ICANN74 | Policy Forum – NextGen Presentations (2 of 2)
Wednesday, June 15, 2022 – 13:15 to 14:30 AMS

DEBORAH ESCALERA: Hello and welcome to the NextGen@ICANN presentations. My name is Deborah Escalera and I am the remote participation manager for this session. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior. During this session, questions or comments submitted in the chat will only be read aloud if put in the proper form, as I've noted in the chat. I will read questions and comments aloud during the time set by the chair or moderator of this session.

Interpretation for this session will include English, Spanish, French, and Russian. Click on the interpretation icon in Zoom and select the language you will listen to during this session.

If you wish to speak, please raise your hand in the Zoom Room. And once the session facilitator calls upon your name, kindly unmute your microphone and take the floor. Before speaking, ensure you have selected the language you will speak from the interpretation menu. Please state your name for the record and language you will speak, if speaking a language other than English. When speaking, be sure to mute all other devices and notifications. Please speak clearly and at a reasonable pace to allow for accurate interpretation.

With that, I would like to welcome you to this session and thank our NextGen@ICANN participants for their hard work in preparing their presentations. I would also like to thank my mentors, Sophie Hey, Dessalegn Yehuala, and Roberto Gaetano who have been working with the students over the past several weeks and guiding them through the ICANN meeting process. I would also like to thank my colleague, Siranush Vardanyan, who will be running the slides today. With that, I will hand the floor over to our first presenter, Juuso Järviniemi. Juuso, the floor is yours.

JUUSO JÄRVINIEMI: Good afternoon. Do we have the slides?

DEBORAH ESCALERA: One moment.

JUUSO JÄRVINIEMI: Okay. Hello, everyone. I'm Juuso Järviniemi, one of the NextGen participants. And today, I will talk about the WHOIS database, especially from the viewpoint of EU regulatory developments. Next slide, please. So I will first briefly present WHOIS and some key debates concerning this database. Then I will talk about the current EU regime, especially the GDPR. Thirdly, I'm going to talk about the upcoming network and information security directive or NIS2 and the debates on WHOIS that have taken place as a part of this process. And finally, I'm going to discuss the implications of these policies to registries and registrants. Next slide, please.

DEBORAH ESCALERA: Juuso, remember to go slowly. Thank you.

JUUSO JÄRVINIEMI: Okay. So WHOIS is a public database of domain registration data. In other words, thanks to this database, you can look up who has registered which domain name. Properly speaking, WHOIS is a system of distributed databases run by the registries and the registrars which collect the data from the registrants. But in any case, through online lookup tools, you can enter a domain name and see who owns it.

This traceability is good for preventing and tackling different kinds of crime, like copyrights and phishing issues, for example. But on the other hand, privacy advocates have been concerned about a public directory like this because, for example, if your contact details are out in the open, you might get unsolicited contacts. So this debate between privacy and security has been very present here and it's also relevant to legislative debates.

Another related issue is the accuracy of data provided into the WHOIS system. ICANN itself works on this. And under the registrar accreditation agreement of 2013, registrars have certain obligations for proactively checking if this data is correct. Data accuracy is another thing I will return to. Next slide, please.

So on GDPR, the European Union's Data Protection Authorities have, for a long time, expressed concern about the publication of data on WHOIS. The predecessor of the current European Data Protection Board has, since 2003, already urged ICANN to ensure data protection in WHOIS.

GDPR entered into force in 2018 and this was a trigger for ICANN to change its mechanisms. ICANN adopted a Temporary Specification for gTLD registration data which continued with the collection of registration data but restricted access to the data so that you could request it for any legitimate purposes only.

Even though GDPR only applies to persons in European economic area, the impact has been global. For example, one study found that more than 60% of At-Large WHOIS data providers have redacted data also from non-EEA registrants. An interim policy is still in place. And drafting of a more permanent Registration Data Policy has been ongoing.

One should note that ICANN policy only concerns gTLD registry operators. But of course, country code TLD registries have been adopting their own compliance mechanisms which have slightly differed from each other.

So in short about GDPR, the dawn of GDPR obligations was a big change for WHOIS and the effects extended beyond the European Union. But on the other hand, this change didn't come from nowhere. As was mentioned, European Data Protection Authorities had, for many years, interacted with ICANN on this issue. And moreover, similar internal discussions also have taken place. For example, in 2013, an expert working group convened by the ICANN Board had indeed recommended a model where data is collected, validated, and disclosed for permissible purposes only. Next slide, please.

So this brings us from the question of disclosure to the issue of collection and data accuracy. I mentioned the NIS2 directive proposal, which is an ongoing legislative process in the EU. The European Commission made a proposal for this directive, which covers different areas of cybersecurity, in December 2020. And one of the many provisions of this directive would require registries and registrars to collect and maintain accurate and complete domain registration data.

The European Parliament and the Council have negotiated on this text. And they reached a provisional agreement in May. Based on what we can know by now, the agreement is quite similar to the original proposal. Next slide, please.

So to analyze this a bit, this is a new legal obligation within the EU framework. The previous NIS directive already gave different obligations to DNS service providers. But registration data accuracy was not one of them. As I mentioned earlier, the ICANN community has also been interested in data accuracy. But nonetheless, the NIS2 directive seems to go further.

The Registrar Accreditation Agreement of 2013 and the community discussions that have taken place since then have mainly focused on ensuring that data is in the right format. So, for example, street address should contain an address that is real. But by contrast, the EU policymaking process seems to be adopting a more robust definition of accuracy, even though this legislative process doesn't yet quite flesh this out in detail.

Now, depending on what accuracy comes to mean in practice, this might entail even new types of ID verifications for people who are registering domain names. So what the accuracy comes to mean in practice is a very important question.

Now, a second point is we should note that NIS2 will be a directive, which means that once the accuracy requirements do come into effect, the registries and registrars would need to see how the obligations are transposed into national legislation. In other words, in each member state, the information to be collected could be a little different.

However, we should note that the outcome of the trialogues, the negotiations between institutions, has specified what kind of data should at least be collected, which someone reduces the potential for national divergence. This also connects to the directive's requirements to have policies and procedures in place to ensure the accurateness of this information.

On the one hand, since everyone is in the same boat with the new legal obligations, one could imagine that there could be a standard template for these policies and procedures and these could enter widespread use, for example. But on the other hand, if different member states set slightly different requirements for what data has to be collected and how, then a company that wants to comply with multiple countries' legislation at once might be inclined to follow the most stringent rules in order to comply. And this would then create convergence towards the more strict rules within the European Union. Next slide, please.

So that brings me to the end of my presentation. Just to summarize, disclosure of WHOIS data and the accuracy of this data have, for many years, been two important questions around the WHOIS system. In recent years, the EU legislature has taken an interest in both of these issues. GDPR pushed the ICANN community to develop policies on data disclosure. And now, similarly, NIS2 is going to push the community to develop practices on accuracy. The NIS2 legislative process is soon going to be finalized. Our sights should be set on how the directive will get implemented.

So in these slides, you can find my bibliography. Thank you so much for listening and I'm looking forward to any questions.

DEBORAH ESCALERA: Thank you, Juuso. I want to remind our presenters to mute your laptops, just in case. I was hearing a little bit of feedback. There is a question online from Lutz Donnerhacke. Question: "What is the original reason to collect the WHOIS data? Is the purpose still served? Can the new purposes—law enforcement, intellectual property—replace the original reason for collection or does this need a new attempt to collect the data. Would not much better to publish the chain of contract down from IANA via registry, registrar, down to the reseller, and drop the registrant data copy out of the local environment altogether? Ultra-thin WHOIS approach."

I want to remind those online to follow the correct format that I put into the chat. Thank you.

JUUSO JÄRVINIEMI: Thank you. I'm looking at the question in writing as well and processing a little. Yes. So indeed, the NIS2 directive, it also has recitals which explain the purpose of the legislation. And in here—I think it's recital 60 or 62—talks about the different possible permissible uses of disclosure. I hope I'm saying things that make sense. And in here, law enforcement, of course, is one of the permissible uses. But the disclosure doesn't need to limit itself to law enforcement. The different possible purposes are listed there.

I should also say that in my view, the question of disclosure has mostly been settled because the new legislation, it mainly circles back to the existing data protection framework that the EU has. If we look at NIS2 directive, basically it always says "in accordance with existing data protection rules," which not only means GDPR. So in my view, this means that NIS2 is especially about accuracy, whereas disclosure, we just look at what the law is at the moment.

DEBORAH ESCALERA: Okay. Thank you. Lutz, you raised your hand. Is that an old hand or a new hand? Oh, you're here. Okay. Please come to the microphone.

LUTZ DONNERHACKE: Thank you for the answer but you missed the point. It's not the question who is able to have access to data. But the question is why should the data be collected? Law enforcement may have access to existing data. But simply because law enforcement want to know something, it's not a reason for collecting data.

It's explicitly forbidden in European law, especially if, as you note, that data or personal data is collected from all your respective environments all over the world into a central database so that law enforcement and intellectual property industry has it made most easily to have somebody who has already broken the law—the various local law—because we have that database and have easy access to it.

I don't think that simply because we do not have the original reasons for collecting that data anymore that we still continue collecting this data, breaking local laws, all over the world in order to make it easy for law enforcement and intellectual property industry to have access to. I do not understand this. I would drop the WHOIS system and replace it by publishing chain of contracts so they can go the way down themselves. Thanks.

JUUSO JÄRVINIEMI: Thank you. Indeed, the legal obligation that is, in all likelihood, coming into place is that there will indeed be an obligation to collect certain data. But then, of course, once must discuss the rationale for introducing such rules, such legislation. So indeed, this is a part of this discussion on privacy and security. Even if the data is not publicly available, it will be available to someone, of course.

I would say the standard arguments about security have come up in the preparation of this legislation—the idea that it should be somehow traceable to enforcement authorities who has these domain names. Indeed, as you say, ultimately, I think it must be a political choice. And there are value judgements. There are arguments on both sides. But that's what laws are made of. And this is the solution that the European Union system seems to be converging into.

DEBORAH ESCALERA: Thank you, Juuso. We're having a little bit of technical difficulty with our presentation laptop. So just bear with us one more minute. Thank you. Are we good to go? Okay. Are there any more questions for Juuso? Okay. So let's just have a quick break. Stretch your legs if you like. Bear with us. Thank you so much. Okay. We're ready. Our next presenter is Dominik Tkalcic. Dominik, please proceed.

DOMINIK TKALCIC: Thank you very much. Good afternoon. As a member of a research team at the University of Mannheim that conducts research on social network analysis, I would like to use the following presentation to introduce you to the aforementioned method in the context of Internet governance. Does it work?

Okay. May I continue? Internet governance, yeah. It's a multistakeholder approach to Internet governance. So we have different stakeholders, different actors from different spheres coming together, and essentially, discussing the governance of the Internet. Next slide, please.

But it's difficult to trace and also to understand the complex interactions and relationships between these actors. Next slide, please. Therefore, I propose, with the following presentation, that social network analysis, as a methodological framework, can map the complex relationships in Internet governance and help us understand them. Next slide, please.

Social network analysis can be understood, essentially, as concepts, methods, and techniques for the study of social relationships. Most striking characteristic is the relational perspective, which presupposes a dependency of interacting actors. Social network analysis is capable of investigating and tracing complex relationships at actor, group, or system level. Moreover, social network analysis is able to deal with forms of social organization that arise only from interaction. Next slide, please.

Social networks, they consist of a fixed set of actors and the predefined relationships among them. They can be modeled by using a graph consisting of nodes and edges between them. Essentially, social networks are simplified representations of complex sets of relationships. And they're illustrated by graphs that reveal structures, patterns, and regularities. Moreover, social networks are conceivable in countless forms and data can be obtained from a wide variety of sources which make social network analysis a very versatile method and tool. Next slide, please.

Then we start off with the nodes. And social agents within networks are usually modeled as nodes. And different levels of aggregation are possible. So nodes could be interpreted as persons, as groups, but also as organizations. But there are also countless other options possible. Next slide.

Then we have the edges. And edges are, essentially, the adjacency between these nodes. And they can be transferred into social concepts—for example, social relationships but also attention, appreciation. So there are also numerous options conceivable. Next slide please.

If we combine nodes and edges, we get the graph. And the graph illustrates the social network. As a little side note, unconnected nodes are also considered as part of the network. Next slides please.

Then we have paths. Paths are a set of edges between two nodes without repetition of nodes. Paths do not necessarily exist between all pairs of nodes. Paths are important for calculating centrality measurements, which I will talk about in the next slide.

We start with the degree, which is the simplest centrality measurement. And the degree is the number of edges of a node. And it’s a local centrality measurement because it represents the size of the direct neighborhood of a social actor within a social network. Next slide, please.

Next to local centrality measurements, we also have global centrality measurements. And the most prominent ones are betweenness and closeness. Betweenness is essentially the number of shortest paths passing over a node. And nodes with a high betweenness are possible to influence flows.

On the other hand, we have closeness. Closeness is the average path lengths of the shortest paths to all other nodes. So it's a relative proximity measurement. And nodes with a high closeness are possible to influence the whole network. Next slide, please.

To illustrate it real quick, if we have nodes, for example, with a low betweenness and a high closeness, it's close to all other nodes but it does not block any paths within a network. If we have, on the other hand, a node, which is high in betweenness but low in closeness, it blocks paths to nodes that are quite remote. But the nodes are definitely looking out for within a network are the ones that are both high in betweenness and high in closeness because these are gatekeepers that reach lots of nodes. Next slide, please.

Then a little bit about the trajectory of SNA research and the criticism of the method. SNA is often criticized for being reductionist and conveying a mechanistic, positivist view of the world. And the major weaknesses of SNA are methodological, particularly with respect to measurement difficulties and data availability. Other points of criticism are the lack of generalizability, inaccuracy, and subjectivity.

However, these problems have been significantly reduced with the advent of the Internet and increasing computer power, especially within the last years and decades. Next slide, please. It’s the case because, with the Internet—and SNA applies to the worldwide web—huge amounts of published data can be collected and analyzed in a relatively short amount of time. And by limiting the data to published data, that risk of data incompleteness is eliminated. The problem of research subjectivity is also significantly reduced.

Another advantage is that data can be passively collected—for instance, through the use of web crawlers, which I will talk about in a few seconds. And applied to the Internet, SNA provides information about structures, behaviors, and interactions online. Next slide, please.

Then I will demonstrate to you real quick an exemplary network on the basis of a sample set—a few domains I considered as relevant or interesting for mapping out a network of Internet governance and ecosystem. A crawler was used to follow the links and to build up the respective network.

And it resulted in an example network with almost 30,000 nodes and more than 38,000 edges, which is quite a lot. And this demonstrates how big and complex Internet governance is. I also picked out some interesting nodes, top nodes, regarding to the degree, the betweenness, and the closeness. And I highlighted ICANN. Even though it's difficult to estimate what the numbers actually say, I want you to compare it with big organizations. You can see ICANN performs quite well. So it’s within the top 10 regarding the degree, the betweenness, and the closeness.

And also, to make it more tangible, I visualized the network. Next slide, please. There you can also see how complex social—how complex Internet governance is with all these stakeholders interacting with each other. And just in case you were wondering where ICANN is positioned within this network—next slide, please—it’s the node at the very bottom.

And that’s it for my presentation. If you have any questions, please reach out to me. I would be happy to provide you with further information. Thank you very much.

DEBORAH ESCALERA: Thank you, Dominik. Are there any questions for Dominik? Okay. Thank you so much. We are going to move on to our next presenter, Annika Linder. We’ll wait for your slides to be put up.

ANNIKA LINDER: Thank you, Deborah. And thank you, everybody, for attending this session. In the current time, we are more and more thinking about how we should prepare our world for the future. With respect to resource management, there is a clear tendency for increased focus on intergenerational responsibility. This is now also reflected by the law. In March 2021, the German Constitutional Court passed a groundbreaking judgment regarding climate change in which it, for the first time ever, recognized an intemporal assessment of rights to freedom as well as freedom restrictions. It sets limits to living at the expense of future generations.

What does a judgment about climate change have to do with the work of ICANN and the Internet, you're probably wondering? Well, this idea has soon been picked up by some scholars which try to argue that the key statements of this ruling can be transferred to other areas—for example, the German social security system as well as matters of government there. But could these ideas also be transferred to a completely different area, namely the Internet?

In this presentation, I will try to argue whether or not this climate change judgment by the German Constitutional Court is transferrable to the Internet and whether or not a right of future generations to stable and functional Internet exists.

To do so, I will firstly introduce you to the key statements of the climate change judgment. Then I will talk about the existence of a fundamental right to Internet on a German, as well as on a European level. And lastly, I will transfer the key statements of this judgment to argue the potential existence of a right to future generations to stable and functional Internet. Next slide, please.

So let me first summarize what the German Constitutional Court said. First of all, the German Constitutional Court has explicitly stated that future generations are not entitled to fundamental rights. Therefore, the duty to afford intergenerational protection has a solidly objective dimension, which basically means that there is a need to guarantee the existence of a set of norms that are necessary to exercise the fundamental rights in question.

Secondly, the possibility of serious or irreversible impairments is a prerequisite for the adoption of a duty to spread opportunities associated with free and proportionately across generations. And lastly, article 20a of the German Basic Law is the central basis for the duty to secure freedom intemporarily, which in summary, states that "mindful also of its responsibility towards future generations, the state shall protect the natural foundations of life and animals." Next slide, please.

Now let us move on to the existence of a fundamental right to Internet. It is important to note that there are two dimensions—on the one hand, Internet infrastructure, and on the other hand, access to Internet content. In some states, such as Portugal and Greece, the right to Internet is already codified in the countries' constitutions. This, however, is not the case in Germany.

However, there are still approaches to argue the existence of such a right in Germany. For example, in 2015, a scholar argued that such a right is implied in the fundamental right to subsistence minimum that is in line with human dignity. The minimum level of participation which is necessary as man exists in social relationships can only be achieved by means of Internet access.

On a European level, the European Court of Human Rights and the Court of Justice of the European Union protect the enjoyment of Internet access and online content against interference by invoking the freedom of expression and information.

So to summarize, there is not yet a universal codification of a human right to Internet. However, as numerous courts and scholars have argued, such a right is implied in other fundamental rights, especially in the right to freedom of expression and information as well as human dignity. Next slide, please.

So let me now move on to the key point of my presentation. And I will be explaining whether or not the key statements of the judgment I mentioned before are transferrable and whether or not the right of future generations to stable and functional Internet exists.

First of all, a potential right of future generations could only have an objective dimension. The German Constitutional Court, as I mentioned before, has explicitly stated that future generations are not entitled to fundamental rights.

But let us take another step back and figure out if such a right even exists. In my opinion, it does not and here is why. One of the prerequisites for the adoption of a duty to spread the opportunities associated with freedom proportionately across generations is the possibility of serious or irreversible impairments.

The Internet has become an integral part of our daily lives. One's ability to educate oneself, have social interactions, and make money strongly depends on it. Therefore, missing Internet access can have substantial damages on individuals. And one could maybe argue that when an entire area is not connected to the Internet at all, the damage done by missing Internet infrastructure leads to serious impairments. And the people living in this area will probably not be able to catch up with the world.

However, let's take a look back at the exact phrasing of the judgment—what we jurists like to do. And it talks about spreading opportunities associated with freedom. If Internet infrastructure is not built up now, current generations suffer as would future generations. Therefore, freedom would not be distributed. Also, future generations, with respect to Internet infrastructure, would now be forced to engage in radical abstinence, as the court called, if current generations do not build up Internet infrastructure now.

Simply put, what I'm trying to say, with climate change, we, the current generation, need to engage in abstinence so that future generations do not have to engage in radical abstinence to prevent reaching the tipping point and basically save the world. With respect to Internet, we, the current generation, would need to invest and proactively work on building up Internet infrastructure so that future generations can benefit.

However, we do not need to restrict ourselves in order to prevent reaching some kind of tipping point, which shows that the discussion about the Internet is not comparable to climate change.

And furthermore, Article 20a of German Basic Law, which as mentioned before, is the central basis for the argumentation of the German Constitutional Court, explicitly mentions a responsibility towards future generations. Again, stating it, it says "mindful also of its responsibility towards future generations, the state shall protect the natural foundations of life and animals." However, the Internet is not part of the natural foundations of life and animals. Therefore, Article 20a of the German Basic Law is not applicable in this case.

To sum up, let us circle back to what I said in the beginning. We're living in a time where there is a clear tendency for increased focus on intergenerational responsibility. Climate change has been used as a vehicle to reflect this change in thinking and the law. This is not only the case in Germany. For example, also in the Netherlands, the Supreme Court ruled in 2019 that that government of the Netherlands has to reduce their emissions in accordance with their human rights obligations.

So although the right of future generations to stable and functional Internet, in my opinion, cannot be derived from the climate change judgment of the German Constitutional Court, it will be very interesting to see how the German Constitutional Court, as well as other courts, will relate to this judgment in other manners and whether or not such a right of future generations, as well as other rights of future generations that reflect the idea of intergenerational responsibility could be derived from future judgments.

Because in the end, there are only two ways in which such intergenerational responsibility can finally get footing. Either a respective law is passed or courts find a way to argue the existence of such rights within the current legal system as the German constitutional court did with climate change. Thank you.

DEBORAH ESCALERA: Thank you, Annika. Are there any questions? Let me check online. Okay. Thank you so much for your presentation. Very well-done.

Okay. We're going to move on to our next presenter, Puthineath Lay. The floor is yours.

PUTHINEATH LAY: Okay. Can I start now? Good afternoon, everyone. First I would like to introduce myself. My name is Puthineath and I'm from Cambodia. And now I'm doing my master's degree in data science and artificial intelligence in France at the University of Grenoble.

So then I also want to introduce the relevance of my project to ICANN's work. The ICANN Organization DNS Security Threat Mitigation Program tries to make the Internet a safer place for end users by using the [inaudible] of the DNS security threats across the Internet. So my project objective is similar. I can say it is a complement to ICANN's work. Because we also want to prevent some academic fraud, we try to publish nonsensical scientific literature. So for the specific scope, my research is called Detecting tortured Phrases in a Scientific Paper.

So now, let's move to the next slide. Can you go back to the previous slide? So for this presentation, the first part I will do the introduction, and then the problem and then the solution.

So now, let's get started with the introduction. Next slide, please. Next slide. Yes. A large number of nonsensical papers have been seen recently. And scholars and some journalists submit these papers to some forums to expose the improper peer review. It means that they submit nonsensical scientific papers and wait to see if those papers are accepted to be published by some publishers or not. And then it happens. Some publishers, they accept those meaningless papers to be published.

Another story in the next slide is that … Next slide, please. A story from Bohannon mentioned in 2013. Here, "the author" refers to the fraudulent authors. They created journals with names like The American Journal of Medical and Dental Science or the European Journal of Chemistry to imitate, and in some cases, literally cloned those of the western academic publishers. This meant that for the fraudulent offers, they tried to create the fake scientific journals and then they claimed that they are in Europe. Actually, they are in Asia or something because they were tracked by the IP address and the bank invoice—so claimed that they are in another country, not in Europe.

The next slide, please. We also have another story because the machine can generate the book. So this is the example of this book. It's called Lithium Ion Batteries. So this book is generated by the machine and the author is not human. The author of this book is the machine. So it consists of 278 pages.

Next slide please. So the nonsensical papers and the nonsensical texts are produced by humans or it can be produced by the machine. So from now on, I will focus on the machine-generated texts and the machine-generated papers.

Next slide, please. So here are the websites that we can generate the computer science research paper. So I would like to introduce the two websites called [inaudible] and [inaudible] here. These websites can generate fake papers.

Let’s move to the next slide. So this tool is called Spinbot. It is a paraphrasing tool. So yeah. The paraphrasing tool is useful, sometimes, because it helps us to paraphrase the text and make us unique and to avoid plagiarism or something like that. But sometimes, it paraphrases the text that should not be paraphrased. For example, the phrase “artificial intelligence.” This phrase is supposed to be artificial intelligence in every context. But when we tested it to the Spinbot tool, it paraphrased to be “manmade brainpower.” So yes. This is a problem of the paraphrasing tool. Now let’s move to the next part about the problem. So next slide, please.

Due to the [inaudible] claim in 2021 that, as a result, meaningless randomly-generated scientific papers end up being [inaudible] and sometimes sold by various publishers with a prevalence estimated to 4.29 papers every one million papers. So this is the problem. As previously mentioned, I worked on the specific scope to detect tortured phrases because we observed that the meaningless paper contained nonsensical text. Next slide, please.

So in this slide, I would like to introduce two new terminology. The first one is the tortured phrases and the second is the expected phrases. So the tortured phrases are the weird phrases used in the text. And it's mostly generated by the machine because of the paraphrasing tool. For example, the example that I have mentioned earlier for the phrase, "counterfeit consciousness" or the "manmade brainpower," it scored the tortured phrase used in the text instead of the expected phrase, "artificial intelligence." Next slide, please.

So now we observed that we got the tortured phrases nowadays from the human evaluation, meaning that the readers detected phrases in the text manually and they collected all of those data that are called tortured phrases.

Now let's move to the solution part. And next slide, please. So this is the clear objective of what we want to do. The clear objective of the tool that we wish to create is that we aim to create a tool that automatically detects those kind of new tortured phrases in a sentence. So we plan to do it based on the current tool and current technologies, such as machine learning and the language model stuff.

Let's move to the next slide. It is an example. "It is commonly acknowledged that [FDR] is one of the essential wellsprings of capital in flow and driving components of financial development in many creating nations." So we want to create our tool to detect automatically that, “Oh, ‘creating nation’ here is not the legitimate phrase. It is the tortured phrase,” because the expected phrase of the “creating nations,” it should be “developing countries.”

And then move to the next slide. So this is my current study—just my project, my research. I try to investigate in various experiments, to differentiate the characteristics of the tortured phrases and the expected phrases in the sentence and in the paragraphs or something like that, based on the classification techniques and other language model techniques.

And that’s all for my presentation. The next slide will show the references. Thank you for your attention.

DEBORAH ESCALERA: Thank you. Are there any questions? Very interesting. Okay. Our final presenter is presenting remotely. And it is Kateryna Kryvko. Kateryna, very nice to see you. We are bringing up your slides now.

KATERYNA KRYVKO: Good afternoon, everyone.

DEBORAH ESCALERA: Wonderful. Okay. We’ll wait for your slides to come up and then you can begin. Thank you so much.

KATERYNA KRYVKO: Okay. Thank you. Good afternoon, everyone. Today I want to walk you through my recent research. It was a part of my translation internship, the topic of which is specifics of translation of Internet governance terminology into the Ukrainian language. Rapid changes in the world require us to be flexible and innovative, especially when it comes to Internet governance and cybersecurity. We are forced to make quick decisions that will help us to ensure stable, secure, and interoperable global Internet. Still, not all changes may be labeled as positive. Next slide, please.

As everybody knows, the devasting hot phase of the Russian war against Ukraine started on the 21st February and unfortunately is still not over. Because of the war—which, by the way, is often mistakenly mislabeled and called “conflict” or “situation” although there is a resolution of the United Nations General Assembly that clearly states that events that are taking place in Ukraine is a war—there is a threat of fragmentation of the Internet. And incorrect naming of events leads to false conclusions, which can lead to a split on the Internet.

Now we can see the tendency to refuse to use the Russian language, which will undoubtedly continue due to the war in Ukraine. And we have to ensure the safe existence of the Internet in Ukraine, showing support to the country which is being under massive attacks right at the moment. Next slide, please.

As more and more people get access to Internet, we should be interested in making the Internet a diverse and multicultural place. So translating ICANN materials into more than United Nations official language will enable greater competition, innovation, and consumer choice. Ukrainian language is one of the most widely-spoken and widely-used in Eastern Europe. That is why translation into Ukrainian can significantly contribute to the spread of ICANN's mission in engaging more people to join us on the way to establishing stable and secure Internet.

To support this tendency, I'd like to present a short analysis on specifics of the translation of some terms related to Internet governance. These are the terms that do not have direct equivalents in the Ukrainian language and therefore may appear complex and challenging to understand. One of the problems of translating materials into Ukrainian is using un-adapted Russian linguistic borrowings although the Ukrainian language provides ample opportunities for more accurate translation. Next slide please.

Multistakholderism is among one of the most difficult terms to translate. Right now, this word functions as a linguistic borrowing, meaning that the term was adopted from the source language, English, into the target language, which is Ukrainian in our case. By the way, there is also no Russian equivalent to this term. So therefore, this term has no authentic equivalent, even though translators have tried to use literal translation approach. However, it leads to conglomeration and confusion. So to standardize translation, we need to develop and disseminate it so the terms do not sound unusual but are a part of the language culture. Next slide, please.

The key term “Internet governance” also appears a complex one. And currently, there are more than five ways of translating this term, which shows that this term is not debated enough and there is no clear understanding of its meaning. Defining the phrase may be more straightforward than translating and standardizing it. Deciding on one way of interpreting term and adding each to the official glossary will make it simpler to complete further translation. Next slide, please.

Another example of a difficult-to-translate term is “ransomware attack.” Most commonly, it is mislabeled as a virus or named “virus extortioner.” So this term cannot be used as a borrowing in the interpreted text because it will not convey its full meaning. So the descriptive method is used for translation to give the reader a complete understanding of this type of digital threat. Next slide, please.

“Public interest” is one more term that I want to draw your attention to. Initially, this term has to show how beneficial and crucial to society is something. However, the difference in translating this term may slightly confuse the reader. Most interpreters use a literal translation approach here but it doesn't sound accurate enough so it requires competency and diligence.

That is why I invite translators of the same language pairs involved in ICANN work to unite to provide others with precise interpretation of source terms and texts. The complex terms need to be harmonized so the target text with their use is accessible to general public. In addition, each of the terms requires discussion by translators who specialize in Internet governance and want to contribute to developing a stable and secure Internet. Here, interpreters play essential part in spreading the word about ICANN and its great mission. Next slide, please.

But supporting multiculturalism, we will raise awareness of the secure internet and engage people with different cultural and academic backgrounds in ensuring a stable and fast Internet since those whose first language is not English are currently excluded from experiencing the full benefits of the Internet. Next slide, please.

As a NextGen, I have no doubt that we are capable of contributing to ICANN, engaging more stakeholders, and uniting under a common goal—one world, one Internet. Thank you so much.

DEBORAH ESCALERA: Very well received, Katy. Are there any questions for Katy? I see that there's a hand up which I cannot address because the person does not have a first and last name properly named in the room. So I cannot call on that hand raised. If there are no further questions, I'd like to thank everybody for attending today's session and remind you that most of the presentations will be posted to the website. And you will be able to access them at your leisure. If you have any further questions, you can also e-mail at engagement@icann.org. Thank you to our presenters. Very well-done today. You did an awesome and excellent job. Have a great rest of your ICANN74. You may end the recording. Thank you.

[END OF TRANSCRIPTION]