MARRAKECH – NextGen Presentations Part 2
Wednesday, June 26, 2019 – 09:30 to 11:45 WET
ICANN65 | Marrakech, Morocco

CYNTHIA JADE MAKORY: …that's a challenge to you, and it's also a challenge to [trade] because companies are also affected. Because if they lose their trade secrets, that's also very detrimental to the companies themselves. According to the United Kingdom's Government Code and Cypher School it estimates that approximately 34 countries have serious, well-funded cyber espionage teams.

So at the end of it all, we have different countries in the world, and it's a fact of life that the world is set up in a very hegemonic dynamic because we have stronger countries, countries which have capabilities that other countries do not have. So what should other countries do?

This is my particular recommendation as to what can be done and what different countries can actually move toward so that we actually have this whole situation where we are aware of what's already happening and that we're not just sitting about hoping that maybe the international order would fix this. That every single person and every single country is responsible for ensuring that we're actually moving toward this secure and actually making our Internet safe. So building capacity.

This enables a country to appreciate and understand where threats come from and respond appropriately. So building capacity is very important because if you're building capacity, you're also trying to come up with structures that also block off some of these attacks that might actually affect your critical infrastructures of a country. Little by little, most of our systems are actually moving into this particular platform which is called cyber, which is all about interconnectedness which is not even limited to the Internet.

But because of connectedness this means that if someone can actually hack the system, it leaves the whole particular infrastructure very vulnerable. Research is something that needs to be emphasized. I don't think it's emphasized enough. This enables a country to [zone in on] the motive and underscore the reason behind the acts which are being carried out. This also enables one to appreciate the users themselves and now also have them at the center so that it's them we're protecting. Because the state has an obligation to its people and coming up with defensive tools. Because it's not just about identifying the problem. It's also about trying to come up with tools that actually provide the country with the capability of protecting itself from these particular threats.

Then there's also the need to evolve. And this requires keeping up with the times and adapting to techniques, thus anticipating

threats. So perhaps a question I'll pose to all of you: how is your country addressing cyber espionage and what regulations nationally, regionally, and internationally can be put in place in response to cyber espionage?

At this particular point I'd like to perhaps share this quote I came across. I feel like it's very important. "Cyber power is now a fundamental fact of global life." So it's here. Given the fact that it's already here, what are different countries doing or how are different countries actually taking this into consideration when they are coming up with different policies. Are your citizens at the center of this whole concept we're talking about in terms of cyber espionage and their protection?

That's my presentation.

DEBORAH ESCALERA: Thank you very much, Jade. Are there any questions? Please?

UNIDENTIFIED MALE: Hi. This is [inaudible]. What I tell my graduate students is that the next world war will not be fought with soldiers [inaudible] guns. It will be fought in cyberspace. Just a few days ago, the president of the United States ordered a cyberattack on Iran. So what is the solution in terms of there are countries that are cyber powers, superpowers and there are countries that are not. So what is

stopping one from attacking the other? What are your recommendations?

CYNTHIA JADE MAKORY: Maybe it's a fortunate or an unfortunate thing that I'm a law student. So I'm very skeptical about the international legal order because at the end of it all, the world is set out in a hegemonic sense where we have stronger countries and we have smaller countries. For there to actually be consensus, different countries need to what's on the table. Even if we're talking about a treaty and trying to draft something that would actually lead to or result in the protection of the interests of different countries.

I think we need to form perhaps a committee because I know before any treaty actually comes into force, we usually have committees which actually carry out research so that we find out exactly how we can make even the small countries benefit from being part of this treaty despite the fact that they are not superpowers.

This also involves having a stronger emphasis on national states having defensive mechanism so that they can also counter some of these attacks. Because for Kenya, for example, there is research that was done that we were actually under attack for seven years and we didn't even know we were under attack. So

we didn't even have the capabilities of detecting some of these challenges we are facing.

That's why I think one of my recommendations is evolution. People need to start looking at the problems that the world is facing and trying to also bring it now to the national level where we actually start seeing these problems as something that different nations need to start focusing on?

Yes?

UNIDENTIFIED MALE: Just one more supplemental question, in terms of an international treaty, do you think we should go to the United Nations to come up with something or we need a separate body?

CYNTHIA JADE MAKORY: Ideally, if you've go to the United Nations, what you'd have are mostly resolutions. And a treaty is something that usually exists outside the UN order because different countries actually decide to sign then opt to ratify. But if you go to the UN, you can get a resolution. But if we do not have a treaty which is independent of the UN where different countries actually commit to taking up these obligations – because when you ratify a treaty, you are obligated – it will not be effective. We need something that actually makes people responsible for the obligations they take

up. So I would actually opt to have something that is outside the United Nations, yes.

DEBORAH ESCALERA: Thank you. Oh, one more question.

UNIDENTIFIED MALE: Okay, just a simple question. Maybe not only to her; maybe all of us. How do you think we can improve protection of critical infrastructure from cyberattacks.

CYNTHIA JADE MAKORY: I'll give the example of Kenya because that's my country. Recently, I don't know whether it was late last year, our government decided to set aside some money that's usually set aside by the communications authority to actually look into research when it comes to now cybersecurity. And that's very important because if different countries make it part of their priority, it also focuses on that and it also enables them to actually work toward creating something that's safe for their citizens. And it has to start at the national level.

Thank you.

DEBORAH ESCALERA: Thank you very much, Jade. Our next presenter is Adisa. Over to you.

ADISA BOLUTIFE: Hello, everyone. My name is Adisa Bolutife. I am going to be speaking about the authentication and adaptive security for the domain name system.

Just a brief outline of the things I'm going to be discussing would be looking at how the DNS actually works. And then some vulnerabilities of the initial domain name system. Also, trying to understand the DNSSEC, which is the domain name security that we currently have. And also, the current state of DNSSEC validation around the world, and especially in Africa. And then to the future, talking about the future recommendations and how we can move forward.

The domain name system, how does it really work? The DNS primarily translates hostnames to IP addresses or IP addresses to hostnames. Basically, it works like when you put a web address into your browser, the DNS basically helps connecting your web address to the IP address then getting you the information you need.

The DNS does this using the resolver. On your browser, there exists a resolver that's transmitted to what we call a recursive

resolver which exists in the DNS system. And the recursive resolver basically goes through all the servers to find out the one that actually consists of the information you're looking for. So basically it goes through a hierarchy. It starts from the root servers and to the other servers.

Basically, this works in a way such that when the resolvers get information once, it stores it in a cache so that next time it has to move it basically accesses the web address you're trying to get through the cache so that you don't have to go through the old resolving process anymore. That's a brief description of what the domain name system really represents.

Now what are the vulnerabilities of the DNS? First of all, to describe the basic domain name system that was developed in the 1980s, the Internet was much smaller then and security was not really a primary consideration in its design. So the open resolvers really allows clients that are not part of the administrative domain to use the server for performing recursive name resolution. Basically, anyone can access the DNS and can run queries on it.

The effect of this basically is that the system is vulnerable to attacks, mostly attacks like denial of service and then distributed denial of service. We'll talk more about that. As a result, when the recursive resolver sends a query to the authoritative name server,

the resolver has no way to verify the authenticity of the response. This is actually one of the major fails.

I'm going to describe a couple of vulnerabilities in the DNS system. I think the first one is cache poisoning attacks which occur when an attacker sends falsified and usually spoofed information to information to a DNS resolver. Usually, I know a couple of us might be familiar with a situation where you go probably to a bank website and then you discover that you're actually going to the wrong one. Basically because these attackers have access to a spoofed data of what you should be receiving on a normal query and then they sent it to the domain name system so that when you query it saves in your cache. From there, the next time you query it doesn't go to the root serer to look for it basically because it has been poisoned with the wrong website. So usually attackers use this to get information on your bank details, and then they go around accessing your bank accounts through this.

I think the other one is amplification and reflection attacks. This basically involves sending DNS messages to multiple open resolvers using forged source IP addresses. This can be used to attack companies, basically sending messages that the companies didn't send using their IP addresses. It just takes some editing. This can actually cause a breakdown in the serer and in their technology, and then [businesses can] move on with this.

The third one is the resource utilization attack which can also happen whereby the attacker would consume all available resources to negatively impact the operation of the open resolver of the domain name system.

It's important that we actually provide some level of security for the open resolver, which brings us to the development of the domain name security system, DNSSEC. DNSSEC basically supplements the hierarchical nature of the DNS with what we call the cryptographic characters. With this, we are able to ensure that the DNS can ensure authenticity of whatever query is being run on the system which makes it more secure.

It uses this through cryptographic signatures, and they are published in a more secure format such that not anyone can just easily access it. And then, of course, we know part of the effect of this is that it uses more bytes in memory. For the normal DNS we have 512 bytes, but for the DNSSEC it is up to 4,096 bytes.

For the adoption rates and validation rates around the world it is considered to be 20%. But for Africa, the DNSSEC validation which is the use peaked at 22% of users in mid-2016. Now we have seen that it has declined to 12% at2019. But in 2019 it has shifted back to 18% adoption. Why is this data fluctuating? Why are people not interested in using this system that seems to actually provide more security for the DNS system?

Some people believe that one of the arguments for the people who do not want to use the DNSSEC is the fact that it increases the size and inefficiencies of the system, considering that at times some legitimate queries might be blocked out. And validation also takes additional time. And also the costs of this might actually outweigh the potential benefits to businesses making them not adopt this security measure.

Then I think for many who use the DNSSEC, which is highly recommended, these are people who consider Internet security a priority. And these are people who consider trust from consumer a priority as well. Also, one interesting thing to consider is the fact that the DNSSEC is a work n progress. Even though not totally perfect, issues are being worked on by engineers every day and we believe that this might actually be something that will ensure more security for the Internet space.

So for future recommendations, we might have to actually ask ourselves: how important is the security of our domain name space compared to the costs that is to afford the companies money in this system? To people like you and I who are potential risk bearers for this situation, we should always think of supporting a more secure and a more trusted domain name system.

My recommendation, which I believe we all should think about, is the fact that for securing the DNS there's really no Plan B beyond the DNSSEC. We have to ensure the DNS security is being supported, is being proposed even by end users as well. And we should know that operational experience would guide further refinement of the DNS security tools and techniques in the coming years.

Thank you very much.

DEBORAH ESCALERA: Thank you very much, Adisa. Are there questions?

ADISA BOLUTIFE: Please?

UNIDENTIFIED FEMALE: Actually, I just want to clarify a little. I just have a doubt. This DNSSEC deployment, can it be done at a personal home level or does it have to be at the ISP level.

ADISA BOLUTIFE: It actually has to be at the ISP level which is why I mentioned that some of them on a business side it's not economical for them and it's really not their problem. But looking at end users like us, we might actually get attacked in the cache poisoning and some of

the things that go on. So it's important that we hold them accountable and ensure that this is actually being implemented.

UNIDENTIFIED FEMALE: Just a follow-up. Also, the DNSSEC is deployed in the authoritative servers that you mentioned. So it does digital signing as you mentioned. So I'm just curious. What's the difference between a digital signature that you have with the URL? You see a lock there, right? When you open your browser and you type a domain. So that's a digital signature, and this is digital signing that your talking about in the authoritative servers. So I just want to know what's the difference and what defense does it provide in terms of security?

ADISA BOLUTIFE: Okay, so the DNS system actually works in two ways. There's a link from the end user while putting in your domain name to the resolver. Now there's a stub resolver. From the stub resolver, it goes to the recursive resolver. So at the recursive resolver level there's a bridge. At the stub resolver level there's another bridge. So within those two spaces, the DNSSEC encrypts the data moving out from those two ends which are the two ends that really could be attacked. So that's what makes it really unique.

Okay, you can.

UNIDENTIFIED FEMALE: There's two signatures. What's the role in the URL?

ADISA BOLUTIFE: Yeah, digital signature, it's actually what the DNSSEC really is, cryptographic keys. So I think when you get the HTTPS it shows that it is a more secure way of accessing the Internet.

UNIDENTIFIED FEMALE: Yeah, I think I'll just make a correction what I was saying. I'm meant there's two certificates. The URL when you see a domain on a website, for example, Facebook.com. Then you see a lock next to it. So what protection does that provide? I'm just curious. I just have a doubt.

ADISA BOLUTIFE: It means that your query is being encrypted, which is exactly what the DNSSEC does. Is that okay?

UNIDENTIFIED FEMALE: Thank you.

UNIDENTIFIED MALE: Just a quick question. So when you are talking about DNSSEC, does it mean an end user has a role to play in ensuring that they

are able to identify how secure a website is to avoid having their data being used by [inaudible]?

ADISA BOLUTIFE: Yes, exactly. That's actually part of the point I'm making. Because most times when a certain technology or a certain improvement doesn't affect the businesses directly, they tend not to take action. We see that in Africa. Some of the cases have been that the DNSSEC has been employed, and then they removed them. Why? Basically, because some of the queries that have been done on it probably slows down the system. It costs more to get the administrative know-how. So they probably have to employ someone who is an expert in handling that. And they're like, okay, the costs, the benefits, so they just bring it down.

So what I'm saying basically is as end users we don't install that, but we can hold them accountable and ensure that the DNS is secure.

Go on, please.

UNIDENTIFIED MALE: Just to make a quick comment answering your question earlier about the browser. When you see that lock, that's basically what it means is that you're using HTTPS. When you're using HTTPS, which is secure, it means that the communication between your

browser and the website is encrypted. Not only that, but also the browser validates the encryption. It says this is a valid website and that the certificate checks with Verisign or whoever. That it's a valid certificate. That's what it means.

Whereas, with DNSSEC what it's doing is on a different level. It's on a lower level, and it just says that this is the real name. So it can prevent some of the attacks like DNS poisoning.

UNIDENTIFIED FEMALE: Thank you.

UNIDENTIFIED MALE: Would you be able to give an example like estimate of costs and the benefits?

ADISA BOLUTIFE: Okay, for that I'll have to get some statistics. But like I mentioned in the slides, I think I talked about the amount of memory that it consumes. So comparing 512 bytes to 4,096 bytes that's a whole difference. Imagine the number of data they have to store for that.

Also, considering the fact that they get to employ someone who is an expert in handling these things, it shows that the cost has actually been increased.

I think one of the downsides as well is the fact that it's not fully refined. The DNSSEC is not fully efficient, and sometimes even legitimate websites sometimes get blocked. And then these businesses don't want to have a downside.

But I believe a lot is being done on the current security for the DNS to get to a point where we'll all be comfortable using it.

ANDY BATES: I don't know if it's any help. I'm Andy Bates from the Global Cyber Alliance. We're and international not-for-profit that fights cybercrime. We built a thing called Quad9 which is a DNS resolver that supports DNSSEC and many of the other technologies that we've just spoken about.

We do have an ROI paper which I'm happy to share that shows he benefits of not only DNS filtering but DNSSEC. I would agree with my learned colleague here, but I would say that between the Quad1 service, Quad8 for Google, and Quad9 from ourselves, all of those things support DNS at no cost. But you're right to say that there would be some minor impact on the computer itself. I hope that was useful.

ADISA BOLUTIFE: Thank you.

UNIDENTIFIED FEMALE: Yesterday I attended the governmental advisory committee. They had this discussion on the policy aspects of DNS over HTTPS and TLS. With respect to now DNSSEC, when you're carrying out an appraisal, what's the benefit of having the DNSSEC or is the DoH just sufficient enough? Because I feel like it still gives this whole – it just says that this particular domain name is authentic. So if you're carrying out an appraisal, what would…?

ADISA BOLUTIFE: I think the DNSSEC is actually one of the security measures you can take, which is one of the major ones. I think there are other technical security measures that you can also apply. But I think the major thing that the [DNS] does is authentication and also encryption, ensuring that no one gets in. Those are the two things it does, and those are pretty basic.

If you need more security, I believe there are many other technologies out there that you can add to the current system and [make your way]. I believe that's what he actually mentioned about Quad9.

DEBORAH ESCALERA: Thank you very much, Adisa. Next up we have Yash. Over to you.

YASHVI PAUPIAH: Hello, everyone. Thank you for coming. I'm Yashvi Paupiah, student in computer science at the University of Mauritius and an associate in cybersecurity. I'm here with the NextGen program.

I'm from a tiny island called Mauritius. Mauritius is located to the right of Madagascar near Réunion Island. It's mostly known for its sandy beaches, for being a tourist haven and the dodo. It's only 2,040 kilometers square.

Mauritius doesn't have any major Internet issues. Here are some promising statistics. According to [ITU] 68.7% of households in 2018 have Internet access. No Internet censorship anywhere. National coverage of fiber optic and four ISPs competing to lower the prices. A new undersea cable named IOX will soon join the country providing more bandwidth. In my opinion, Mauritius is [in the line of] it becoming one of the leading countries in terms of Internet-related activities. We just need to bring the price of Internet a little bit down though. That's all.

This presentation though is not about the Internet in Mauritius. It's about a team who is trying to make a change in the country. Who are we? We are hackers.mu, a nonprofit organization which I'm a member of. Our role is to empower the youth and the general population with the tools required for them to succeed and create a better country.

We've started small doing supplementary [free lessons], such as how to use GitHub, competitions, hackathons, such as the AIS, Google coding, and IETF. We've mentored students from high school to do that. We've also done some source code [batching], DNS analysis. All of these at the university level and also at the national level.

Our current project right now is building a framework to ease development of software and allow better coding practice. [This are some features of our framework.] It will be built upon zend framework 3. It will be released with an open source license to allow contribution from anyone, from anywhere in the world. Model view controllers will be simplified using patterns. It will be an entity-based framework. The create, read, update, delete operation will be much easier.

With a few simple [configurations], you'll have end-to-end encryption for [inaudible] application or mobile application [inaudible] with it. And automatic security upgrade. Like if a liability is discovered, the changes will be replicated everywhere. No need to do anything around that. The main goal for that framework is to build projects to ease the life of people and empower them. All of these are community projects.

Here are the projects we are currently working on using that framework on a beta phase. We have mobile and web application

providing food recommendations through machine learning to people with diabetes, cholesterol. Because in Mauritius in 2015 the standard prevalence of diabetes was 22.8%.

The second service will allow easy blood transfusion for any people by region as well as helping medical researchers to conduct blood-related research.

The third one is simple food wastage prevention service linking people in need of food and those with a surplus of food. Just to mention this is all a community project, and everything is free there.

This is the team responsible for trying that change. We have our founder Pirabarlen Cheenaramen who works with the Fintech company in Denmark. A senior software engineer Yasir Auleear. Myself. We have Neeraj Joypaul, student at the British Computer Society. And Rajeesen Poongavanan, Student in the Electronics Engineering. Please visit us at hackers.mu. You'll find more details there.

Thank you.

DEBORAH ESCALERA: Thank you very much, Yashvi. Are there any questions?

UNIDENTIFIED MALE: I guess I'll ask one if I can. Is there any support you need from the wider community?

YASHVI PAUPIAH: Sure. We are in need of support, but at the national level we try to get the companies involved with us, like supporting us. Because those projects are all community projects. If the company can provide anything, we are all in.

Any other questions? Thank you.

DEBORAH ESCALERA: Thank you very much. Our next presenter is Ajani.

OLUWASEUN AJANI: Hi, everyone. My name is Oluwaseun Ajani, master student in urban and regional planning from the Nigerian premier university, University of Ibadan, Nigeria.

The topic before me this morning is smart city solutions and intellectual property. I'm going to follow this outline for this presentation. The aim and objective is to examine the concept of smart cities and identify smart city solutions and [inaudible] between smart cities and intellectual property.

[inaudible] smart city is diverse, complex, and [inaudible] and is a concept that integrates information and communication

technology and various physical devices that are connected to the Internet of Things network to optimize the efficiency of city operations and services. Smart city solutions create livable, sustainable, and prosperous cities globally.

Smart city solutions also achieve a sustainable development. It increases the quality of life of citizens and improves the efficiency of existing and new infrastructure.

Smart city solutions are used in various ways, such as the monitoring of traffic situation in the city. It's used to improve the air quality and to reduce traffic congestion in the city. It's also used in energy and grid management whereby we try to maximize the use of energy in the city. It also provides insights into the usage of water in the city.

Using sensors is also applicable in smart city solutions in terms of real time data on waste management, prevention of crime, and crime-mapping platforms such as [inaudible] and smart lights. Smart city solutions are also used in emergency management institutions.

Now to conceptualize intellectual property, World Intellectual Property Organization (WIPO) defines intellectual property as a condition of mind, inventions, and literary and artistic works which involves symbols, names, images that are used in

commerce. It can be categorized into two different aspects which includes industrial property and copyrights.

Industrial property includes patents for inventions, trademarks, industrial designs, and geographical indications. In terms of geographical indications, we have [inaudible] on the .AMAZON that they want the domain name to be used for their business but the Amazon countries are not agreeing with them. It's part of their industrial property, so they have to advocate for that.

Intellectual property rights are the exclusive rights [inaudible] of a creator to his ideas and tangible assets. We have different types of intellectual property. Copyrights are used to protect literary, dramatic, and artistic creations of authors, such as poems and novels.

Patents are used for protection of innovative solutions to problems. The solutions must be characterized with novelty, inventions, discoveries, and mathematical methods.

We also have trademarks which provide protection and exclusive rights to the owner. They are used to identify a particular good or product. This can also be used to identify a company. We have [inaudible] tech companies like Google, Microsoft. They have their various trademarks.

Another form of intellect property is trade secrets. Trade secrets are used for business in order for them to have an economic edge over other businesses.

Now [next] we examine the nexus between intellectual property and smart city solutions. There is a general issue over data ownership because smart city solutions produce an [urban] big data which can be used to generate predictions, visualizations, and can be used in [urban] big data analysis.

Still the question here before us is who is going to govern the data in this smart city? Who has the rights to own the data and who controls the data? Because these are [inaudible] the smart cities are the taxpayers. They should have the rights to their data and not the businesses who use it for their own profit. They should have the [consent] to give to the business owners so that they can use it anytime they want.

Another issue that is [germane] is privacy. As I said earlier, smart city solutions are connected to Internet of Things. The issue with Internet of Things is privacy and security. If we are going to maximize the [inaudible] of smart cities, researchers must focus on how to protect the privacy and security of these solutions for us to have sustainable growth and development of these solutions.

How does ICANN relate to intellectual property? ICANN has an Intellectual Property Constituency which represents the views and interests of the intellectual property community [network] worldwide with particular emphasis on trademark, security, related intellectual property rights and their effect and interaction with domain name systems.

As I said earlier, on the issue of .AMAZON, if a city wants to use a particular domain name for their smart city solution, they have the right to this because it is their intellectual property. It's a geographic indicator. So ICANN should try to make sure that cities' rights are protected when domain names are being registered.

Conclusion and recommendation. Smart cities provide myriad of opportunities for innovation in sustainable cities. Intellectual property protection is germane for the growth and expansion of these solutions. If we are going to have a good [inaudible] of smart city solutions [and this allows interconnectivity], we must ensure that we protect the intellectual property of the creators of these smart city solutions.

It is also important for us to have a data governance strategy of the [urban] big data that smart city solutions are providing so that users' privacy will be adequately protected. We can use patents, trademarks, copyrights, and trade secrets which will promote

innovations and will give the creator of those smart city solutions explicit rights to their inventions.

Thank you very much for listening.

DEBORAH ESCALERA: Thank you very much, Ajani. Are there any questions?

IHITA GANGAVARAPU: Thank you, Ajani, for your presentation. I am Ihita, NextGen Ambassador. I just wanted to know if there are any recommendations or policies or proposals within your country that have been put forward by either the government or any organization in the private sector. For when it comes to answering the questions that you mentioned, who should have the ownership of the data? Who has the ownership and who must have the ownership, and what is the process? And also, are there any recommendations or policies [inaudible] within your country? [Or] talk about it? Thank you.

OLUWASEUN AJANI: [So far in Africa generally] there is no real policy on who governs the data for smart city solutions because we are just [inaudible] smart cities. Smart city solutions are just beginning to penetrate into the IoT market in [sub-Saharan] Africa. So the issues of

protection of the data of the users is not really a concern for now. But there's a digital rights and freedom [bill] that has been submitted to the president of Nigeria for [assent], but it has not been approved. Thank you.

UNIDENTIFIED MALE: This is a comment and maybe sort of a recommendation. What is happening is that everyone is collecting data and they are keeping it buried like a treasure, which is of no use to anyone. Whatever data is collected should be made available to the academic community [inaudible] and whoever can use it for data mining or whatever purposes and see what intelligence and knowledge we can get from the data. So I think that should be one of the recommendations.

UNIDENTIFIED MALE: So actually a question and something to add to that. First of all, we've built a big IoT honeypot. As you know a honeypot pretends to be IoT devices. So we're sharing the data with some universities around the world, but we'd be happy to share more.

My question is to load IoT devices into a honeypot, we need to take that software. And your issue is very much about intellectual property. So you giving software to someone you never met before is a big IPR issue. So I guess, do you have any thoughts

around – well, the benefits of a honeypot are to protect IoT devices in the field. It's a good thing. The challenge is it challenges all of the IPR things that you've discussed, and it's not normal for an inventor to release their code to another third party. So I don't know if you've got any comments around that, please.

OLUWASEUN AJANI: Yeah. Intellectual property, we promote competition between businesses. That is why it is important. A creator or an inventor should try to protect that intellectual property so that others will be innovative enough to develop their own smart city solutions. That will bring about proper sustainable development.

GLENN MCKNIGHT: Hi. Glenn McKnight, I'm a board member with ISOC and a volunteer for NextGen. I'm involved with something called IEEE Smart Villages which has a project in Nigeria. Have you looked at taking this concept of smart cities and break it down into smart villages concept?

OLUWASEUN AJANI: No.

GLENN MCKNIGHT: Okay, I'll give you a contact for Smart Villages.

OLUWASEUN AJANI: Thank you.

DEBORAH ESCALERA: Any other questions? Okay, with that, we're over to our last presenter, Sulaimon. One second, and I'll share your presentation.

MORIAM SULAIMON: Hi, everyone. My name is Moriam Sulaimon, a third-year student of University of Ilorin, Nigeria. I will be presenting the topic Internet: A Tool for Empowering African Women.

Introduction: Access to the Internet in Africa is limited leading to a low penetration rate when compared to the rest of the world. Only a quarter of Africans have access to fast and reliable Internet though the region is seeing the strongest growth. According to the ITU, the growth of Internet access in Africa is [10.325%] from year 2000 to year 2019.

The low Internet penetration in Africa is also because women are more in number than the male counterparts. According to the UN, the [females are] 54%. And most of them are not empowered to use the Internet [inaudible] support the activities [inaudible] the Internet. They are mostly seen as objects that are meant to bear

children and look after them without having a voice. However, the Internet is meant to be a voice for all.

We have barriers to African women's Internet access and use. African women's access to Internet is increasing, but a number of difficult and persistent barriers still remain. The following is a highlight of some.

The lack of awareness about Internet and its use. Most of the women in Africa do not even know what the Internet is about. They don't know how it works, let alone make use of it. They don't have sufficient information about Internet.

And the [language] [inaudible] social and cultural barriers as well [inaudible]. Like most people, like males in Africa, they are some [inaudible] that are really interested in making use of the Internet. They want to know what the Internet is about. But when they make an inquiry about the Internet, they are being told there is no point in making use of the Internet because they believe they are just meant to take care of their kids, take care of the home, and take of their family.

Then the design and usability is also a barrier for African women in Internet access and use. Let's talk about websites here. Website design can be a factor that [inaudible] participation. Most of Africa – we have different countries in Africa, and each country in Africa has their own native language they use. Like for Nigeria, we

have the Hausa, we have Igbo, we have Yoruba, and a couple of others. So we have to have a standard language or [inaudible] for Internet that should actually support different languages so that when women are even interested in making use of it, they're not having issues with the designs. They're not having issues with [inaudible] and having issues in how websites are being designed.

Then the affordability issues. Most African women, a lot of them are [merely] full-time housewives. Most of them don't have a work they do. They are sitting at home taking care of homes, and most of the [things] they need are being provided by their fiancés, their husbands, [inaudible] families. So they don't have the money. They don't have the finances to be able to even get [closer] to using the Internet and accessing it.

Then the cyberbullying, women are mostly being affected by this on the Internet. They are communications [inaudible] messages [inaudible] and threatening them even when they really want to make use of the Internet.

Then the lower level of literacy and education. According to the UN report, two-third of the world's 876 million [inaudible] are women who mostly reside in developing countries, which Africa is a developing country. So they are less likely to know the international language that dominates the web. They lack computer skills. Most of them don't have the training. They don't

have a formal education. They don't understand other languages apart from their own native language.

Then another factor or barrier that affects is their [less time]. Women in Africa have a higher burden of domestic work and responsibility. They have less time. They don't really have much time, and even most of [inaudible] have interest in making use of the Internet don't even have the time to actually make use to it, to actually access it.

Then we will talk about the geographical location. Women in Africa tend to [inaudible] rural areas more than men. In these rural areas, infrastructure is less dependable. For them, traveling to the [inaudible] is difficult due to the cost, the time, and some cultural reasons.

Then the climate of science and engineering departments at colleges and universities. Most of the universities where they have these science departments, engineering departments, [inaudible] departments have been dominated by males. When the few of the females that have interest in actually going to this department, they are being intimidated. Because most people there – when you see like example in my school computer science department, we have quite a lot of females actually. But most times even [inaudible] when you come to class and see that the number of females in the class are much more than that of the

males, they are always like, “Wow. What are the females looking for in computer science? You guys [don’t have time]. If you plan going into programming, what time do you have? You have kids to take care of. You have families to look after.” And [inaudible] they are not being encouraged. We are being discouraged in actually having a say, in actually having a voice in the Internet.

Then I went on to giving some points in overcoming these barriers. For African women access and use of the Internet to be addressed, certain measures must be put in place. Now some of these measures are we have the formal training and education. I’ll talk about the older women. Most of them don’t know how to use these devices, this [inaudible] equipment. But there can be formal training put in place for them where you’re [inaudible] like a tech outreach like bring [inaudible] together and giving them just a little training. A little training can actually made these older women be able to make use of this [inaudible] equipment.

I’m going to talk about education for the less [inaudible] we have inclusion of Internet education in school curriculum whereby from the start you’ve already included this [inaudible] education, and from the start they are already having interest in it because they’ve started learning it from when they were young.

Then you have to encourage local adoption and use. [inaudible] that produce local content and applications, attracting local

users and serving local needs. That is most of these women [live in rural areas] [inaudible] we consider local. So now if we are making sure that the Internet, if we are encouraging the local adoption, we attract local users and we are serving local needs, they would also be interested because they would consider this local content is beneficial to them and they will actually want to [inaudible] this and maybe make use of [inaudible] and make use of the Internet because it will actually [inaudible].

Then the ongoing support and advice in using the Internet. We should keep on advising, keep on supporting, and keep on giving them [inaudible], keep on empowering them in [inaudible]. Then we should [inaudible] the women, we should [inaudible] giving them ongoing support and advice.

I believe this [inaudible] have attitudinal change toward the use of the Internet. Because even if we're giving them formal training, giving them education, ongoing support and advice, they still need to have this attitudinal change toward the use of the Internet. So whenever [inaudible] change where they believe, yes, this thing is actually good for me, this thing is useful for me, I can make use of it, definitely we will actually make progress.

Then exposure to successful female role models in IT field. When we expose them to successful females in the IT field, they will also want to participate. Because when they see that their fellow

women are in this space and they are actually making progress, they will actually have it [inaudible] I can also make this progress. I can also be like this person. I can also be a role model.

Then promoting increased employment in the IT sector for women. Most of the IT [firms] we have don't really have females as their employees because we don't encourage it in Africans. We believe that men can actually work better than women when it comes to the IT field, but that's not true. When we increase the employment of women in this sector, I believe other women will also say that, yes, they're actually employing females in this sector. I can also go into this sector, and I can also be employed in this sector.

Because even some of them they believe that if females are not being much employed in that field, they don't want to even go near it because they believe even if after they go to school, go [inaudible] and graduate, they won't even be [able to find] employment in those fields. But when they see that they are already employing females, we are having increased numbers of females in the field, I believe a lot of women will also want to go into the IT sector.

Then improve design and usability. Like simplifying the design so it can be simple and readily understood. Make sure the language,

we make use of local and native languages. Local languages [inaudible] different countries.

Then the providing coverage and access. Now providing coverage and access, most of these rural areas in Africa are not able to make use of the Internet, unable to access the Internet, probably due to because they are in the rural area and deploying of the Internet is not being done in those areas because they are believed to be rural and they don't make use of it. But if we can expand it to the rural areas, women can actually make use of it without having to travel, without having to leave those rural areas to where [inaudible] centers are. They can use the Internet close to their homes. They don't have to go to a far place. [inaudible] will actually be empowering them to actually make use of the Internet.

Then affordable devices and services. This [inaudible] equipment, making sure that they are not that expensive. [inaudible] females can be able to actually buy them. [inaudible] actually full-time housewives [they don't] have a lot of income, so by making this equipment also cheaper I believe they would also be able to buy and make use of it.

Then we have to promote the understanding of the Internet's value. They need to know the value of making use of the Internet. They need to know that making use of the Internet is going to be

of a greater impact on them rather than having a negative impact on them.

Then the road ahead. Trying to succeed or survive in the future, the advent of the Internet actually changing the global scenario and many unexplored areas are now being explored. It is for the African [women] to utilize the benefits to the maximum possible extent. Like I already talked about the barriers and [the economic] barriers. Okay, we have been able to work on these barriers, but the [inaudible] like the future still depends on if we African women [inaudible] are actually ready to [accept] it. Okay, you've [accepted] that. We've encouraged them in [making use] of it. We've encouraged them in participating.

Now each [home] in Africa, the traditional [homes], the orthodox families, they should allow the women to participate using the Internet from their respective homes without having to leave their homes. They can be able to take care of their kids, take care of their homes and families even without leaving their houses.

There is also an abundance of women entrepreneurs who are capable of making their mark at the global level. Only if they participate. Only if their family encourages. Only if they see other female role models. Only if they are being employed in these IT sectors. With simple training and awareness programs we can actually make a big difference.

Then to my conclusion. Although the Internet offers generic advantages of efficiency and productivity gains; information sharing, storage, and communication; faster knowledge accumulation, dissemination and application in support of the specific purposes for which they are used, there are still some formidable barriers to overcome in increasing African women's access and use of the Internet and ensuring that they participate fully in the Internet ecosystem.

African women must have a growth mindset that intelligence can be developed. They must believe in themselves. They must persist despite obstacles. They should see effort as path to mastery and embrace the challenge of using and supporting the stability and security of the Internet. They must engage with the technology if they want to have a say in shaping the Internet ecosystem. By engaging in and by embracing the challenge of using and supporting the Internet stability and security, we can change it for the benefit of women not only in Africa but around the world. We can actually have more say. Women can have a part, and this will actually encourage an inclusive Internet ecosystem where everybody has a say. Not just the male, not just the female, but both genders have a say in the Internet ecosystem.

Thank you for listening.

DEBORAH ESCALERA: Thank you very much. Are there questions?

IHITA GANGAVARAPU: Thank you for your presentation. I don't have a question, actually. I just have a small suggestion. I'm sure when you go back to your country after the meeting you have plans of organizing events. It can be an awareness program or it can be a skill training workshop. So what I suggest, we organized at IGF India six months back in India, and we organized it in a women's university. So you mentioned there's a problem of orthodox families not letting girls, didn't encourage girls to participate in these activities, right? So what we did is that we went to the women's university. We organized the event over there. And then there was media coverage after that.

So you can start off with girls who are already involved in studying maybe IT or any technical course or policy or law. It doesn't matter. So they're all university students. So when you start off with these students, what happens is you have a team. You have a team that will [work] forward, and then you can go and train them to reach families that might not encourage their girls. So you can go ahead with that. And secondly, media coverage. It really helps, especially in our developing country case. Thank you.

MORIAM SULAIMON: Okay, thank you. I understand what you said.

INNOCENT ADRIKO: Thank you. Okay, I want to take a case scenario of Uganda. In Uganda, we don't really undermine women because they really cover so many positions both in tech space and every other space that you talked of. But my question right now is are women really interested in this tech space? Because in Uganda, even though we have the floor open to them, we really see very few of them in the tech space.

Because like, for example, in my class in IT science we are about 30 and we had only 4 ladies. So my question is, are the ladies really interested in this tech space? And if they are not, how can we bring them onboard? How can we bring to their awareness that they actually need to be part of this?

You've talked about of course there are some other factors. Traditionally of course in Africa we know ladies are supposed to be maybe in the kitchen. But now we've moved out of that era. I think so, yeah? I think we've moved out of that era. So if you [be thinking] of the next [inaudible] like not looking [inaudible] the women supposed to be [inaudible] I think we should be pushing them. Thank you.

CYNTHIA JADE MAKORY: Just maybe a follow up of what Innocent has brought out. Perhaps is this a paper you're writing? It's not a paper you're writing? Because I feel like having Africa be the focus and given how even geographically there's usually that disparity between different people from Africa and even within a country setup. Say, from your capital, from the rural areas there's usually a difference. So I feel like a blanket of African women would not really be the best depiction because different places have different realities.

DEBORAH ESCALERA: We have some questions behind you.

MARCUS OKWU EKE: My name is Marcus Okwu Eke from the BC. Thank you very much for the presentation. I just want to make a suggestion. I think in Africa, the majority of the women are [inaudible]. For me, when you talk about access and use of the Internet for the women, I think we need to also focus on what exactly are they doing with the Internet.

So if I am to make a suggestion, I would like to say that if we have a project or a strategy on how to include the women financially so that they can be able to do business on the Internet. So if there

is a project or a program that can be organized for most of this trade [inaudible] business because this covers a large population of these women. How we can involve them and bring them to understand [inaudible] and how to use the basic tools to do business. I think that should be our focus. Thank you.

UNIDENTIFIED FEMALE: My name is [inaudible]. I'm from Nigeria. I am with the Business Constituency of ICANN. That was a good presentation, but I have been in the tech space for over 20 years. Interestingly, the tech space for women, especially in Nigeria – I can speak for Nigeria; I cannot speak for Africa – is a big challenging. It practically turns you into a man because now you have to act and think like a man. I was privileged to be the only female in my class for five years in the university from matriculation to graduation. So I can understand where she's coming from.

But there are some NGOs that are working presently on the [STEM] project in Nigeria. You have the [inaudible] tech. You have [inaudible] women's center. The primary focus would not be to try to bring them to the complex point of the technology. It will be to take technology to them. You don't bring them in, but you take it to them.

Like you rightly pointed out, most of them are into trading. I know I have supported projects where those women do [inaudible]

trading. Some of them are good with arts and crafts. What you do is to teach them maybe how to promote their businesses on social media, how to encourage them to make sales. It's a gradual process. It's not a one-day thing. It's going to come step by step.

You will meet stumbling blocks along the way in your projects, but do not be discouraged. I remember in 1998 when we took Nigeria to the WITSA, I was the only female again. And presently on the BC, I'm the only African female. So these are things you face, but you have to keep pushing because if you do not do it, it's going to be the same thing in another 50 years that somebody will be coming up with a project like this. So you keep at it, and it will work out.

MORIAM SULAIMON: Thank you very much, [inaudible].

ROGER BAAH: My name is Roger Baah. I'm from Ghana. I'm also part of the BC. I think the presentation is good. I really was following with keen interest because I'm working on a project in Ghana with [inaudible]. We call it e-skills for girls. There's a need that has been known over the years, and we saw that even the curricula that are used in schools are not feminine friendly or are not friendly for women.

So what we are doing now is that we are working with a minister of education where the curriculum is being developed especially within the technical space. We are working with [inaudible] technical and vocational institution to actually redevelop the curriculum to be able to make it even friendly for ladies to join. Because the technical schools you go and there are only men. So this time around we're trying to introduce new courses that are attractive for the women to join.

So this is a very good step, and it goes even beyond your small organization trying to get the women. It's in a broader perspective. The actual curriculum that are used in our institutions need to be looked at. So I think it's a very good step, and we all will follow. Any support you need, we're ready to help. Thank you.

MORIAM SULAIMON: Thank you.

DEBORAH ESCALERA: Any other questions? Since we have a bit more time, are there any remaining questions for earlier presenters? Or for those of you who were here yesterday, any remaining questions or comments on any of the presentations you've seen? Feel free.

UNIDENTIFIED MALE: A question for Adisa. It's just a follow-up of what I was asking a bit earlier. Could you kindly point out the difference between DNS over HTTPS, DNS over TLS, and now DNSSEC?

ADISA BOLUTIFE: Okay, thank you for the question. I think the DNSSEC is quite different form the DNS over HTTPS and the DoT as well. Basically, the DNSSEC works on authentication and ensuring that the domain name is actually authentic and valid. But I think the DoH which is DNS over HTTPS does encryption and on a different level. So for the DoT, the encryption is not done on the user level. Which means the stub resolver is not encrypted. But for the DNS over HTTPS, you get an encryption that goes from the user end down to the recursive resolver which is on the domain name system.

So the DoH is actually considered more secure than the DoT, which based on the current recommendation it's actually [inaudible] as a more secure [inaudible]. And I think that is the same thing Ihita was trying to clarify as well. That's why it's advised now that when you use a website that has HTTPS on it, it's a more secure way of connecting to the Internet.

So I hope I've been able to answer that.

DEBORAH ESCALERA: Thank you. Yes?

ANDY BATES: I can add a little bit more. There are some great slides from yesterday's session. So I completely agree with everything you said. You would be right to say that it's good to have DNSSEC and then implement one of the other two features, either DoH or DoT. So they complement each other. And as our learned colleague said, DNSSEC confirms the DNS entry. What the other two solutions do is prevent what's called a man-in-the-middle attack. I should say person-in-the-middle attack probably. It prevents somebody spying on what goes through.

And as you said, one goes end to end. But there was much debate yesterday about the fact that browsers, so for example the Mozilla browser automatically configures to which resolver it goes to. And there was some emotion in the room that said, well, you then as a user have to do things to override that. So although you're right to say that one is completely end to end which feels great, it has some downsides in terms of which DNS service it takes you to.

But in essence, I think doing DNSSEC and either DoH or DoT, don't get too involved in the debate. Just let's turn them all on and the world becomes a safer place is the big message.

DEBORAH ESCALERA: Thank you. Could you clarify which session yesterday just so they can all go back and watch it if they haven't yet?

ANDY BATES: Yeah. Give me a minute to find it.

DEBORAH ESCALERA: Mel?

MELCHIZEDEK ALIPIO: Hi. I'm Mel, NextGen ambassador. My question is for Ajani Oluwaseun. I'm just curious if you had additional research on African research on smart cities, and were they able to apply for a patent or a copyright on these research projects about smart city solutions?

OLUWASEUN AJANI: Thank you. The presentation is just an [area] paper. So we tried to scope the study in the context of Nigeria.

MELCHIZEDEK ALIPIO: But are you aware of any African university or even in your home country developing some smart city? Maybe not that huge project but a small project involving solutions for smarter city?

OLUWASEUN AJANI: Actually, there are a number of businesses that are developing IoT solutions for smart cities, but I can't really remember their names. So you can see me and I will give you some proper details on them.

MELCHIZEDEK ALIPIO: Okay, or maybe you can….

UNIDENTIFIED MALE: Based on my experience in Nigeria I think one of the major challenges of smart cities really has been the connectivity. So to develop such technology you need a certain speed, a certain level of – because currently in Nigeria we have issues with constant electricity. So to develop something as advanced as that there's always a challenge with the current issues with electricity and also with the broadband.

I think for the current discussion in the U.S. and China they're thinking of 5G which would really be for innovation like a smart city. But in Nigeria, the network is still pretty slow and we are still trying to adopt a couple of other things. And I think for Africa it might actually be the same case for some other countries. But I know South Africa and I don't know probably Kenya they're actually developing things relating to that.

UNIDENTIFIED FEMALE: So maybe something that you can also maybe look at is the [inaudible] local [physical] development plan. It's a Kenyan smart city project. Kenya is trying to come up with a technopolis that will I think be a very great thing to just look at as now you just build on your research, you see what they are doing. Try and compare. I think South Africa had something they were doing. So I think you can just share information.

DEBORAH ESCALERA: We have the name of the session.

ANDY BATES: It was yesterday at 15:15 and it's uniquely called "Policy Aspects of DNS over HTTPS (DoH) and DNS over TLS (DoT) and Related Issues."

DEBORAH ESCALERA: Thank you. So NextGen, please take note and watch this session. All the sessions are posted online after the meeting, so you can go back and watch that if you didn't have the chance to attend yesterday.

Any last questions? We have one behind [inaudible].

UNIDENTIFIED MALE: Thank you. Hello. My name is [inaudible] from Botswana. I want to comment on the presentation by Cynthia. She was talking about cyber. With cyber it's difficult. We can't [inaudible] with people that don't have rules, so we can only try. We can try to assess our critical infrastructure time and again to make them as good as we can. And we can also deploy the [inaudible] to try and fight this war. Thank you.

UNIDENTIFIED MALE: I just need clarity on going back to the sessions that you'd like to watch online. I was trying to check but I think I couldn't find the links. I don't know if you would be able to help with that.

DEBORAH ESCALERA: I can absolutely help. We'll meet after. Just so you know, they're not all posted directly after. It takes them some time to upload them. So be patient, but also feel free to come see me.

Glenn has an announcement.

GLENN MCKNIGHT: Some of you are asking me about the pictures. Some of you are asking me about the videos. The pictures already are up. Does everyone have the link for the Flickr? Everybody has the Flickr link?

DEBORAH ESCALERA: I have e-mailed it out.

GLENN MCKNIGHT: Okay, so no one is going to come and ask me again, right? Okay, number one. Number two, they're all Creative Commons, so they're full version pictures, so feel free to take them. Strongly recommend them. Send them to your mother, your grandmother, to your employer, to your professors. This is a very important thing you've done here. Not everybody is selected for the NextGen, so it's important for you to use social media effectively and tell why you are doing it.

Number two, the videos were asked. I had to run to take another photo, but I think I've gotten all the videos except the first lady. So if I can arrange a meeting, we can do it again. But everyone's video will be uploaded. Some are done. I can't upload until I'm done. So we're finished with the videos, right? Okay, they were great. Thank you for your hard work.

Oh, you have a question for me?

UNIDENTIFIED FEMALE: Yeah. I'm just looking at the video. You have exchanged two videos. My work and [inaudible]'s work, the different. But you put

them as his work is mine, my work is his. And also the spelling of the names.

GLENN MCKNIGHT: Okay, I'll check.

UNIDENTIFIED FEMALE: Cool.

UNIDENTIFIED MALE: One more thing. I think you mentioned a certain research your organization was working on. Also, I would be able to get that from you maybe.

ANDY BATES: Yeah, absolutely. Global Cyber Alliance is an international NGO that fights cybercrime. GlobalCyberAlliance.org, all of our material is there. And I'm abates@globalcyberalliance.org uniquely. So if absolutely wants any help with any of the subjects we spoke about, that's why I'm here.

UNIDENTIFIED MALE: Thank you.

DEBORAH ESCALERA: Any last questions? With that, we will close this session a bit early, but let's give one more round of applause for this excellent group of NextGen. Thank you all for your hard work. And as Glenn said, do be sure to share what you've done here back home. We'll speak about this further at lunch, but just really be proud of what you've done and be sure to explain to others at your home university what you're working on. Thank you.

GLENN MCKNIGHT: As a board member with ISOC, we've just revamped our fellowship program. So please look into ISOC. Look at it because we've changed it so it's really focused on people in their mid-career. So having this as part of your resume is not a bad idea.

[END OF TRANSCRIPTION]