk about institutional analysis of the IANA transition. It's about new institution and economists approach a given situation. To understand this, I will explain the concept of governance, and that is something I'm interested in.

So, what is governance? Governance is almost of coordinating social action in a human society. It's as simple as that, right? And we have multiple players to internet governance. It can be [inaudible] by governments, hierarchy, networks, and also markets. The thing that we need to notice here, is government is one of the player to [inaudible] governance and services, and not the one player, right?

And many governments tried to, try not to understand this in the right way, because it also infringers on their autonomy and sovereignty, and we have an issue there. And the other thing that makes governance essential are institutions. And what are institutions? Institutions are the rules that we as humans use while we interact with other individuals and other organizations.

So, for any governance system to work, institutions play a key role. And my study is about how ICANN as an institution as a wall to address internet governance challenges. And for my study, I've used, relied heavily on [inaudible].

So for a really long period of time, economists have a very simpler view of understanding things. For them, it was just markets and government delivering public and private goods to an individual who they considered rational, and that's not always the case because as human beings, we know ourselves pretty well. We're complex. And so, that is this inherent need to understand complex systems, and that is what they framed as well.

So, by [inaudible], he said, humans we study have complex motivational structures, and we establish private for-profit governmental community institutional arrangements, that work at multiple levels to produce innovative and sometimes destructive solutions.

So, to understand this complex systems, they come up with this concept of polycentric governance model. And how does this work? So, in a polycentric system, you analyze multiple centers of [inaudible], multiple centers of [inaudible] making, and you analyze them whether they function independently, or interdependent, what other contractual mechanisms, how do they cooperate? What jurisdictions they come under?

And how this leads to predictable patterns of interactions, which let's them reach a solution. And to qualify them, they came up with the IAD framework, which is the Institutional Analysis and Development Framework. So, the first three categories, bio-physical characteristics, [inaudible] roots of the community, rule and use, is about defining what the issue is so…

In the case of IANA transition on the internet, internet would be the bio-physical characteristics in the study. [Inaudible] roots of community is, what makes this community work together, like, why they work together, how they [inaudible] together, and their capabilities that they bring to the table and then negotiate and stuff.

And the rules that they haven't used because every constituency, every stakeholder group, have their own set of rules that they use when they engage with everyone else, right? And the action arena is ICANN, a situation is the IANA transition that I'll be looking at. And then I'll be tracking the patterns of interactions and essential outcome.

So, why IANA transition? To me, I think it's one of the best case studies, simply because a lot of people from around the world came together, the enormous effort in terms of the hours they worked, liked 800 plus, 30,000 mailing exchanges, 600 total calls and meetings. And also what makes this special is, we had people from all around the world who grew up with different value systems. But then, they decided to come together to work under the roof of ICANN, and subscribe to the value systems of

ICANN because they believe in keeping the internet open and global, right?

So, that kind of makes it special. And as I said, I'll be analyzing the [inaudible] variables, and also the [inaudible] situation in terms of participants, their position, the outcome, and then how they control information. It's essentially the interactions that takes place. And also, individual actors in terms of their knowledge level, the selection, and the results they bring to the table.

All right. So, what is the need for the study? Because ICANN is special. ICANN is special, but ICANN is not perfect. I think what makes it special is, it is still functional, which is not the case with other intergovernmental organizations. So, multistakeholderism as a concept has been kind of…

World governments have been trying to enforce this since 1990s. They tried this with climate conferences and global, other global problems, but it never happened. And it sort of came together in 1998 through ICANN in addressing internet governance challenges, and I mean, I see ICANN as a system that's constantly evolving, it's not perfect, but it's functional, and that's what makes it special.

The need for tracing the study is because it helps us understand how complex governance systems work. And it helps us understand past efforts and like in 30 years, if someone else takes over ICANN, and they change all of the value systems, we can go back to the study and see this is how we were, and this is strong, and this is not happening. Thank you.

[Applause]

DEBORAH ESCALERA: Thank you Krishna. Do we have any questions for Krishna?

Okay, thank you. Our next presenter is Luã.

LUÃ FERGUS: Is this working? Okay. So, for those who don't know me. My name is Luã, and I'm a Brazilian law student, but currently, I'm living in Lisbon and studying at the [inaudible] University of Lisborn. And I'm going to talk to you today about youth internet governance. And I choose this topic because I'm into this topic since the last three years, when I got engaged in an organization called the youth of [inaudible], which is an organization within the ISOC, the global ISOC.

We are like a special interest group. And well, does the word belong to the young? And at this speech from Obama, he said that the future belongs to young people with the education and the imagination to create, that's the source of power in this century.

Everybody can agree that youth people are going to be the next leaders, and will take the world, but what about right now? Next, please. But do they really allow us to have a say in the formation of the future in which we will live? Like these guys, like Obama, our boss, and people who want to, that we engage it?

So, yes, no, maybe. So, I'm going to try to talk about some challenge and opportunities to bring you to the IG discussions. In the youth declaration written in 2015 by the participants of the youth [inaudible] program, they said that they have two major problems in engaging in internet governance, which was the language limitations, and the economic climate.

So, as language limitation is like a huge topic with cultural diversity, I will pass this so focus on the economic element. So, the first question, how [inaudible] from our sponsorship and capacity building initiatives? How can we reach them? How can we reach these organizations involved in IG discussions, as ISOC or ICANN?

And I'm going to show you some, that's current, the current opportunity that's already happening to engage youth in internet governance. So like the NextGen, that we're in to. In

Latin America, we have also this governance prime, which is a free course made by, sponsored by ICANN, and which they bring like during one month, go to the university, and teach people basic knowledge about internet governance and ICANN and all of this stuff related to internet issues.

ISOC has also these two problems, the youth at IGF program, which is also was viewed together with the CGI, which is a Brazilian steering community. We have here [inaudible] who is also, help to create this program. They bring a lot of people, they create like this capacity building program during two month, it's really hard and they have tutors.

I was like a Fellow in the first year, and then I was a tutor in the second year, and it's a really complete course, and then the use people that participation in this first program, they create like a youth observatory where they try to engage people around Latin America and now around the world to engage in these discussions, going to the forums and do this capacity building, and these organizations is what I'm working right now.

We also have like this internet governance school, like the south school of internet governance, the summer school of internet governance. And Brazil have our Brazilian internet school. So, these are like the current, major current opportunities that youth people can engage in internet governance discussions.

But would those actions be sufficient, because it seems like we're living, as my experience, we're living in a little internet governance bubble with the same youth people, and the same guys doing all of this stuff. And I see that we need to reach other places, the universities, or the private sector that it's effected by internet, but it's not really into the internet.

They don't have like internet related problems, but they use internet for example, so… And other question about the economic element is like, what influence do Fellows play? Because in most discussions on internet governance and the multistakeholder process, the funders and the economic interest are neglected at some point, because we only always seems like, oh I have to put the guy from Africa, one person from Asia, one person from Latin America, and have like to gender base it.

Like, you gender division. But who is paying for these people? And who is funding them to get into the discussions? So, that's a topic that, why do people want to bring these people to the discussions? This is a question that we have to ask, and this is a question that I give it to you, to think.

Because I think back. So, I bring this excerpt from an article from Luca [inaudible], it should be considered that stakeholder participation to pass development [inaudible] might be motivated by the perspective of achieving an outcome that may maximize its own utility, by self-interest, or by the intention to log for an outcome that may maximize its further interest.

And there is also a curiosity, because inside the stakeholders like Civil Society, ITR, academia, there are a lot of different perspective and a lot of different opinions, and different versions of opinions at some point. But only those who get funds can come to these discussions and show their perspective.

So, a lot of other groups are excluded from these discussions, and that's another thing that I would like to say because everybody would go to the website from IGF or even ICANN, and it tells that, oh, this is enough space you can come here and talk, and never think, but as youth, we have like this economic issue that we can travelling through the world, and discuss, and have this discussion and campaigning the discussions.

Okay, we have like the remote participation, but it's like, it's not that much, it's not that great right now. But I know some people are trying to prove that. So, how much people engage in the IG are attentive to the interest of their founders, and what interests are at stake in promoting [inaudible] participation of young people, that's an impression there I leave to you.

And another topic that is [inaudible] person, that I would like to present to you, is like representatives and [inaudible], because unlike the representative assistance, where individuals like other individuals to represent their interest, and in stakeholder process, it's like, it's voluntary. You can come here and say okay, I'm from civil society, I'm from academia, and everybody, they might think that your opinion is the opinion of whole Civil Society on that issue, or the whole academia on that topic.

So, it will have like an informal symbolic of a presentation, and as I said, only a few members of a particular stakeholder have resources to participate in internet governance, even. So, we start to create a global internet governance elite with that grass root, that group movement, Civil Society groups, and citizens initiatives that analyze the structure. Yeah. Kind of.

And about the legitimacy, as I was saying, we have this problem, like, can we say that we are [inaudible] the youth people, who are out there. And do we represent the connected youth, or there is this legitimacy to speak on their behalf, because that's something that's really happening in a lot of forums, like at the IGF or even national IGF or regional IGF, or other ones.

Okay. What about now? We want to be heard, okay, but now what? Okay, we kept saying, oh, we want to be heard, we want to participate. And when we got a seat at the table, that's going to happen. So, I put this three topics that I would like to… As my past experience.

We need even more space in the debate. Okay, we have some space, but we need even more, and we have to make a different [inaudible] of youth, like in this discussion, they kept saying, okay, we have to, we want to say something, so okay. You want to say something, say it, what we're going to say.

So, it's better quality rather than quantity. So, if you have like 20 young people talking, talking, talking, but we thought nothing to say, or we thought the proper knowledge, it became less respected. So, it's important that improve the quality. So, thank you.

[Applause]

DEBORAH ESCALERA: Thank you. And I apologize for the format of the slides. We're having some difficulties with this computer, and trying to format them.

Do we have any questions for Luã?

FRANK: Hi, my name is Frank [inaudible], I'm from a registrar, [inaudible] registrations. You mention sort of economic impact on why you can't participate. Do you not feel that the remote participation and mailing discussion lists are useful to you?

LUÃ FERGUS: Sorry?

FRANK: I said, do you not feel that the remote participation that's offered at ICANN and even IGF type events, and the internet email mailing lists, allow you to participate in the way you would like to?

LUÃ FERGUS: Yeah. Like, you talk about mailing lists like the ITF, about mailing lists, but I'm talking about the events, and you have people participating, and we don't see like the youth people participating as remote, or we have to engage them also in remote participation, but also come to these events.

Like, I have to have both things. Mailing lists, okay, remote participation, but they have to come here and see the face of the people who they are talking to, and to be better engaged at this point. And as my experience, the youth people, they don't have like the economic conditions, come to this place, and they would be only on the mailing list, or only through the web during this remote participation, it's not fair.

FRANK: I believe there are also, sometimes there are hubs setup in other countries, where you can join in and [CROSSTALK] face to face.

LUÃ FERGUS: In Brazil, we did a hub in the last inter-community event from ISOC. It was really great, like we put 20 people in University to talk about internet related issues in the hub. So, we are trying to engage people and try to create new options so people can discuss this, even they are too far, or too [inaudible] to do this.

FRANK: Thank you.

LUÃ FERGUS: Any more questions?

JANICE DOUMA LANGE: This is Janice Lange, ICANN staff. I would just like to address that in the sense that we do offer, through our global engagement stakeholder team, to meet the members of Rodrigo de la Para's team here, Danielle Think who focuses on Brazil. Rodrigo [inaudible], and Albert Daniels in the Caribbean. And we'd be very happy to help arrange an event, help you with outreach materials, because to this gentleman's point, and to your point, I think it is very good to have the face to face, but the face to face doesn't have to be at the meeting, if you could provide an event, and a webinar, and remote participation and access that way.

But I hear your concern, and it's a call to action, I think, and given a platform that will respond to the youth, that will engage them and make them think they're part of things, and invited up to the table. So, I respect what you're saying, and I think the gentleman in the audience was certainly trying to present to you that there are many options, we just need to focus on the youth, and what's going to bring them to the table.

It can't always be travel funding to come to a meeting, but it certainly can be support from the ICANN team, and from other internet entities that will help bring that engagement to the table.

So, work with Deborah to get introduced to Rodrigo, and start some conversation about how we can help you bring this very valuable, you know, entity, the youth, which we need, and youth is 18 to 30 something, and those are the faces that we need.

So, great comment, and I think we can work with this.

DEBORAH ESCALERA: Any other questions for Luã?

Okay, so hopefully maybe our slides will start to look a little better. Our next presenter is Matthias Hudobnik.

MATTHAIS HUBOBNIK: Does it work?

DEBORAH ESCALERA: It does if you point it this way.

Towards the computer. This way. Matthais, this way.

MATTHAIS HUBOBNIK: It's not working.

Okay, hello everybody. My name is Matthias, I'm from Austria. I'm studding law, and I will talk about the regulation of the digital environment, and will [inaudible] how the different concepts like cyber-libertarianism, cyber-paternalism, and network [inaudible] will affect the citizen of cyberspace.

Sorry. First of all, what is cyberspace? Cyberspace can be equated with their internet, and their internet can be defined as a network of interconnected computers. So, the question is, is it a kind of place? In other words, little space that consists of all of the data and information, or is it a sort of medium?

A very good article of [inaudible] problem, also you can see it on the one hand from a user's internet perspective, like the internet as a little world of cyberspace, or you can also see it from an excellent point of view, like the internet as a fiscal network. So really, it really depends on one's view.

So, this brings me to the next question, should cyberspace be regulated? The question is also, can it be regulated? If you see cyberspace like a medium, there is one definition also of Mike [inaudible], he just states that cyberspace is a kind of new media. So, it's not comparable with, for example, the television or like the telephone like many to many, or one to many medium, it's a kind of many to many media.

Cyberspace in the definition of [inaudible], he defined it like public space, like his argument that the new or the old times of media like publisher, broadcaster, distributer, or [inaudible] area, do not fit for this new physical, for this space. And this is like public new area with this certain digital characteristics.

So, the next question is also what is meant by a regulation. So, in some sort, a regulation means to monitor or control a process or set of behavior according to some requirements, or protocols, or standards. So, there are then two aspects to regulate.

On one hand, you can regulate like the content, on the other hand, the process. In like physical regulation machines, you have both of them. Then the last important question is, who should be responsible for the regulation? Should it be the government? Should it be private organizations? Or the users themselves?

So, the first concept was established in the late 1990s. [Inaudible], as some of you know him, it was John Berry [inaudible], he was a cyber-libertarian, perfect networks. And the original view was, cyberspace was unable to regulate. There are two very nice papers, one of, it is from John Berry [inaudible], the second one is from David Post and David Johnson.

And the key thesis of these papers were that cyberspace was not able to regulate because law is constrained by borders, and the internet is not law, and therefore it's not effective in cyberspace. It's a narrow view, and in fact, you see that this is not possible in particular use, because we need some sort of regulation.

In response to this view, there was also a paternalistic view from eminent law professors, most of them from Harvard Law School, Joe [inaudible], Lawrence [inaudible] Goldsmith, and they state that there should be a strong regulation regime, and the strongest one should be the regulation, why the architecture.

So, that means that digital environment is made by code, and the effort is almost as one to regulate this environment. A very well known example is the concept of the formalities of regulation. This is law of social norms, the market, and the architecture. So, Lawrence [inaudible] states that the user is seen as the pathetic dot.

I will give you a quick example. If you want, for example, to regulate smoking. The first law would be, for example, you just make a law which allows you to smoke within the age of 18 or something like that. Social norms would mean that nobody will, for example, smoke in a private place without asking the owner.

The market would be regulation wire on the prize or the taxation. And the architecture, of course, is the strongest one. This means like directly manipulate, for example, the nicotine level of the cigarettes, for example.

Then last but not least, the concept of the network [inaudible], it's from a law professor, most of them from the UK, like Andrew Murray and Colin Scott. Their argument is from cultural to community. This means that in most of the regulation regimes, the community is almost seen as they are typically regulated.

This is almost a problem. He states in his concept, the user as an active dot, and his idea is to make a kind of symbiotic regulation that means you should not build regulation upon the interactive users. You should use the community to make the regulation.

A good example for that is that the music service like Spotify, because nobody will, or a lot of people are just using this service, and they're not downloading illegal music. The percentage like in UK was really decreasing rapidly, because if you give the community what they want, they would not use the illegal service anymore, or at least, they would lesser use it.

Okay, then to the final argument of Andrew Murray, he also has the idea that some of the dots have, of course, more authority than other ones. For example, a really big gatekeepers, or highly influential like big tech firms like Facebook, or Google, or Yahoo. And they have a lot of influence in the Internet Society, B and C are smaller one.

B would be like governmental websites, and C would be, for example, like news media sites or something like that.

Finally, to sum it up, [inaudible] criticized [inaudible] theory that the regulatory [inaudible], is a kind of, that there is a kind of leg of accountability, like the normal detector, [inaudible] which you have in a regulatory regime. And the problem is also that they missed the big power of the community, of course.

The cyber-libertarian view in some way, is not really useful in practical issues, because you really have to regulate your internet. You can see it with all of the problems like hate speech and all of the crime which is going on.

Finally, also have some nice case. It's CDB versus newsgroup, newspaper. It was a case about some publication of information in social websites. There was a kind of injunction against this CDB. It was [inaudible] and meanwhile, when did the injunction, a lot of people were just retweeting the pictures and just said, oh this is Ryan [inaudible], and there was a lot of gagging and gossip going on, and they just stopped the court because it was not a strong case anymore.

And this is a very good example for the power of the community, and also kind of Streisand Effect. So it was almost unable for the court to start a judgment because so many people were re-Tweeting this, that ti was just not useful anymore.

Thank you very much and feel free to ask questions.

[Applause]

DEBORAH ESCALERA: Thank you Matthias. Any questions?

Okay. Our next presenter is Nertil Berdufi.

One moment while your slides load.

NERTIL BERDUFI: Hello. I am Nertil Berdufi from Albania. I'm actually working as a lecturer for [inaudible] at University [inaudible]. I'm talking about today following the investigation of cybercrime Albania, but this is related to the EU agenda or the convention of the Council of Europe.

It's not working, I think.

We are… I have started this presentation with a photo that shows very, that shows the weapons that we have used before to fight before, and this is taken from the [inaudible] Review magazine, 2013. You can see very well that in 1913, the weapons were like all the origin one. And in 2013, we have changed that. Now, we are doing work with electronics, with just a button.

And we can see, after that, the cybersecurity with the button. So, it's relation that [inaudible] has shown. Also, there is a big deal. The Director of CIA in 2011, I think, he talked about the new Pearl Harbor that could be very well a cyberattack. This shows the responsibility of the problems that we have the cybercrime now.

The [inaudible] of cybercrime. As we know, cybercrime today is one of the greatest legal challenges. Cybercrime is a criminal activity that includes information, technology infrastructures, [inaudible] access [inaudible], data interception, electronic forgery and fraud.

This is taken by the convention, and this is what we have got also in the Albanian legislation. It's not a lot. As we have seen, or now from the year 2000 2016, we have the rate of expanding the internet globally in 918.3%. That is around… We can see the 4 billion, around 4 billion, because as we saw in the morning, it was 3.9 billion persons are online today.

Almost all crimes can be committed with the usage of the computers, analyzes of the correct situation and being related to the legal standards, mechanism for the investigation and persecution of the cybercrime, and the identification of problems is what we are talking now.

Here is compressive fashion activities that shoots across three key pillars, that are NIS, law enforcement, and defense. Here we can see that you have their own produce, their own agenda. And the network and the information situation, they are composing about [inaudible] network of contacting authorities, etc.

And the national aspect is with national threats and [inaudible] authorities. Also, for the law enforcement we have, in Europe, that is [inaudible] and C-Pol. Also in national area, we would have national cybercrime units to fight the part. Defense is the main, or the other problem that we have with cybercrime.

And the European Union has done his own job. He has created Europe and Defense Agency that works very well in this field.

Also, the nations has done changes according to this part, and national defense is in security authorities has been created. What is very important and very interesting here is that, industry and the academia. Which role is very important to fight or to create laws, etc. for the fighting of the cybercrime?

Here is line chart, where we can see that in Albania, we have started combatting cybercrime, starting from 2008. Before this year, it wasn't convicted. It wasn't a crime, because we haven't entered in our legislation. So, after we have ratified the convention of cybercrime, after that, we have done the changes in the criminal court, and just a few years after that, we have had the first cases, just and convicted persons.

Now, as we are preparing to part of the… So, we are going in a higher level of using cybercrime. What is criminal evidence? In our panel court, criminal court is a notice of information, all the facts and circumstances related to the criminal offenses, which are obtained from sources provided for by the criminal procedural law, in accordance with the roles prescribed by it, and which serves to prove, or not, the commission of the criminal offenses.

This is the only article that we have in our procedural criminal court. The problem with the jurisdiction, as I remember Katharin talked about, that, so it's a big problem for us. The jurisdiction in this part of fighting the cybercrime. And here, we can see, I'm not repeating what she has said before, because it was very deep.

Electronic evidence. What we can use as evidence. As you see, computer system, hand devices, such as cellphones, smart phones, PDA, [inaudible] computers, [inaudible] GPS, etc. can be all of this can be part of the electronic evidence.

In fact, in 2009, the Albanian state police with the support of the Office of the Crime and Drug of United Nation, has drafted the manual guide for cybercrime investigation and computer evidence in service of the state college. The [inaudible] gridlines of types of computer evidence, and how to deal with them step by step.

This product is confidential because it's very important to get it by the police and by the structures that are responsible. In 2014…

DEBORAH ESCALERA: Slow down just a little bit for the interpreters, please. Thank you.

NERTIL BERDUFI: Sorry. In 2014, we have created the first cybercrime investigation units, and this was expanded by specialists in police department also in the prosecutor office. So, the cybercrime sector, and specialist structures, near eight districts prosecution office where established. This was the first time that we have created a responsible persons who can take, or who can be very qualified to get in the cybercrime investigation units.

Also, in the sector of cybercrime investigation, attacks for the [inaudible] created by the police, and this was during that year that we were talking 2014, it was 180 offences were recorded, the area of cybercrime, which from which 76 were discovered. That shows that we have around 100 of the cases were not solved.

So, it's a big problem for us. Also, what I have done, is that I have interviewed four of the main important persons that fights the cybercrime in Albania, which are the heart of the cybercrime unit of the prosecution offices, which is the case that is a need in fighting a faster way of international information exchange for investigation of cybercrime, instead of letter or regulatory.

This is a big problem to get the information, and this takes time a lot. So, one big solution it was found with the Facebook, that they have done good work together, so they can get information without two weeks, and this is a big deal because in our country, they have a lot of crime that are committed by the Facebook, or using the Facebook.

The challenges that we have is that ISP do not have the facilities for the storage of the minimum information required by the law. More than technology and the [inaudible], but lack of humor resources. That is the big problem, the qualification of the human resources are very down.

Also, the lack of expert for expectation and protection of digital evidence, as well as the presentation of the evidence in the court, with cooperation with the ICP, lack of will to cooperate with them. [Inaudible] a national authority, as we talked before that each national nation should have a [inaudible] this institution is not working.

They do not have nothing, they have done nothing until now. Also, the problems that the challenges that we have, according to the security policy expert, the biggest challenges is the identification of the critical infrastructures, and the expectation of national security strategy. This is for our state. We do not have until now, what are the critical infrastructures?

That's the list. Also, one other thing is that, even through training about cybercrime investigation are frequently held, they are all organized by foreign organization, as FBI, [inaudible], COE, none of them is organized by the Albanian [inaudible] or the Albania personal. Training persons never stay in their assignment position for long time, which results both in economy costs, and lack of expert in the field.

What is the problem? We can get a person qualified doing a master PhD, or whatever, outside our country. Be an expert, after that, he came at the Albania, he works at the same position that he held, after one year or two years, he leaves that part. He goes outside in the private sector to get a better wage and so on.

Conclusion is that the Albanian legislation is in accordance with European standards and international conventions. Sign it and ratify it, all international conventions related to cybercrime. Legislation still need to be updated to be in our criminal court. So, we are just doing the ratification, we thought incorporate them in our panel or procedural panel code.

Also, is the active implementation is also crucial. Which means that after we have done the implementation, or writing of the laws, we need the persons who will do the job.

This is what I have. Thank you.

[Applause]

DEBORAH ESCALERA: Thank you Nertil. Are there any questions for Nertil?

Thank you. Okay, our next presenter is Olga Kyrliuk. Probably butchered that last name.

One moment while your slides load.

OLGA KYRLIUK: So, this discussion has already been studied by Jackie, Katharin, Krishna, and Matthias, but what I [inaudible] is just to look a little bit more into the global processes of internet governance institutionalization and try to understand where we are at the moment. It's too fast?

DEBORAH ESCALERA: Olga, I just want to remind you to speak slowly for the interpreters.

OLGA KYRLIUK: So, what I wanted to do now is just to look a little bit more into the, what are the global processes of the internet governance institutionalization? In order to understand where we are at the moment, is the point of the cooperation, or are we approaching that firstly, the threshold of the [inaudible].

It doesn't work. Yeah, it works. So, I'm Olga, I'm Ukrainian, and the reason I'm here is that I was lucky to be selected as the

NextGen Fellow, and the reason why I selected this topic, okay, NextGen. Just NextGen. And the reason why I selected this topic is because I have always been interested in this process, how the internet governance is happening and another thing is that it has become part of my thesis, and I little bit covered it within my research topic.

So, in case you will be interested in somehow following this discussion, you can always find me on Facebook, LinkedIn, or email me. And coming back to the topic. I would like to start with the quotation of the person you all know quite well, he's known as the founder of the internet.

And what he said is just that, that no matter what you do, any country in the world is going to have the ability to set its own rules internally. Any country in the world can pull the plug. It's not the question of technical issues. It's not the question of right or wrong, it's not a question of where the global internet governance is right or wrong, it's just with us.

And that's what I like so much. It's not about whether we want it or not. Internet governance is just here. It's not the question of whether we accept it or not, it's developing. It's going its own way. The only thing that we can do is just like to step up on this path, and try to understand how it's the best way to govern these processes, how is the best way to try to get as many people as possible to take part in these processes.

For quite long, it was a standard that only the states were the only ones who had the power to set the standards for the international relations. They were the only ones. They were the most powerful, but now these things are changing. Now more and more stakeholders are getting into this stage, and they are getting their voice, and they are getting their opportunities for their voices to be heard.

Let's try to look at the [inaudible] example, that internet governance is. And I often to imagine it as the bicycle mechanism. In order to make this mechanism work, we need to have two wheels, both two wheels operational. If only one wheel will be operational, and the other wheel will be slowing down, this whole mechanism, or the bicycle, will not work.

So, if we imagine one of the wheels as the internet exceptionally, why exceptionally? Because the internet is such an unique structure, which is global by its nature, which is trans-national, which doesn't know the borders, and I'm trying to be slower, but it seems to be fast.

So, that's why the internet is that much exceptional, and that's why it requires the spatial regulation. It requires the spatial mechanisms to approach it and to govern it. And one such mechanism, which at the moment, seems to be the most appropriate and the most efficient, is the multistakeholder.

Th emultistakeholder is the, each and every stakeholder who has something to do with the internet, should have his voice heard. It means that each stakeholder on the [inaudible] their decisions, which are in anyway related to the internet, may have the effect, may in anyway effect his rights, interest, should have the right to step in and participate in this process of global governance.

Currently, the two basic models which we have, are the multilateral model and the multistakeholder model of internet governance. I will start with the multilateral model, since it is the one which is based on the mostly [inaudible] participation, and it is something which has been known for quite long, and we should historically be, like the only recognized model for the global processes of governance.

So, to start with, will be the ITU. It is the organization which is, at the moment, trying to have its stake in the processes of internet governance. But, being based on the sovereignty of the states, the ITU doesn't have that much opportunities to be the only, and the main stakeholder in the processes of internet governance.

Anyway here, the ways the ITU is trying to influence the internet ecosystem, is by having the plenary conference is by discussing the issues of the internet governance, somehow trying to point that probably by broadening the very notions, which have been used by this organization like the traffic, like to cover the internet as well, they are trying in that way to be the step in the processes of internet governance.

The next one is UNESCO, which is known for its programs on education, e-knowledge, and on trying to make the internet as multilingual as possible, trying to get the content in as many languages as possible, so that people all over the world can understand what kind of information is being transmitted through the internet.

And in this sense, the IDNs make a very good work, because they help the people to have the access, and to have the content in their own local languages. The next organization I would refer to is the world intellectual property organization, which is mostly known to be connected to the internet by its so-called internet treaties.

[Inaudible] which are not that popular and not that much discussed are the open government partnership and the freedom online college, and this also state based initiatives. The first is currently consistent of 75 countries all over the world, and the second one includes 30 countries, and they're basically trying to make the operation of states more transparent, more accountable, and to prove that the states can do as much to help their people to exercise their rights, not only offline but also online on the equal basis.

And the one which is probably my favorite is the world internet conference, which is also known as the [inaudible] summit. It is the China, it is the Chinese initiative, which is already been convened for three consecutive years. And it is interesting in a way that China is trying to say they have their own stake in internet governance processes.

They're trying to create this regional ecosystem, and they are trying to push the agenda that the cyber sovereignty and the cybersecurity should be, there are issues which still play a very important role in the internet governance ecosystem. But the thing is that the security and privacy, they are not mutually exclusive.

This are things which should be very complimentary, because when we are talking about security, it doesn't mean that with the security comes the [inaudible] comes the control from the state.

And when we say about privacy, it doesn't mean that, and when they say about the free flow of information, it doesn't mean that you can do anything you want. Still, there are some remits that your rights, so they should not in any way [inaudible] the rights of the other person.

And here we come to the next model, which is completely different from this one, and it is based on the participation of all of the stakeholders, and that's why we are calling it the multistakeholder model. And this model studied back in 2003, 2005 when it was convened, the world summit on information society, and even it was convened on the initiative of the ITU.

This summit became the first global meeting of the stakeholders has the opportunity to discuss the issues of internet governance. The other one is the IGF, and the European [inaudible] of this, is the EuroDIG. Quite interest [inaudible] was the Netmundial, which was going to be, in Brazil, and which was supposed to… Some had even felt that it will become the substitute the idea, but it didn't happen because unlike the one time initiative, and the our favorite is ICANN, which is probably the future of the internet governance, and probably the organization which has the very big potential, the huge potential that will govern all of this processes.

This is what happened not so long ago, the IANA transition, and when this function was transferred from NTA to the global mutlistakeholder community, and what we have at the moment is that we need to come up with the transparency and the accountability rules, how this system should function in the future, and what we should do.

And another reason for me for choosing this topic was so that at the moment, there is the open call for the accountability and transparency review team [inaudible] don't know how much we can do, and how much we can get engaged in this process. But, if there is any opportunity, I would like to look for the race to be engaged into that, and wrap it up, since we don't have any more time.

Like on this picture, you can see like many of you may know Dr. Strange, the superhero over American, and he didn't believe at first this interconnected worlds, but it's our choice what to choose, bodily space or bodily place, and it's always our own choice to adopt or to resist the changes.

So, if it was my choice, I would always opt for the multistakeholder model, for the engagement of all of the stakeholders or all the people, so that all the voices all over the world will be had. Thank you.

[Applause]

DEBORAH ESCALERA: Okay. Are there any questions for Olga?

Okay. Our next presenter is Peter Chon. And remember, speak slowly for the interpreters.

PETER CHON: Is this on? Yeah.

All right, great. Hello everybody, my name is Peter Chon. I'm currently a student at the University of Cambridge, where I study computer science and technology policy. But today, I would like to present some work that I did as a Google Policy Fellow for Learn Asia, which is a think tank focused on information technology development, in the emerging Asia Pacific.

In particular, I looked at zero rating. So, for those who may not be familiar, zero rating is a practice that is undertaken by mobile operators. Now, they will generally offer data for free, but that data is limited in content. And we're generally talking about mobile data.

So, this feature, zero rating, we use for a number of different purposes, but in the competitive marketplace in the global south, in particular, it's being used for access development. So, we're thinking of an important statistic is relevant here is that the network infrastructure is in place to serve about 70% of the global population to connect 70% to the internet today, and yet only about 45% are actively online.

Now, research has shown that one, there is a concern about affordability, two, even if people afford access, there is a question of relevancy. I haven't gone online before, what does it actually have to offer for me.

And so, enter zero rating, which would offer the idea of free content to deal with the affordability issue, but also offer a teaser in the sense of, this is what could be relevant to me on the internet. Now, this is somewhat controversial, so many of you may be familiar with Facebook free basic, it's probably the most notorious version of zero rating, which is an operation in over 50 countries in the world.

But there are other versions as well, Facebook, excuse me, Wikipedia free is another popular option. Now, this debate is centered around the idea of a walled garden. So, if we're bringing people online for the first time, they may come to understand the internet to be something that is limited to corporate sponsored content, and they may not push to access all here at ICANN we're trying to offer in terms of the open internet.

And so this has been a net neutrality debate taking place in countries around the world, and we may know, India, the regulator there determined that zero rating is illegal in 2016.

But, I would offer that much of this debate is based on empirical assumptions, for which there has been little research thus far.

In particular, a key question is, when people go online with free basics, do they truly stay within the walled garden, or do they transition to the open internet, having gone online for the first time with free basics? So, my research looked at me and Martin in particular, and offer us a little bit of context.

So, the past few years, market liberalization about 2012, it's rather they change the mobile landscape in [inaudible]. So, SIM costs went from costing thousands of US dollars, down to under $1.50 today. And with that, we've seen mobile penetration increase tremendously. So, one metric has more penetration up to 90% as of last year. Learn Asia, has conducted a representative survey of the entire country, and they put that number a little bit more conservatively at 83%.

But that global disparity between network access and use of the internet remains present in [inaudible] as well. So we'll see about only 40% of those who have access are actually connecting to the internet. And so enter zero rating as an option that marketers have been, or telecom regulators, telecom operators, excuse me, have been looking to use in [inaudible] in particular.

So, in 2016, two offers launched. Facebook free basic is one that many of you may be familiar with, and I guess I should explain, briefly, what free basic is. So, free basics is Facebook without images and without video, available for free.

Messenger, available for free. And then a number of country dependent offering. So, Wikipedia may be available in many countries, local news sources, UNESCO, or other UN sponsored content available as well. Now, that's free basics.

[Inaudible], another operator, in [inaudible] launched about a month later, to compete that was offered by MPT. And their promotion was a little bit different. So, in terms of structure, they offered free Facebook, with complete content. So, people could watch video, people could look at images.

For 150 megabytes a day. They also offered free text on [inaudible]. And so this was an effort to spread access, and to have competitive marketplace. So, my research was looking at how people were using these features. So, my research focused in [inaudible], I did eight focus groups in the city, and then two in a rural area surrounding the city of [inaudible], with a total of 63 users.

It should be noted that this was purpose of sampling, so those that we talked to used internet data, and so we should not construe these findings to be representative of the entire country. Instead, they are qualitative deep findings, we should understand in context and their limitations.

Furthermore, conducted a few stakeholder groups to understand the internet marketplace that's in [inaudible] and how it's expanding. So, I'll jump into a few key findings. I only have time to talk about three, but I would urge you to see the report if you're interested in knowing a bit more.

So, first and foremost, although Facebook sells free basic to stakeholders around the world as a means to introduce people to the internet for the first time. The way it's marked and practiced, may not align to that sort of high goal. Instead, in [inaudible] we found that those we talked to did not know the Facebook free basics was more than Facebook.

And this arguably could be a function of the way it was being marketed there, so MPT was essentially marketing this promotion as free Facebook, and that was it. And so, I would argue that given this understanding of, if zero rating is to be permitted around the world, it's important that jurisdictions look at the way in which it's marketed to people quite critically.

Another important finding is that design choices about promotional construction and also user interface, are very important in determining how people actually use the offers.

So, the two offers, Facebook free basics with MBT, which has this limited video content was used very differently then [inaudible].

So, I can sort of explain that a bit more, I think. Essentially, with MPT free basics, because there was no video content, there was no photo content. People felt pressured to sort of shift back and forth between free mode and paid mode, if they were scrolling through.

One stakeholder sort of put this quite nicely by saying, Facebook without this visual content is essentially like curry without the sauce. So, it's like, what is the motivation to use that? We don't have that. And so this switching back and forth in addition to quite slow data speeds, led a number of people to either stop using the promotion after they tried it, or to heavily restrict their use to particular cases.

Say, someone was out, they ran out of their top up, but they wanted to keep in touch with people before they go to the vendor at the market and buy another top up, they would use the free version temporarily. Now, this sort of content limitation led to people to understand quite well when they were using a free zero rated promotion versus the open internet.

The contrast was quite stark, but this differed considerable with those on [inaudible] free. So, those on [inaudible], used the promotion quite extensively, and actually increased data use while on the promotion. So, some people tried video for the first time on this free promotion. And many increased their consumption, they paid for this increased consumption, and you could essentially call this an on ramping effect.

Yet, this on ramping effect was limited to Facebook. So, people were using more data, but they were staying within the walled garden. Furthermore, there was a tendency to conflate this free data, which was only for Facebook, with free data at large. People would refer to this as my daily allotment of data. And not be quite explicit with the limitations therein.

And so, this scrutiny about design and design with the user interface, but also design with the promotion, I would argue, is also warranted when we're looking at debating whether or not we want zero rated content.

Nonetheless, in the interviews, it became apparent that most respondents did indeed exit this walled garden, so they did use content that was not zero rated. So, this took the form of many different things. Generally people would use other apps like Clash of Clans, or Google, or [inaudible] which is a messaging application that is quite popular in [inaudible].

And so, that's an important finding to know that people, although they do heavily to use these promotions that they may, that they do indeed exit the walled garden.

And last but not least, I think this finding has the most relevance to ICANN in particular here, is this idea that those who are going online, those as access spread, are tending to use apps more than a browser. It's only about one third of those who I spoke to used a browser on the phone to access the internet.

Instead, when they were using mobile data, they were using through an application. And so, I think that that is relevant to ICANN in two ways. So, one over the past few days, have been hearing a lot about, sort of focus on the end user, and who that end user is, and how ICANN can sort of better incorporate the end user into the multistakeholder model.

With an increase and reliance on apps, I would argue that sort of separates the end user, an additional step or two from the mission of ICANN. So, if someone never types in a domain, or an URL, when they're browsing the internet, they focus simply with an application, that reduces the relevancy to ICANN to that new person who is coming online.

And so I think as the CEO this morning spoke about, sort of trying to raise the diversity in ICANN and do a better outreach to these end users who are coming online for the first time, this is an important challenge to remain relevant, and to seek these end users. And two, I fear that this could lead to defining down what an end user is, so if we're thinking of those who go online to apps, perhaps ICANN could pick the easy way out and define end user as those who create the applications, and those who simply register the domains, but forget that end step of the people that are actually using the domains that are using the application and I fear that that is an easy way out.

That we may be pressured to take. So, I would urge us not to do that. That's all from me. If you're interested in seeing the report, please check out my handle on Twitter and it's up there. Thank you very much.

[Applause]

DEBORAH ESCALERA: Thank you Peter. Do we have any questions for Peter?

Okay. Our next presenter is Valerie Filnovych.

VALERIE FILNOVYCH: May I start? Okay. My name is Valerie Filnovych. I'm from Ukraine. I have a PhD in law and work as a lecturer in the university, the lecturer of intellectual property law. Today's presentation is named problems of national regulation of domain names in Ukraine.

And if I have enough time, I'll speak also about the infringement of copyright in Ukraine.

So, domain names. First of all, let's speak of such problem, the national regulation of delegation of domain names in Ukraine. I should underline that there is now specific legislation on the transfer of domain names, on delegation of rights on them. Such a transfer is just concession, could only be a concession of rights on such domain names.

And such rights appear at the moment of the conclusion of the relevant agreement between the perspective [inaudible] and the registrar. The next problem which [inaudible], please look at this image. It's a form which should be held up for the registration of domain name in Ukraine.

I'd like to speak of the advantages of the system. First of all, if we need a domain name registered in the national domain, dot UA, we need a trademark to be received before the domain registration, because if you do not have the trademark for the domain you needed, you will not get it.

But, if you want to register a domain of lower level, such as dot [inaudible] UA or dot N UA or something like that, your registration process very soft, very loyal. So, you need only four things to get a new domain. First of all, you need a name and surname, even [inaudible], even fake, because no one checks your documents.

The next one, you'll need cell phone number, just in case you forget your passport and want to recover it. Next one, email. It's clear. And the last thing to do is to agree with the terms of the service agreement. So, such a situation with the registration, with [inaudible] registration, arrives now the problems.

First of all, therefore anyone can easily register a new domain, and some place legal content on the website under such domain. The next problem. The proof of the IDN [inaudible] of the person who can be an offender, yes? The problem of his identity would become a very complicated cause of the reason, we do not know, who is the perspective of such domain.

The next one. The unified domain name resolution, dispute resolution policy is still not applicable in Ukraine. Yes, one of our administration of public domain, dot UA, presented such proposition to make this policy the main policy for the dispute resolution [inaudible] but, this proposition was not, did not receive the support.

So, our citizens are to defend their rights only by means of traditional judicial process. If you'll compare, it was [inaudible] the last one, seems to be cheaper, seems to be faster, and of course, more convenient for the people, now for the parties.

Also, do not forget about the level of corruption in our Ukrainian courts. So, there are some things which should be done as to the problems I have spoke about. So, first of all, it should be provided a straighter procedure of domain name registration. Of course, it should consist of [inaudible] verification for the personality of the owner of the domain.

For example, in Russia, you should provide this scan of your identity card, such as first [inaudible] passport, you get a new domain. Also, they have such rule, the domain name should not contain abuse of [inaudible] different [inaudible] calls or so on, or your registration will not be admitted.

In our… As I have said, in our, we do not have the proper legislation in Ukraine on such topic. But, we have some temporary rules made by non-governmental organizations, and such temporary rules as to the registry of domain in dot [inaudible] domain. This regulation, this rules have a special stop list of us, and expressions, which are not to be admitted in the domain name.

The next thing to do, it should be created a uniform state registrar, of all owners of the domain names in Ukraine national zone, dot UA, and regional such as [inaudible] and so on. Also, there should be developed special regulation, which will fix rules and regulations of the registration of the domain name.

Do I have enough time? Okay. I'll speak about the corporate infringement on the internet, of course, about Ukraine. Okay.

The first thing I want to [inaudible] the procedure, or means of [inaudible] of copyright infringement on the internet in Ukraine.

The decree of, the plan of supreme economic court of Ukraine, number 12, contain a list of possible evidence of copyright infringement on the internet. So they are, bring to webpages, videos, audios, and certificates. Print webpages, but not every print page can be in evidence. So, print webpages but those which were witnessed by the institution [inaudible] person within their powers, within their jurisdiction, and then this print webpage should be sealed.

The next one. Video and audio. Video and audio containing the process of research through the website, by any interested person, made on electronic or of the material [inaudible]. To be submitted to the court. Yes, of course. Indicating the time when was this, the time of, the time, the conditions of establishment of such records, and the personality of a creator of such record.

Then certificate received from network providers from, for example, search [inaudible] things to do.

Sorry.

So, things to do for the defense of copyright on the internet. First of all, our list of copyright [inaudible] in the copyright law in Ukraine, should be updated with the notion of the website.

[Inaudible] should be added with the list of specific guidelines to, and as far as responsibilities for violation of intellectual property rights through the internet of, for informational [inaudible] diaries for owners and users of internet, yeah, of the website.

The next one. That should be developed a common set of model contracts on creation of the website, then of hosting service for the implement on these server for domain name registration. So, there should be created an unified system of right protection by such X. By such contracts.

Then, there should be made a providers responsible for supervising after the files applauded by the user, because users are the most, they often…

They became offenders of copyright law on the internet very often. And the next one, there should be borrowed some provisions from stop [inaudible] from USA, as to blocking domains, and from [inaudible] as to the exchange of data of cyberthreats between government and commercial organizations.

Many thanks for your attention. Questions welcomed.

[Applause]

DEBORAH ESCALERA: Thank you, and I love the picture at the end there. Questions?

UNKNOWN SPEAKER: Hello, [inaudible]. I just, those last points about copyright protections, was that your suggestions? Was that your suggestions? Your ideas, or the general idea…

VALERIE FILNOVYCH: I gave some suggestions on the last slide, not with [inaudible]… [CROSSTALK]

UNKNOWN SPEAKER: …the hosting provider should monitor the content of the, what the users upload is very controversial. Don't you think?

VALERIE FILNOVYCH: Yes, but as I say to my students while teaching the intellectual property on the websites, I ask, I advise them to make, for example, watermarks on the images place on the websites then to conclude agreements of all sorts. It's for the owners of websites. So their information, their website, will not, became [inaudible]…

So, watermarks and special agreements with [inaudible], with the creators of the computer program for the website, because every website has a [inaudible] license agreement with the user not to do so.

UNKNOWN SPEAKER: I see. So, it's not so much that the person uploading content… The person uploading content could be a third party, maybe someone like Facebook, their users are uploading pictures or something like that, rather than somebody who has created a websites, uploaded it, and then their hosting provider should be scanning and looking at all of their pictures to see if they infringe a copyright.

How would they be able to make that judgment?

It's very complicated, sorry.

VALERIE FLINOVYCH: I'll think about your question.

DEBORAH ESCALERA: Okay, I think Valerie will have to… If you would like to email, we can take that question offline. Thank you, Valerie. Any other questions?

Okay, our final presenter, last but not least, Yousra Hsina.

YOUSRA HSINA: Hello. My presentation will be about internet service providers and online privacy.

DEBORAH ESCALERA: Please speak into the microphone and speak slowly. Thank you.

YOUSRA HSINA: Thank you. So, I said this presentation will be about internet service providers and online privacy. So, we all know that social media and the websites we visit, collect information about us, and that they use it for advertising purposes. However, we rarely stopped to realize does our internet service provider can also collect information about us.

The fact is that you can choose which to sign up for social media. You can choose to visit a website or not. But once you stop [inaudible] for an ISP, it's a bit different. [Inaudible] service is different.

Because when you sign up for an ISP, there is like no way to go back. The user have a little flexibility to change his mind, and also he cannot avoid that network. I mean, think about it. Your ISP handles all of your network traffic. That means, it has an overview and a wide view of all of your internet traffic.

The websites you visit, the apps you use, everything.

However, we do not deny that nowadays ISPs are slightly limited by some technological developments. [Inaudible] ends, encryption protocols, and the [inaudible] of devices, because obviously, nowadays, nobody has only one devices. We have multiple devices.

So, I will go back to the virtual private networks. When using virtual private networks, the user's computer creates an encrypted channel to the VPN server, then according to the VPN integration, can send some internet traffic to the VPN server.

But the other point is, that's all the VPNs have been commercially available for years, they are poorly adopted. And also, they cannot provide complete protection for the user. As for the encryption protocols, truly pervasive encryption is still a long way off, because if we compare the fraction of the internet traffic that is encrypted with the fraction of internet traffic that is uninterrupted, we would find that the latter is bigger than the former.

The internet fraction that is not encrypted is a poor proxy for the privacy interests for the typical internet user. I will give you the example of the [inaudible] categories of research that are health, shopping, and use, obviously.

The studies or the statistics have found that more than 85% of the top 15 sites that we visit, still fail to adopt encryption protocols into their web browsing. So, obviously, ISPs can then have access to all kinds of information that shows that when we're looking for medical health, when we're looking for advice about that, or just when you're buying a product.

Another point is that… Another point in the same section, is that even with HTTPS, the ISP can still learn about the user. How is that? Is that even with HTTPS, the ISP can still see the domains that the subscribes visit. And that's going to be very revealing. As I said, even we've encrypted the websites, ISPs can access a lot of sensitive information about their customers.

A group of research has… A group of computer scientist researchers have found that ISP can access a large amount of content about their users, encrypted content, to be precise, without breaking it or even weakening it. Simply by analyzing the features of the packets, such as the time, the timing of the packets, the size, and also the destination of the packets.

ISPs could learn more informative habits about their customers, that can uniquely identify, for example, the webpage visits, or just other information about the contents.

And now after [inaudible] the facts, I will talk about the regulation, specifically the example of the US. So, American internet users, last year, won a significant victory when the

Federal Communications Commission adopted their broadband privacy rules, that was last year.

And those rules state that the ISPs need to first, before sharing the sensitive information of their customers, they need an opt in customer permission in order to share this information. The rules require the ISPs to protect the instances of information of the users, and to specify some technical steps to do that.

Now this was going to be a successful example, but unfortunately it's not because the regulation was supposed to take place two weeks ago, but it didn't. The critics have complained that the ISPs and other, not only the ISPs, but other online companies have also access to our information. So the question that was…

Should government privacy regulation protects consumer's internet day from an invasion by all internet companies, or be only a few? So the answer is obviously A, which is not the case of the regulation of ISPs. The problem that was, that was, or the what was contested, is that other online companies, such as search engines, and the websites, and in operations assistance of [inaudible], they weren't required, or they weren't into the regulation.

It was only about the ISPs. And that was seen as a form of discrimination against the ISPs, so it was contested, and it was not adopted.

Okay, that's all I said, because the known ISPs intrusion, in online privacy is as much as important as ISPs. It's clear that there is still long way, and there is a lot to do to regulate ISPs, and that would obviously take time, and there is still controversy.

I will end my presentation simply by reminding what the consumer wants, so what we want is consistency, uniformity, simplicity, and transparency from our ISPs. Thank you.

[Applause]

DEBORAH ESCALERA: Thank you Yousra. Are there any questions?

Yes, no we can go forward… That concludes our presentations for the day for our audience members, and we would like to thank you for joining us today. I know it's a little bit before schedule, but we'll continue on with the questions from the NextGen members. So Rachel?

RACHEL: I actually like, if it's okay to make a few general comments from throughout the day, because I waited until now. And so, I'll try to be quit. So, first I would like to just thank all of the… Yeah.

Well, it's based on the presentations. Is that…? [CROSSTALK] in the audience, it's okay.

So, just to say to all 15 of you, thank you so much for the effort that you put in, and it was really interesting, and I've learned about all kinds of topics. I knew very little before like block chain technology and how zero rating has actually been taken up in practice. And so, that was really fantastic.

I wanted to make a very small correction or addition to one point, just because I work on this topic. On this slide, about the multistakeholder model and the multilateral models, just to add that because I work at UNESCO. UNESCO is a multilateral institution, but it has strongly endorsed the multistakeholder model for internet governance and move that up to a positive thumbs up on that slide.

It's just a joke. And so, a more general comment, again based on my work which is to promote freedom of expression, I think several of the presentations, there were ideas presented, and I think it's fantastic and really important to come with fresh ideas, new perspectives. On some issues, there may be human rights applications that haven't been thought through as much about what it would mean for privacy and freedom of expression, to not allow anonymity or to have a personally connected IP addresses, to shut down domain names based on copyright infringement.

So, some of those issues, what I would encourage you maybe is to think about the human rights applications. There is also a session at 3:15 this afternoon with the European Data Commission, data commissioners, data protection commissioners, and also the UN special rapporteur on privacy.

So, I think that will be a really interesting session. And then, more generally, I think a suggestion would be to come in and bring your expertise, and your ideas, and also to be open to other perspectives.

So, if you come in as, with a security background, or an intellectual property background, or human rights background, talk to the other side and be open to their arguments, and because I think that's how for me, the multistakeholder model really works is by people coming together sharing understanding and reaching compromise.

And the question of youth engagement that came up, and I think that was a really interesting and a lot of valid critical questions raised, my own feeling is that it is, you can do a lot with remote participation, but there is also an importance of bringing people to a physical meeting, at least the first time.

In the literature of network work, by [inaudible] they talk about the importance of face to face interactions, that then can build the foundation for online email exchanges, conference calls. So, I just want to express my strong support for the NextGen program, and I think this is a really important and strong initiative.

And as the CEO said, I think it was yesterday, the youth are the future of the internet and the future of internet governance, and so ICANN needs you, and thank you for all of your efforts. Thanks.

[Applause]

DEBORAH ESCALERA: Thank you.

UNKNOWN SPEAKER: If all NextGen could remain in the room, because I would like to discuss some things with you.

DEBORAH ESCALERA: Does anybody have any questions for the presenters, your fellow presenters? And we'll just go around on the round and follow-up on you presentation. Did you have something?

UNKNOWN SPEAKER: I think I have a stupid question, but is it possible to have all the slides of the presenters?

[SPEAKER OFF MICROPHONE]

Yeah, perfect.

DEBORAH ESCALERA: Does anybody have any questions for their fellow presenters? Okay, Carolina.

CAROLINA MATAMOROS: Okay. Thank you for the space to actually make some questions. First, I wanted to talk about this child pornography and on this, so I would like to talk to that. I wanted to know from the prosecution point of view, does this [inaudible] as just where the crime was committed? Or also when the user consumes these products?

Like, how the prosecution goes. Because if I like make a parallel let's say with drug abuse, usually you do prosecute both things, both the production and commercialization of things, as well as the usage. So, I wanted to know this [inaudible] for the child pornography crimes.

UNKNOWN SPEAKER: So, it depends on the national laws of each country, but mostly they all criminalize both production and usage.

DEBORAH ESCALERA: Go ahead. Please state your name, I think we're still recording.

PETER CHON: My name is Peter Chon. I have a question for Abdu about the block chain, and your work in particular for the tech 4D project, which as I understand it, is to use block chain technology to facilitate to NGOs. And I'm not an expert on this by any means, but I'm curious. It seems like the block chain would help with trust and verification of the transaction, but does it do anything to address the issue that I think is central and sort of concerning funding of NGOs? Which is, once the money arrives there, once the transaction is completed, how can you then have the trust and verification that it's used for what it is to be used for.

So, is there any kind of use for the block chain technology to further compliance down the chain? To use that word again, but to further compliance once the NGO has the funding, could block chain technology mandate or ensure that they use it as they said they were going to use it.

So, to ensure contractual obligation after the transfer is completed.

ABDERRAHMAN AIT-ALI: Thank you Peter, that's a very good question, actually. What we basically do is, so there is like this phase of using block chain as a tool for smart contract. And there are also other functionalities that we added to the tool. The tool is actually in early stage development, so we are still doing several [inaudible] and putting it into tests for different…

We have a prototype and we have a NGO that is working with refugees in Syria, basically in the boundaries with Turkey. So, what we first do is we use a [inaudible], a [inaudible] block chain, so we didn't opt for our own block chain software, because there is already a lot of APIs for [inaudible].

So, we used that and then the NGOs are basically getting funding from different funders. And once there are multi-stage funding. We basically launched the first level of funding when it's achieved, we stopped it, and will the NGO get the funding once it's on the field, there is a process of following the NGO in terms of activities. So, in the interface in the prototype, there is a feedback platform with pictures and all of the proofs, and then we can go to the next level of funding.

So on and so forth, and until all the project is basically funded. That's basically how we follow it. And of course, the prototype is open for additional functionalities, along the way we basically, based on the feedback that we get from the NGOs, and also the funders, we will add more and more functionalities.

But basically, this is how the prototype looks like to it.

[SPEAKER OFF MICROPHONE]

OLGA KYRYIUK: Olga Kyryiuk, Ukraine. Thank you for the comment. [Inaudible] for the UNESCO is not to offend it or it's bad, it's only… The point was to show that the main difference between these two models is that like multilateral is based on the organizations which were initially [inaudible] consisted of the states, and that only now they own different place, [inaudible] to engage the other stakeholders.

They can't avoid that, of course, because that is the trend which is happening now. That's like the states have been the major ones during quite a long time, and it's only now that they are trying to engage others. But like the multistakeholder ones, but they initially were created as [inaudible] had all of these stakeholders that are presented inside.

UNKNOWN SPEAKER: I have a question to Valerie about the dot… [Inaudible] from France. And I'm making a PhD about domain name evaluations and the use of domain name for a population. I'm thinking about dot UA, and the need to have the [inaudible] system, and the idea of having some copyright agreement and so on.

I remember, the creation and the delegation of country code top level domains has always been a problem for 1985 when it has been invented, three years ago, if I would remember, ICANN launched the program of new gTLD.

In two years, we will have more and more gTLD, I mean, now we are at about 3,000 gTLD. Is it useful, in 2017, to develop a country code top level domain? ccTLD. Is it interested to develop a ccTLD when you know that you can create a domain name with a link, with a topic, and not with the country.

VALERIE FILNOVYCH: I think that the… As I have said, the UDRPs, the policy will be enough for the domain name resolution in Ukraine, but the proposition host master of the administration of public domain dot UA, wasn't, was not approved. So, maybe they should again, provide such a draft project to our government to, for it to be approved.

DEBORAH ESCALERA: Any other questions or comments, Peter?

A bit of coordination issue here.

JACQUELINE EGGENSCHWILER: Jacqueline Eggenschwiler. I had a question for Carolina. Regarding this very interesting triangle that you presented us with. And I was just wondering, it's a very high level question, whether you were thinking of any possible coordination mechanisms that could deal with this Venn diagram of defense and security, the internet on the other side, and exactly government as the third component. Thank you.

CAROLINA MATAMOROS: You're right regarding the high level way of the question, because we're currently anyone is actually dealing with that. I brought it up here to ICANN because I think they have the opportunity to take that space. Because some organizations are worried between like the security of internet [inaudible], or the security of states, but not all in that triple diagram.

So, in here, we have the safety and stability advisory committee that, in theory, takes into account that, but they are only making advisory kind of statements, or way to do it. And it's really difficult in the way to do it, but on my perspective, they can actually do something about it.

Here, the domains and the names are put into use, and it's the way the internet is built, so there are some organizations, such as this one, that can actually do something about it. And I actually wanted to make a comment on what you said regarding the protection of human rights, and it's actually a question for like to ponder about, because we all have different responsibilities as different agencies, and for example, here in ICANN, I did ask what's the main security issue. What are you protecting? And that's not clear. They are protecting the internet. Are they protecting the users? Are they protecting the human rights?

In some cases, those things came in contradiction. So, these entities, especially the security and stability at the [inaudible] committee, needs to clear out what they pretend to protect in order from this to be actually effective. And it's something that needs to start. I think that's about it, but it's still a broad question, it's not closed, and it's a lot of work to do.

UNKNOWN SPEAKER: Sorry, just to make a very quick, or just to highlight again, I think it's important to remember the mission of ICANN, and it's limited scope, that's really only the domain name system, names and numbers. And so, the idea of addressing cyber warfare or cybercrime issues that aren't related to domains, it may not…

And so, DNSSEC maybe, Lauren could shed more light about that. But it's like their different concerns about the security of DNS as a system versus the security that states provide for the protection of their citizens, and anyway, maybe Lauren could go on. But just as a reminder to everyone of like, ICANN domain name system, and not beyond.

CAROLINA MATAMOROS: It's clear. It's just, according to the mission, it's to keep an open and interconnected internet. So, the security advisory team objective, should also be related to that. I know it's not their focus, and I know it's not more technical, but it's a space that is missing right now, as I said at the beginning. Like nobody is really paying attention to that point, and that's actually putting the internet under a threat, as we like it.

So, it's just an open question.

UNKNOWN SPEAKER: You have to take also into account that a lot of organizations, they are dealing with internet governance and dealing with securities. So it's not just ICANN responsibility to focus on this. So, when we talk about the protection, we have to take into account like all actually stakeholders. And especially the institution that they have this role in protecting the rights.

PETER CHON: This is Peter Chon. I have a question for Chawana. I really enjoyed your presentation, though I don't think I necessarily agree with the idea presented. You raise a lot of questions and it makes me think it's interesting. So, I would like to pose maybe another question that you could consider, which is we present each individual in the world with a personal IP address, something to think about is sort of the international context, and that of global interoperability, right?

So, I could imagine this would facilitate the tracking of any individual by any government or organization around the world. And so, this could lead to a race to the bottom where a given nation may want to protect its citizens, or may feel that it's mandate is to protect its citizens, and thereby withdraw itself from ICANN and the global internet, and lead to a fracturing of the internet.

So, that's kind of a doom and gloom scenario, perhaps to think through. Thanks.

DEBORAH ESCALERA: Just to note, we will have to wrap-up in one minute because another session will start.

CHAWANA HUANGSUNTOMACHAI: Okay. Thank you Peter for remarks. It's, yeah, it's interesting remark, actually. If we're going to do this in the idea like, if it's going to happen, I think we need to work some more, like okay, then who owned the database? Like, maybe state, maybe certain states may not have database on IP address like for identification, like for some other country, citizens, because it must work that way, in my opinion, further discussions should be made. Thank you.

DEBORAH ESCALERA: Okay, everybody. Thank you for your presentations today. You all did a fabulous job. [Applause] Give yourselves a hand.

[END OF TRANSCRIPTION]