MONTREAL – NextGen Presentation Session
Tuesday, November 5, 2019 – 13:30 to 15:00 EDT
ICANN66 | Montréal, Canada

DEBORAH ESCALERA: Okay, it's 13:30, so we're going to start right on time. I'd like to thank you all for being here today. My name is Deborah Escalera. Welcome to the ICANN66 NextGen Presentations. We're going to start right on time. First of all, I'd like to welcome and thank my NextGen Ambassadors for joining me and supporting me during ICANN66. João Pedro Martins from ICANN63, Jaewon Son from ICANN64, and Stefan Filipovic from ICANN63, thank you so much for being here and for your support, and for returning as my support at ICANN66.

We'll go ahead and start with our first presenter, who is Abdeali Saherwala. Abdeali, please begin.

ABDEALI SAHERWALA: Good afternoon ladies and gentlemen. My name is Abdeali Saherwala, and I'm a fourth-year undergraduate student in the faculty of Environmental Studies at York University. Despite my unique background, I'm here to discuss a critical issue plaguing our modern society, which is the rise of post-truth society through social media and its political implications.

Before I begin, I would like to read a small land acknowledgement, which is that the Kanien'kehá:ka Nation is recognized as the custodians of the lands and the waters on which we gather today. We

respect the continued connections with the past, present and future and our ongoing relationships with Indigenous and other peoples within the Montreal community.

In the midst of the 21st Century, social media has truly revolutionized the way we communicate, connect and share our lives with people from around the world. In seconds, through social media, I'm able to know the shenanigans and accomplishments of my friends and family. In seconds, I'm able to know the seismic and small activities occurring around the world, such as Greece's economic meltdown, and small events, such as the Adani's Coal Mine approval in Australia.

That is the power of social media; it shapes our thoughts, our emotions, our identities in real time. It shapes our opinions and views from the world from very little information. It can change completely our being or cause us to divide impulsively without weighing all of the facts or figures. It can make a lonely teenager in the United States, Canada, or Europe to seek comfort from groups who practice terrorism, white nationalism, Antisemitism, or Islamophobia.

It can create doubts within our mind for science and medicine; the fundamental instrument which have improved our lives in ways that we cannot account for. It can break decades of improvement, such as the anti-vaccination movement, which were labeled the top ten threats to humanity by the world health organization in 2019.

Let me address the elephant in the room; in the election and coverage of Donald Trump has officially propelled the hidden post-truth aspects

of our society into the mainstream. We were always post-truth in some ways, such as people not believing that the moon landing was real.

However, with the election and coverage, that hidden aspect has now become a reality. The easiest way to think about post-truth is from the graphic above in which, on one side, Rene Descartes states, "I think, therefore I am." Meaning, through research, education and search for knowledge, we can mold who we are. It is said to have been the birth of consciousness for Rene himself.

On the other side, we see John Doe whose statements resemble that, "Someone feeling something to be true is the same thing as it being true." According to the Oxford Dictionary, post-truth means that relating to or denoting circumstances in which objective facts are less real are less influential in shaping public opinion then appeals to emotion and personal belief."

In recent year, post-truth has increasingly become embedded in our society as individuals are not trusting, questioning and even doubting established institutions such as Universities, Governments, mainstream media, political parties and International Organizations such as United Nations, due to the perceived lack of response to issues occurring from around the world.

There are several elements as to the rise and installation to the rise of post-truth in our society. However, the biggest is social media companies. Social media such as Facebook, WhatsApp, YouTube,

Twitter and Instagram are all, in one way or another, profiting from fake news.

There are hundreds of millions of people around the world who have social media. Many of us have multiple accounts on social media platform. I have Facebook, Twitter, Instagram, LinkedIn and WhatsApp. Many people have multiple accounts on even the same platform. In 2018, Facebook has 2.6 billion people. YouTube has 1.9 billion. Instagram has 1 billion people, and Twitter has 330 million people. That is insane when you think about it, because in 2008, Facebook only had 100 million people, and in a decade, it grew by 26 folds.

One of the greatest philosophical ideas comes from Spiderman that, "With great power, comes great responsibility," and Facebook has not been that great when it comes to undertaking the responsibility to curb fake news, hate speech, and bullshit in general.

In the following slides, you'll be inundated with a bunch of graphs and facts of the number of individuals from different age groups who get their news from social media. According to Peer Research Center, close to half of a million adults obtain their news from Facebook, and more than two thirds of American adults obtain their news from social media.

In the Middle East, approximately 28% of people obtain their news from WhatsApp, and close to half obtain their news from Facebook. In the U.K., second most popular source of news is Facebook, and the

consumption of news from Facebook and social media in general grew from 2018 to 2019 as investigations were rolling along.

A real-world consequence of Facebook's laxity on monitoring and removing fake news from their platform was the Rohingya genocide in Myanmar. It took Facebook more than one and a half years to remove one of the most prominent individuals responsible for the Rohingya genocide and displacement; Ashin Wirathu, who you can see is up there on the slide. Throughout his entire life, he has posted multiple hateful and Islamophobic and generally fake comments about the Rohingya people.

Additionally, in interviews, he had said some horrifying and disgusting things, and despite that, Facebook took more than one and a half years to remove his profile from their platform, despite the fact the U.N. had stated that Facebook was a key factor in this human rights atrocity.

These countries around the world such as Spain, U.K., France and Germany have all supported in one way or another to curb and mitigate this issue, such as in Spain; the government is now demanding action from Facebook to curb their fake news. In the U.K., there are possible multiple investigations and legislation as well.

In France, Emmanuel Macron has proposed to ban fake news on websites and in social media during elections. So have the Germans as well. In the United States, approximately 50% of the population

now supports having an investigation in social media companies for their possible foreign interference in the 2016 election.

Facebook on its own part is now turning its attention to groups where so much amplification happens. Private or semi-private groups have exploded in popularity in recent year, in part thanks to a push by Facebook to promote communities. At the same time, they have become a petri dish of misinformation, radicalization and abuse. YouTube, on its end, has altered its algorithm to make it harder to find problematic videos. Finally, the department of defense has officially created a program under DARPA to root out fakes amongst samples of photos, videos, and audio clips.

My recommendations are that social media consumers need to be educated in recognizing fake news, bots, and trolls. Social media companies need to hire an army of fact checkers, and they need to hire an army of individuals who can translate and understand the linguistics behind non-English posts.

Finally, governments need to hold social media companies accountable for their inaction in mitigating fake news, trolls and bots, and also governments need to monitor the social dynamics between their citizens to prevent violent uprising, death and destruction against one another. Thank you so much for your time.

DEBORAH ESCALERA: Thank you, Abdeali. It sounds like you put a lot of work into that. We will first go to the audience and see if there are any audience questions? Please?

DAVID MARGLIN: Is Facebook maliciously trying to amass power, in your view?

ABDEALI SAHERWALA: I honestly don't know how to answer that. But I think that they can definitely do more on their end to make sure that individuals, such as Ashin Wiradu do not have a continued existence on their platform, considering his history. So, yeah.

LUKAS BUNDONIS: My name is Lukas Bundonis from the United States. My question has to do with this concept of post-truth. There are a few different historical examples of times when appeals to emotion kind of ruled supreme over truth. The Catholic Church controlled most of the truth of Western Europe for hundreds of years. Nazi and Stasi propaganda in Germany. What would you have to say to the accuracy or the helpfulness of using post-truth to define this new age? Is it helpful, or is it more of what we've seen in the past, just with a new character?

ABDEALI SAHERWALA: I think it's the same thing, however, what has happened is that rather than having a single entity like the Catholic Church control most, if not

all of the information, what is happening is that governments or groups are now trying to create their own reality or create part of the reality and use social media companies as a way to funnel that content into hundreds of millions of people. And now, with the expansion of the Internet into the African continent, it could soon be billions of people.

DEBORAH ESCALERA: Any more questions? Okay, thank you, Abdeali. Our next presenter is Akshay Broota. Akshay?

AKSHAY BROOTA: Thank you, Deborah. Good afternoon, everyone. I'm here to present about the GDPR. It's going to be a high-level overview of what is GDPR and what are its consequences, and what is its impact outside of the European Union.

I'll start by introducing myself; my name is Akshay Broota, and I'm currently a final-year master student and University of Colorado Boulder. I'm pursuing my Master's in network engineering, and I undertook a course of the Legal Mitigations Policy, where I was introduced to the GDPR and its impacts. So, let's get started.

Before GDPR, there was a law called The Data Protection Directive, it was adopted in 1995. The The Data Protection Directive was way before there was an Internet explosion and the smartphones were introduced into society. It was not at all effective, and it was very

lacking in terms of the personal data from the consumers would be protected.

The main goal of The Data Protection Directive was, however, to protect the personal data from getting misused. GDPR eventually replaced that. The first draft of GDPR was enlisted in 2012, and it was adopted in the European Union Parliament in 2016. Finally, it was enforced on 20th of May 2018.

So, now we know that when GDPR came into existence, let's know what is GDPR. GDPR is basically a law which regulates how companies should protect personal data. It is devised to harmonize data privacy laws across the European Union. The GDPR, the main goal was, GDPR was to cover the loopholes which were existing in the RD II Directive, and it to provide transparency in respect to how companies were handling consumer data. The companies which failed to comply with the GDPR are subject to stiff penalties. This includes 4% of the annual global income of the company, or up to 20 million euros.

Why GDPR? As I mentioned before, we had outdated rules in the II Diction Directive. These rules were made before the invention of smartphones, and they did not address any new privacy issues concerning the personal data. We also lacked a very transparent and detailed framework regarding how the controllers are accessing the data of personal users, and how they are selling it to third parties, and how they are targeting specific products to the consumers. Yes, people didn't have any control over their own personal data.

These are the other following rights of the GDPR. Together, these rights empower the consumer to have more power over their own personal data, and what they can enable the controller to do with that data. This includes the right to be informed, the right to access, the right to erasure, the right to object, right to data proclivity and right to restricted processing and right to rectification. Since I come from a background of Network Engineering and I am myself a user of a lot of social media platforms and a lot of service providers and a lot of ISPs, I'll be focusing more on right to data proclivity.

Before we go to right to data proclivity, we'll be concerning ourselves with some issues with GDPR. As GDPR came into existence to work on the loopholes of the II Directive, it still has some loopholes which will be hopefully covered up in future. So, GDPR does not mention what particular format the data has to be transferred between a controller when the consumer evokes its right to D II proclivity. It only mentions about the machine-readable format.

There can exist many machine-readable formats, as we know, like the JSON Format, or the PDF or the Excel or the CSV. So, there is a lack of detailed explanation about what particular format which is widely used in our society, and which is easily able to transfer the data from one controller to another.

Another thing regarding GDPR is that it does not mention how third parties' access or increase the time that's required for accessing a particular website. Also, when we are talking about transfer data proclivity from one company to another company, the costs which are

incurred in doing this data proclivity detail transfer, we do not know whether it's cost from Company A or Company B. GDPR does mention that the consumer is not liable for any cost incurred during this transition, but it does not mention about whether it should be company A, or company B.

We're coming back to data proclivity; so, data proclivity is ability for people to use their data across devices and services. It is mentioned that GDPR article 20. For example, I, being a user, I'm using the services of Company A here for a long time, and I am thinking that I want to switch to Company B, and to use their services instead. I can invoke my right to data proclivity wherein all my data gathered by Company A has to be transferred in a timely and in a machine-readable format to Company B.

When we compare this particular data protection directive in GDPR in terms of data proclivity, yes, in part matters of time, GDPR mentions that this has to be done within a month. The cost will be incurred on data controller, but it does not mention which company should take the cost. The format is again machine-readable, and it mentions that it has to be one of the widely used formats, but it does not specify which one. Yes, liability, again, it's a bit weak. We do not know which party to hold accountable in case of any loss occurred over the data during the data transition.

In general, GDPR has been the most consequential regulated development in Information Policy. Many critics believe that it has been successful so far, but it has only been one and a half years since

it was implemented. There have been some concerns since GDPR was implemented, there was a deluge of e-mails people started getting due to GDPR related activities. Like, people started getting e-mails regarding GDPR, e-mails regarding, you have to change your privacy settings, or we need your consent regarding this particular data gathering. So, there have been phishing scams regarding this particular e-mail deluge.

I don't know if you know about Max Shem, he is an Austrian activist. After midnight on the 25th of May 2018 when the GDPR was launched, he sued Google because Google was forcing its consumers to consent to its data gathering practices. And if they wouldn't consent, they would not be able to use their services.

The impact of GDPR, outside of EU has been huge, so I, coming from an Asian country in India, and I'm living currently in U.S.A., we know that in California there has been a new California Consumer Privacy Act. It will be started, and it will go into effect from 1st of January 2020. This particular act in the State of California enables the Californian residents to be more accountable and be more in charge of their own data and how companies like Facebook or Google do with their data, how they are selling their data to third-parties.

The impact has been huge, and we'll just have to wait and see how successful GDPR is. GDPR is somewhat- it brings personal data into a complex and protective regime, but it does for the European citizens who are outside of Europe, or companies who are based in Europe, but they are applicable to the citizens. So, GDPR does allow flexible- it

allows the members of the legislature to bring some changes, and we just have to wait and watch of how successful GDPR is going to be in the coming years. Thank you. Questions?

DEBORAH ESCALERA: Thank you, Akshay. Do we have questions from the audience? No, no questions, thank you so much. Our next presenter is Ariane Nakpokou Houessou.

ARIANE NAKPOKOU: Thanks, Deborah. Hi everyone, thank you for being here. My name is Ariane Nakpokou, and I'm really pleased to be a NextGen member of ICANN66. I just completed last May a bachelor's in business administration. My minor was in Professional Accounting. Actually, I'm involved in CDL Montreal, a six-stage program for Artificial Intelligence based company.

As I'm coming from the business world, it was an interesting adventure for me to learn about the basic assumption of AI and to dig in this world. My first point today is, we are going to talk about some generals about what is AI, or what I understand about AI. After we are going to talk about DNS fraud and what AI can do to prevent some fraud that come in DNS' world. After that, we are going to the hot topic of ICANN66, the conflict between WHOIS and GDPR.

And after that, I'm going to just make a review of what ICANN is doing now to address the issues. And I have since Saturday, we are here

since Saturday, I have a chance to learn more about that. I learned about what people said, so it's going to be a brief review of what is being done now. After that, we are going to move into a fabulous subject about AI, WHOIS designs.

AI was very welcome in a world that a thousand projects and now based on this concept. If you don't know, Montreal is making use of investments in this field to be the lead and an important player on this ecosystem. So, what is Intelligence, is what we are doing every day is the ability to reason, to perceive relationship and analogies to calculate, to learn from experience and to adjust our response to a situation based on that experience.

That's particularly what our brand does every day, and that's what we are waiting from a system based on AI. So, it's a subject that really fits, it's quite difficult to know how far we can go with that technology, and what we can expect from that. And it's definitely a very twenty concepts.

It's really huge when you talk about AI; there are so many little details to take into account. Just to make a brief wrap-up is; AI has different research domains as natural language processing, expert systems, neural networks. We have also robotic fuzzy logic systems. And the most popular, the most used expert systems neural networks. And what is an expert system?

It is to make a system as it could have a human expertise. You can use it in things like finance and generating medical diagnosis. And you

have neural networks who are used to recognize patterns to learn and to adjust from a previous learning. To put this system in place, there are common techniques that have been used, and we have machine learning that practically gives data to having a machine learning use algorithm to pass data, the system learns from that data and makes informed decisions based on what he has already learned.

Deep learning is a subfield of machine learning. Machine learning, now we are going to be more, you are going to create a newer network and access a newer network that can learn of its own and make intelligent decisions on his own.

The difference between the two of them is that machine learning, you can just put one data and expect him to have a similar response every time he sees something like that, but in deep learning, it's unautomated and continuously process, so that's why you need big data; you have to provide him a lot of data to help him make the connection and the analogies that are going to help him to get where you want him to go.

What are we doing with that within the DNS world? It's really interesting in terms of cyber risk. Because AI is an important tool to hosting providers to mitigate cyber risk. For technology used to protect the customers is here to detect and recognize the pattern of cyber-attacks. So, they learn from that to improve the defense from last time, and it's also able to implement on his own intelligent measures and to alert the registrar and the consumer when they are facing cyber-attack.

You can use it also to protect your domain names. This means that if you have someone who is making an action to purchase to register a domain name similar to yours, you can use it via a process server, you can just be alerted, be informed by this attempt. And it's really helpful, because it can help you to protect your business and your online reputation. If it's accepting of a counterfeit site or is trying to defraud people using your image or your website, you are going to be able to respond quickly to that threat.

Also, you can improve your domain performance because hosting providers who are using AI technology is able to make that analysis from previous site to see how well a domain name is going to perform. To see how well it's going to perform and to give you the best domain name to meet your content and your traffic and commission rates.

When you are using AI to manage your domain name system, you have an Internet with that intake, and you can definitely have a more accurate WHOIS. And that's why we switched in our, in the topic about WHOIS and GDPR, because what always overlaps each other and where we put [inaudible] for the right to know.

There is a lot of things, and we all should go on the Internet and we all should know, for a chance to -- we all should have the chance to know who we can keep accountable for information that the CDC is advocating for. That is, it's ensuring for ours too for making our mind for about this topic. But at the same time, personal information can be used to arm people and take away all the fundamental rights such as freedom of speech, security and privacy.

If we think about it, it is that the process and the control is only carried out by company and is best which sufficient technical how now, the risk of the constitution of power is obviously a concern and we can also have this tool in the hand of a totalitarian regime can help to manipulate, it could have access to the internet. So, censorship becomes faster and easier.

ICANN is trying to make -- GDPR introduces privacy by design. And ICANN and the WHOIS system is about the right to law, so there is obviously a conflict, and now ICANN is making efforts to the PDP committee to be recognized by the European -- to be recognized by the coordinative authority for the WHOIS system, and to make sure that the different, the registrar and the registrar are going to be able to provide to stay legal by providing information to the WHOIS system.

Just about privacy by design, I'm cautioned that I'm already past my time, and I can respond in the questions, if you want? Just one more.

So yes, GDPR is about privacy by design, and what one thing really important in AI is to be sure that we stay ethical when we are making the system, and when we are making information, it's really important to stay human well-oriented to make sure that we are not transposing our buyers to [inaudible] and to make sure that these are opportunities that is behind AI is not going to be a reproduction of other inequities we already have seen in our society. Thank you so much for listening to me.

DEBORAH ESCALERA: Thank you, Ariane. Okay, questions? Go ahead, João.

JOAO PEDRO MARTINS: João Pedro speaking from Portugal. Does this mean that ICANN is now responsible in some sense to start and think about how to create algorithms that are ethical? Because I know that you're from a business background, and you could also argue that the ones who are providing the product will kind of self-regulate in these terms. But this is my area of study, so this involves a lot of research, a lot of time. Usually I would point out this as a new discussion from the ICANN point of view, so what do you think about it?

ARIANE NAKPOKOU: Every time we brought this question, there is always the assumption that ICANN is dealing with content of things, and it showed that if even ICANN can really say what is inside the data and everything, we are going to move somewhere. We are going to have more policy about many things.

Canada just adopted policy about how to be ethical and AI, and maybe someday like GDPR is going to overlap some policy in ICANN. So, why not start now to make sure that when we are making policy, we still keep it in mind; human well-being. In whatever policy we are making.

LUKAS BUNDONIS: Hi, Lukas Bundonis from the United States. Ariane, first of all, thank you for a fascinating presentation. I can't really see around Josh's head. Anyway, AI has become trendy for a lot of reasons. First of all, there is numerous opportunities surrounding the technology, it's just really exciting to see all the different fields that it applies to.

But this trendiness has caused a lot of companies to brand products that don't actually use actual Artificial Intelligence with the label to sell more units, or just make better sales pitches. Do you worry, as a business professional, about non-technical customers buying AI branded solutions that they don't properly understand?

ARIANE NAKPOKOU: Totally. I had a chance to work with CDL in Montreal, and we have funding, Artificial Intelligence based company, and for me it was really difficult to understand what is really AI and what is not really AI and it took me a lot of time to really make, not making [inaudible]. So I can, as a businesswoman ensure that it is a constant, because it puts a lot of effort to put some kind of solution in place and to sell a product. So, when you have people who are labeled firstly a product as AI, it's definitely bad and you want to have a fair competition.

LUKAS BUNDONIS: If I could ask a follow-up question; do you have any thoughts on how that kind of literacy can be built across the business community?

ARIANE NAKPOKOU: I can respond to you, but it's definitely a discussion that we have to make.

DAVID MARGLIN: David Marglin, United States. So, you've shown some positive uses of AI and pointed to them. I guess you're pretty sanguine about AI. A lot of people think maybe the technology is neutral; it's what you do with it. But then, they also say, "Guns don't kill people, people kill people."

I'm wondering if you think that AI is ultimately, at least at this moment, a net positive or looking like a net positive, or if you are, as I am, deeply concerned that most and many uses of AI are either simply about selling us more stuff, or possibly more nefarious going back to the earlier presentation?

ARIANE NAKPOKOU: It's like everything; we always move into something new with some concern, with some uncertainty because we don't really know what we can expect, but it's already there so we have to make sure, like our Internet is already there to put the right guidance and to make sure that it's not going to, I don't know how to say it in English, to make sure that we can still control the situation.

For when I started working with CDN Montreal, I was really impressed by what you can do good with that. I wear glasses, and I'm going to wear it for my life, and they are really extraordinary solution for people like me in using AI, making more accurate medical diagnosis.

So, like the Internet, we are going to use it, it's always about humans choose to use some things and that's all about choice. You have to make a constant choice as a society and be sure that people are going to take advantage of this technology to make bad things, and we have to make sure that we are putting the right boundaries in this field.

DEBORAH ESCALARA: Thank you, we'll have one last question, thank you.

KUSHAGRA BHARGAVA: Hi, my name is Kushagra, I am from University of Southern California in Los Angeles. First of all, very nice presentation. My question is a very open-ended question which researchers like us and the University keep on encountering every time; when we say, "Right to know, privacy by design, and ethics by design," what are your thoughts, it's an open-ended question, so what are your thoughts on whether all these three always go together, privacy by design and ethics by design, both of them always go together, or is there something when they have different directions?

ARIANE NAKPOKOU: I think that privacy by design is a little more tight than ethics by design, because you can respect someone's' privacy, but by putting data in an algorithm, you can put your own BI's, you can just transfer your [inaudible] because technically you are saying to the machine,

"This is a banana, say banana," so it's your perception of what is a banana.

It's sure that if you are ethical by design, you are surely going to be privacy be design because you care about making sure that your consumer is going to, you are thinking about your consumer when you are designing your algorithm. But you can be privacy by design and otherwise, like people ethically have, you should think of.

KUSHAGRA BHARGAVA: Thank you very much, it was a good response.

DEBORAH ESCALARA: Thank you, Ariane. Okay, our final presenters, they are doing a dual presentation; Austin Bollinger and Lilia Herdegen.

LILIA HERDEGEN: Testing, one, two three, hello! H, everyone, thank you for coming to our presentation. This is the wonderful world of DNSSEC that we will be presenting on. My name is Lilia Herdegen, and I am currently attending Ferris State University, pursuing my masters' in Information Security and Intelligence.

AUSTIN BOLLINGER: My name is Austin Bollinger, we're both from Grand Rapids, Michigan area, and I am currently an IT Security Analyst, and I also study IT Security at Grand Rapids Community College. We're going to be going

over a brief history, very brief, along with problems and some wins of DNSSEC.

I'd like to start off by saying all the information contained within is strictly for educational and informational purposes only, and it's important to note that any protocol when misconfigured poses security risk and opens the door to vulnerability.

LILIA HERDEGEN: Yes, we just want to make sure that we're not stepping on anybody's toes; it's just what we've observed since DNSSEC has been pushed by ICANN in the recent years.

So, why DNSSEC? Back in 1990, Steve Bolovin demonstrated something known as, "Cache Poisoning," and one type of cache poisoning is DNS cache poisoning. Those who were working on DNS early on proposed the solution to cryptically sign DNS requests.

Up here on our slide we also have an example of what DNS cache poisoning is; it's when a user sends a DNS request to a compromised recursive resolver, and that request will either go to a poison cache, which will be a malicious site, or it will go to a clean cache, which would be the intended site.

Along with that as well, if a user was to go to a login site for their college board, they'd be logging in with their username and password. If the site was poisoned, it could look similar to, or exactly like what they should be logging into, but it could be a malicious site which

would be harvesting their credentials. That's just an example of DNS cache poisoning.

AUSTIN BOLLINGER: Up here, we have some DNSSEC adoption rates. The graph is a bit interesting; we did make this out of sourced information, but you can see in 2015, DNSSEC signed domains was up at 40 thousand, and there's quite a big spike in 2018 in DNSSEC adoption rates up to 200 thousand.

A lot of this DNSSEC signing of domains is directly linked to ICANNs awareness on DNSSEC, which is very wonderful in the sense that it is solving the problem of DNS cache poisoning, but there's also some related things going on here at the same time, so I think that's really important to take observation of.

LILIA HERDEGEN: Associated with those DNSSEC adoption rates, we have DNS amplification. DNS [inaudible] tax report in 2019 said that it made up almost 66% of all denial service activities. Back in 2018 where that was that push, there was approximately 1040% increase in these attacks. Then, in 2019, the first quarter, there was another increase with 31%.

This is just a quick example of the comparison of the 66% compared to other tax, such as HTTP floods, HTTPS floods, that kind of thing.

AUSTIN BOLLINGER: DNS can utilize TCP or UDP, most commonly UDP. And it's important to note with the TCP protocol, you've got a three-way handshake, it looks like a SEN, SENAC, AC; with UDP you don't really have that handshake there to make sure that the origin IP address is in fact what it is, so an attacker could potentially spoof the origin IP address, and then that's going to cause the reflection attack.

In the specific case of handling a DNS reflection attack, this is a DNS amplification attack. Again, IP spoofing, you can go ahead and carry out against port 53, which is utilized by DNS, and in the cases of DNSSEC being introduced, it allows for stronger attack, and we'll see that here in the next slide or so.

LILIA HERDEGEN: Yes, so here we have a DNS amplification attack example. On the left, you can see the attacker. They, in this case, will be sending thousands of bots to open DNS resolvers with spoofed IP requests, and these open DNS resolvers are not properly configured, so they will not block out any of these spoofed IPs, and they will all send those requests to a target victim, which will end up in a denial of service for anyone who would try to go to that site that is being attacked.

Another quick couple of things about DNSSEC implication; back in 2015, economy found some traffic shows large number of attacks utilizing DNSSEC configured domains. That goes along with the push that was a push for implementation by ICANN on promoting DNSSEC.

AUSTIN BOLLINGER: And with that graph that we showed earlier in 2018 where we saw 200 thousand DNSSEC signed domains, keep in mind that large uptake, we also notice that on CSO MAG, they've reported since 2018 a 1000% uptick in DNS amplification attacks, so I believe that information, it looks very close together, and when exploited, of course, you can utilize DNSSEC extra information within the protocol to amplify attacks, and in that case, it looks like attacks can be 36 to 70 times stronger.

So, it does solve problems, but at the same time, by adding the extra information into that protocol, it also potentially allows attackers to generate stronger attacks. So, it's security that unfortunately adds some potential issue.

LILIA HERDEGEN: OWASP top ten, for those who are not familiar with OWASP, OWASP is Open Web Application Security Project. This is a group of people who take information from the Internet, the data, and collects it and every couple of years they post the top ten vulnerabilities that pose risks.

Listed in the top ten back from 2017, which is the latest information we have from them listed were, security misconfigurations, and this goes along with DNS. DNS configurations need to be rate limited and restricted to trusted sources as default configurations may not be safe, and typically aren't for any type of default processes.

AUSTIN BOLLINGER: Back in 2013, ICANN recommended mitigating DNS amplification, and that looks like disabling recursion on authoritative name servers, along with limiting recursion to authorized clients and rate limiting of recursive name servers. It's important to note that ICANN was recommending these DNS amplification mitigations early on, and I think that it would be important that also when recommending to turn DNSSEC on, also recommending these fixes to mitigate default configurations that can allow stronger attacks.

INX, they've posted on their website about DNSSEC outages, along with validation failures. This can potentially cause issues going forward for domains, but it's important to note educom.edu had basically just bogus entries for DNSSEC delegation for at least five years, so it's interesting. I think people are kind of testing this out, and with publishing these records, it's just really interesting to see the potential for failure.

Right now, when people implement TLS and HTTPS, you see sites expire. I'm just curious how that's going to look like, maintaining, going forward, when some people can't keep their HTTPS and TLS certificates renewed, now you're adding an additional thing to maintain for individuals into the future.

It's also important to note that if you'd like to continue on going to a website that's failing DNSSEC, which will generate a serve fail, then you would have to have your DNS server go ahead and disable that DNSSEC checking. I guess going forward, I'm really interested to see

how browsers handle DNSSEC validation, what that's going to look like.

LILIA HERDEGEN: Some takeaway from this; we found that minimal threat is posed as long as DNS servers are appropriately configured, and DNS mitigates DNS cache poisoning as well.

AUSTIN BOLLINGER: DNSSEC is most certainly not encryption, and in the community, I know there is talk about DNS over HTTPS/TLS, so that's the encryption. DNSSEC is more about authenticity, and it really just helps in that sense mainly. It's also important to note that our main emphasis on this topic is that default configurations just open the door to vulnerability and allow attacks to be performed.

LILIA HERDEGEN: That is our presentation, if you would like to contact us, we have our information here. If you would like the QR codes or something. And we want to give a quick shout out to our colleagues who are tuning in right now from Grand Rapids, Michigan. Hi, everyone! That's it, thank you for listening. Thank you for ICANN, for everything that they've done for us, and we appreciate that. So, thank you.

AUSTIN BOLLINGER: Yeah, we are very happy to be here with the NextGen group, it's really a blessing and we're both very thankful to be here. I'd also like to mention one last thing; DNSSEC does solve a problem, so I'm not against DNSSEC at all; I think that there is some importance in it. It's just important, I think, for example, telling someone that running is healthy, also telling someone not to run with scissors at the same time. Thank you.

DEBORAH ESCALARA: Great presentation, thank you so much. Do we have questions? We'll start here.

AKSHAY BROOTA: My name is Akshay, I am from University of Colorado, USA. Thank you for your presentation. DNSSEC is as secure as it can, but with security it also increases complexity, and it also has a bigger packet size, and it requests more bandwidth. So, what's your take on that? As we believe in DNSSEC in the network, we allow for the bandwidth to be utilized more for the DNS traffic, rather than for any other normal traffic. What's your take on that?

AUSTIN BOLLINGER: I'm trying to understand the question. I think the main importance is not utilizing default configurations on servers. I understand increased bandwidth is going to be important, but allowing misuse of bandwidth, for example, abuse of the DNS system, I guess indirectly, it

just causes an issue of concern, because not everybody has their configurations locked down.

Security can be a challenge, and so recommending people add authenticity without having default server configurations locked down is the main concern. Is that helpful, or would you like to re-ask the question maybe?

AKSHAY BROOTA: In data Internet networks, we generally prefer not to make it more secure because it requires more bandwidth, so I was just wondering in a network which has a restricted amount of bandwidth, will DNSSEC be the only solution, or are there any methods which we can opt to? Because everyone might not have that flexibility to implement DNSSEC since we are restricted in bandwidth.

AUSTIN BOLLINGER: I feel like that is definitely an interesting question and I would say that's more of a networking type of concern. That's quite an interesting network concern, but I would say with the focus on DNSSEC, it mostly focuses on resolving the issue of DNS cache poisoning, and with, for example, encryption of DNS coming forward that kind of resolves the issue at the same time, so I guess in terms of the added or the increased bandwidth that you would see with DNSSEC, I'd say there is an expense there and that's kind of where DNS over HTTPS can come into play.

I know that Mozilla, Firefox, they're looking into utilizing Cloudflair, so offloading the bandwidth to, for example, a cloud service provider is probably going to make the most sense. I would say utilizing a CDN for that traffic could be a solution. That's the interesting thing is that DNSSEC, along with encrypting DNS traffic is coming along at the same time.

I think there needs to be more work on that together, because you have the encryption piece, and the authenticity piece and focusing on that together in one group I think would be really helpful, instead of separating those two. Because encryption and authenticity, they can certainly go together, and I think it needs to be team worked.

DEBORAH ESCALARA: We have a couple of online comments. "Thanks for the shout out from GRCC." And from Lynn L., "No questions from me, just want to say great presentation." Any more questions from the audience? Okay, go ahead.

ABDEALI SAHERWALA: Can you explain to people like me who are not technically literate that what is cache, and what is cache poisoning?

AUSTIN BOLLINGER: Yes, so basically when you've got a cache, let's say that, I'll give a good example of browser cache, that's probably the easiest to understand. When you go out and you load a website, there's data that gets

downloaded and you get your JavaScript files and images. You can enable caching, what that's going to do in a web browser is keep those image files and maybe some of that JavaScript in the browser on that local machine, so that way you don't have to keep going and getting those files all the time.

DNS has a similar way that it handles caching, so that way you're constantly not hitting DNS queries across the networks. When you have a DNS cache, it basically goes out, it resolves the records, and then keeps that there. In the case of DNS cache poisoning, an attacker gets in between there, and he serves you incorrect information.

So, in a sense, it's a man in the middle attack where an individual is getting between the user and their cache, and they're injecting a malicious address. So, you're going to get that cache information, it's the wrong information, you just basically been man in the middle attacked and now the attacker can serve up incorrect information.

ABDEALI SAHERWALA: They do it through the system?

JOAO PEDRO MARTINS: Going a little bit back to the nice that you were mentioning, you mentioned associated two critical security requirements. Would you go into formulating perhaps a new protocol that would implement both of them, which would imply a lot of rewriting, redesigning, perhaps going back to the drawing table? Or, would you say that

combining two existing tools or protocols would be like more efficient at the be ready point of view in terms of continuity and long-term view would be less efficient?

AUSTIN BOLLINGER: I definitely think that that's probably the best question so far, so thank you, first of all. And second of all, at the SSAC meeting, they talk about security concerns within ICANN and an individual brought up a very neat concept on introducing blockchain type technologies to DNS and how that could potentially look. I think decentralization of the domain system is very tricky, and then what would that look like for ICANN type of thing?

So, I mean, ICANN is quite centralized in terms of how domains are managed. There is some splitting up, but I guess the main idea I would have for introducing some sort of authenticity is somewhat similar to how blockchains manage that, in the sense that you're not focusing on one trusted root zone being signed correctly. What's that look like in the case of there being a war, and then one country just saying, "Hey, we're pulling that." All those domains.

I think going into the future, that's very powerful, to just be able to go up to that root zone and say, "Your entire set is done." That sounds very powerful, so I think in terms of a new protocol, that's a neat idea. It has taken twenty years to get to where it is right now, and Internet protocol change, it takes so much time and it feels kind of slow, and it's constantly changing at the same time. So, I'm not sure how to

perfectly answer that question, but it seems like we're twenty years deep and things are still changing.

DEBORAH ESCALERA: Any other questions? Okay, thank you so much for your presentation. That concludes our presentations for today. I want to thank our presenters today; you are all very well prepared. I saw no nerves, that was incredible, so very well done.

Thank you to my Ambassadors for your support today. I want to remind everybody that we have a second round of presentations tomorrow that being at 15:15 in room 512G, so spread the word. I hope to see more audience participation tomorrow as well. Thank you so much for being with us today.

[END OF TRANSCRIPTION]