ICANN71 | Virtual Policy Forum – NextGen Presentations Day 1
Monday, June 14, 2021 – 14:30 to 16:00 CEST

DEBORAH ESCALERA: Okay, I'd like to thank everybody for joining us today. Good morning, good afternoon, good evening. Hello and welcome to the ICANN 71 presentation. My name is Deborah Escalera, I work for the public responsibility support department and I manage the NextGen@ICANN program. I will be your remote participation manager for this session. Please note that this session is being recorded and follows the ICANN expected standards of behavior. During the session, questions or comments will only be read aloud if submitted within the Q&A pod. I will read them aloud during the time set by the chair or moderator of the session.

Interpretation for the session will include many languages. Click on interpretation ICANN 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, our technical support team will allow you to unmute your microphone. Before speaking, ensure you have selected the language you will speak from the interpretation menu. Please state your name for the record and the language that you'll 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. All participants in the session may make comments in

the chat. Please use the drop-down menu in the chat pod and select "respond to all panelists and attendees." This will allow everyone to view your comment.

Please note that private chats are only possible among panelists in the Zoom webinar format. Any message sent by a panelist or a standard attendee to another standard attendee will also be seen by the session host, cohost and other panelists.

Okay, with that, I'd like to give a special thanks to my mentors who have been helping me with the students, helping them prepare in the weeks leading up to ICANN 71. They have done a fantastic job. Cherie Stubbs, Aris Ignacio and Dessalegn Yehuala. Thank you very much. They have been an incredible support to me, they have helped the students prepare for ICANN 71, they have been incredible mentors helping them get ready for ICANN 71, leading them through the process and getting them ready for today.

Our very first presenter is Daniil Golubev, and hopefully he's in the room and ready to go. Fernanda, my coworker, is helping me run the slides today. Thank you so much, Fernanda, for helping me and assisting me today. Daniil, are you in the room?

DANIIL GOLUBEV: Yes, I am, and I'm ready to present. Good afternoon, everyone.

DEBORAH ESCALERA: Okay. So I want to remind all of our presenters to speak slowly and at a reasonable rate because our interpreters will be translating everything that you say. And I'll remind you to just say “Next slide, please” for Fernanda. Thank you so much, Daniil, you may begin.

DANIIL GOLUBEV: Okay. Good afternoon, everyone, dear colleauges. I would like to do a talk about rather specific issue, about Russian digital technology association positions on Internet regulation and the general state of Internet freedom in Russia. Of course, it is rather specific issue, but it could be extrapolated from Russia to other countries. Next slide, please.

So in Russia, there are associations that aim to develop the Internet industry, so called Internet associations. Their [inaudible] of existence and the nature of their [inaudible] differ. The main criteria of selecting the associations for this presentation was that they position themselves as state independent. However, as I analyzed the work and the functioning of such associations, it may not appear to be entirely true, and in this presentation, I made an attempt to define associations’ positions concerning Internet regulations expressed via different means.

I considered such associations and organizations in Russia for this presentation: association for the protection of copyright on the Internet, media and communication union, regional public center for Internet technologies, Russian association of electronic communication, and Internet development institute. Of course, there

are much more associations in Russia, but I selected the most large and significant in the Russian segment of the Internet. Next slide, please.

I would like to give you some background about the Internet state of freedom in Russia. Russian authorities try to control Russian segment of the Internet as much as they can, and there are some cases about how Internet is associated with the government in Russia and [how it is] regulated there.

There is a Russian executive body called Roskomnadzor, which is censoring the Russian segment of Internet and blocking many sites considered violating Russian law according to Russian authorities. Much information is blocked in Russia because of this executive body.

Again, Russian citizens can be punished for making offensive comments about the authorities on the Internet. In Russia, recently, there were protests, demonstrations, and the mobile network shutdowns were often detected, [not without the] involvement of the government.

There are attempts to make the Russian segment of the Internet isolated from the rest of the world, so called sovereign Internet, or RUnet as we call it in Russia. And international companies working in the IT industry are obliged to store their data about Russian users on the territory of Russia so that the Russian authorities could have access to the data of Russian users. Next slide, please.

Okay, so the first association I would like to talk about is association for the protection of copyright on the Internet, or in Russian, it's AZAPI. It's a nonprofit partnership that aims to combat the illegal placement of

book and audio products on the Internet. So it is mostly associated with copyright problems. AZAPI participates in the discussion of draft laws related to the protection of copyright on the Russian segment of the Internet, and its clients include major Russian book publishers which strive to defend their copyright. Unfortunately, this association does not provide very satisfactory means to satisfy that demand. Next slide, please.

How did AZAPI interact with Russian government? In 2015, AZAPI appealed to the Moscow city court with a request to block the torrent tracker, RuTracker, which happened to store the objects of the copyright of the clients of AZAPI. So it didn't just satisfy it but it also happened to request to block the entire site, the entire torrent tracker, which unfortunately not really good for the state of the Internet.

In 2016, AZAPI has appealed to the Moscow city court with a request to oblige Yandex search engine—which is second most popular search engine in Russia after Google—to remove links to books related to RuTracker from the search, which were located there.

In 2019, AZAPI appealed to the Moscow city court with a series of lawsuits against the resource Archive.org, which stored digital copies of audiobooks by writers Dmitry Glukhovsky and Daria Dontsova in the cache, which were the clients of AZAPI as well.

And in 2020, AZAPI appealed to the European Commission to hold Google accountable for refusing to remove apps from Google Play that allow "massive copyright violations" on e-books. These sites were Ok.ru, Mail.ru, Telegram, YouTube, and WattPad. Next slide, please.

Next association is media and communication union, or in Russian, MKS. It was formed in 2014 by the largest players in the media and telecommunications industries. It's a nonprofit partnership of Russian media companies and telecom operators that serves as an intermediary between telecom and media market companies. Next slide, please.

Media and communication union has proposed several law in drafts to the Russian government in different years, mostly under the management of Pavel Stepanov, who was a president of MKS from 2016 to 2018. MKS proposed such [inaudible] as extrajudicial blocking of mirrors of pirate sites, blocking torrents a the UDP protocol level, restricting the operation of VPN services, regulation of messenger apps, and regulation of online movie theater operations. Next slide, please.

Another association is Regional Public Center for Internet Technologies, or ROCIT in Russian. It was founded in 1996. The members of the ROCIT board include representatives of government agencies and commercial companies. It receives funding from Russian Presidential Grants Fund. So it is indirectly funded by the government, even though it's a nongovernmental association. It aims to create a friendly Internet environment and popularize Internet technologies. It is positioned as a platform for interaction between users, business and the state, as well as for solving issues related to the IT industry. Next slide, please.

ROCIT is associated with the reaction of Russian authorities to the protests. In 2021, Russia witnessed massive protests against the

government, and it was heavily suppressed by the government physically and digitally. The reaction of ROCIT to the distribution of content by social networks according to the organization promoting extremist actions, such as this.

"ROCIT experts note a sharp increase in content materials directed against public safety on the Internet." In this message, they criticize the content which simply informs people about the protest activities. And they call the materials about protest actions extremist and even terroristic.

ROCIT appealed to social networks to stop the distribution of such content related to protest activity. ROCIT position coincided with the government one. Next slide, please.

Another association is Russian Association of Electronic Communications, or RAEC in Russian. It was founded in 2006. It is included in the list of recipients of state support in the field of electronic media, so it is also funded by the government. Among the major participants of the RAEC are Mail.ru Group, Kaspersky Lab, VKontakte, Rostelecom, the largest IT companies in Russia.

There are state-owned companies as well, such as inform agency Russia Today and news agency TASS. It's a nonprofit association of representatives of the Russian electronic communications market, which aims to consolidate the opinions of industry leaders and interact with government agencies. Next slide, please.

The position on the regulation of RAEC on the Internet can be expressed via Runet Award. It's an award organized by RAEC which marks the achievements in the industry of Russian segment of the Internet, and since 2011, the Runet Award has been filled with nominations related to the regulation of the Russian segment of the Internet, such as safe Runet, Internet without extremism, socially important projects, in particular, children protection, strengthening the digital immunity of the Runet.

In most cases, in these categories, the only winners were state-owned companies which aimed to censor the Russian segment of the Internet. In the categories related to the information content of the Internet, in most cases, preference was being given to state resources. Next slide, please.

The last association I would like to talk about is Internet Development Institute, in Russian, IRI. It was founded 2015 with the support of the presidential administration. However, it was still aimed as a nongovernmental association. It's an autonomous nonprofit organization whose main activity is the production of socially significant content on the Internet and work on industry-specific draft laws. It serves as an intermediary between members of the digital industry and government agencies, and it announces competitions for the production of videos on the subject of social advertising and patriotic content. Basically, it's like a market for content on the Internet, in Russian segment of the Internet, on social thematics. Next slide, please.

How did IRI participate in the digital industry regulation in different years? It proposed a list of Russian software for preinstallation on laptops and smartphones. It proposed an esports electives program. It proposed the development of a memorandum on social advertising. It proposed the creation of a safe digital environment for the younger generation. It proposed a creation of educational programs on digital technologies. And it also proposed a regulation of anonymizers in Russia, also included VPN. Next slide, please.

How are these associations connected? For these associations, there is no collaborative body working on Internet Governance issues. However, members of associations are present in one another. Basically, members of MKS are present in ROCIT as well, and Russian government is a member or some kind of influencer in some capacity of every association listed.

How is this related to ICANN? ROCIT and IRI are one of the founders of coordination center of top-level domains in Russia which maintains the functionality of top-level Russian domains such as .ru and .rf. So basically, through such nongovernmental associations, even though it is related to the government, the government can influence the policy of top-level domains and the work of every association. Next slide, please.

To sum up, first, many Internet associations, even though they are registered as non-profit and non-governmental, they are linked with state structures in Russia, receive funding from the state budget and work on state orders, and representatives of the government are

present in association and it influences the expression of opinions of such associations.

The reactions expressed by associations are reached by the majority of the members, which include Russian authorities. In most of the cases, they are positive, they support the regulation of the Internet. In very rare cases, they are moderately critical on certain issues.

And the third one, the associations themselves benefit from the regulations because they work on execution of state orders for the implementation of adopted laws. They are lobbying their interests when discussing or introducing draft laws, and they try to monopolize certain commercial fields by concentrating aspects around one association and weakening competitors.

To conclude, I would like to say that Russian government is trying to control as much Internet as possible, and associations are one of the ways for the government, for Russian authorities, to reach their goals, and even though the associations are not governmental, at least on paper, they are controlled by the government in some capacity. Thank you for your attention.

DEBORAH ESCALERA: Wonderful. Thank you, Daniil. Are there any questions for Daniel? You can raise your hand or put the question in the chat.

DANIIL GOLUBEV: There is a question from Pablo.

DEBORAH ESCALERA: Okay, Pablo, you can unmute yourself and ask the question.

PABLO BURDIAK: Yes. Hello everyone. First of all, I would like to thank you a lot, Daniil, for such a fantastic presentation and very informative. I am very interested in this topic as I am partially researching the Russian case as well, and I was wondering whether you could also provide some more details on whether there are Internet associations which are not directly linked to the government or indirectly linked to the government, meaning independent Internet associations.

DANIIL GOLUBEV: Thank you for your wonderful question, Pablo. Unfortunately, I was limited by the time, I was only allowed to present for ten minutes. Yes, there are associations which are totally independent, but they are not allowed to be legally registered in most of the cases, because in order to be totally registered, you need to comply with Russian laws and legislations. You need to find some compromise, and in most of the cases, it does not work.

There is an association called Roskomsvoboda. It works on the freedom on the Internet, and it is an authorized branch of ICANN in Russia in some ways. It strives for the freedom of the Internet and it tries to make the state of freedom of the Internet in Russia as big as possible. However, unfortunately, in most of the cases, they are not allowed to operate on official level.

DEBORAH ESCALERA: Okay. Thank you. And we have a question from Riccardo Nanni. Riccardo.

RICCARDO NANNI: Thank you, and thank you, Daniil, for your very interesting presentation, also very clarificatory because sometimes when we hear information about Runet, it tends to be quite a catchphrase and it's quite hard to gauge what it actually means.

So there's been some talk recently about the possibility, maybe, for Russia to establish a sort of Russian DNS. Is it just a general talk, or is there something more concrete that is potentially going to happen? Do you have a view on that? Thank you.

DANIIL GOLUBEV: Thank you for your question, Riccardo. Yes, there are attempts to make a so-called sovereign Internet, Runet, with Russian DNS. There are talks about it since, I guess, 2010 or something like this. Russian government and the IT specialists working for the government tried to establish so called independent Internet position of Russia.

However, their qualification is not quite enough. In 2017, Russia tried to block Telegram. It did not work. Telegram still operated in Russia. In this year, they tried to block Twitter. It did not work, as well, and now there are talks about blocking YouTube, which is quite ... I don't think

that will be possible, because the qualifications of IT specialist working for the government are simply not satisfactory.

Yes, there are talks about making it more sovereign, but I don't think that in the current state of Internet spread in Russia, it's possible to make situation similar to China. The worldwide community is simply too integrated in Russia segment of the Internet, and I don't think it will be possible on very large scale.

DEBORAH ESCALERA: Thank you so much for your wonderful presentation, Daniil. Okay, we're going to go ahead and move on to our next presenter, Weronika Slominska.

WERONIKA SLOMINSKA: Hello.

DEBORAH ESCALERA: As a reminder, you will have ten minutes, and if you're running over, I will make sure that I give you a warning. And again, please speak clearly and slowly. Thank you.

WERONIKA SLOMINSKA: Okay. Thank you. Hello everyone. Thank you, Daniil, for a very interesting presentation. I'm Weronika, I'm studying international public management, and today I would like to talk about cybersecurity

and related challenges for policymakers in this field and the need for improving awareness on the issue. Next slide, please.

Thank you. So cybersecurity is a topic that keeps growing in scope and frequency all around the world. New types of cyberthreats are constantly emerging and cyberattacks can have very severe consequences on all people and organizations, which means that the issue really needs to be taken care of using a top-down approach.

Cybersecurity is a highly multifaceted issue and it needs cooperation of both people that are dealing with its technical aspects as well as governance, and that's the angle I will take today.

In the world of Internet of Things, more and more physical objects feature an IP address for Internet connectivity and communication, which means that the society is more dependent on cyberspace. However, even though managing cyberspace is so crucial, governments don't seem to do enough to ensure its safety and cybersecurity doesn't really get the attention that it requires. Next slide, please.

That's because policymaking in the field of cybersecurity is facing many paradoxes, first of which is that governments want to ensure cybersecurity, but on the other hand, they want the data of citizens for surveillance purposes. So on one hand, governments want the citizens to protect themselves, but on the other, they don't really want them to use encryption and other cybersecurity measures, because those matters can be also used by criminals and terrorists.

Another paradox is that cybersecurity is a truly global phenomenon and it cannot be handled within national borders and it needs transnational cooperation. But some governments don't even trust each other and they're not willing to cooperate. They might even be hacking each other. So this makes it complicated.

Another very important paradox is that there is no set right amount of government spending on cybersecurity, because too little spending doesn't ensure enough protection, but too much spending can send a message that something very concerning, something very wrong is happening, and it may create fear. So ensuring the balance is very important. Next slide, please.

So, four main causes have been determined explaining why policymaking in the cybersecurity field is so challenging, first of which is limited visibility. Since the impact of cybersecurity breaches is often not visible in the physical sense, and the topic is not easy to explain to the public, the public doesn't really feel the impact of the problem. So it's hard to make policies to organize something new on something that is not visible.

The second problem is that the social technological complexity of cybersecurity, because while IT infrastructure and policies are crucial in ensuring cybersecurity, the main role is played by humans which are responsible for maintaining the systems and implementing policies, but a lot of people and organizations lack awareness or they don't even have resources to take action.

the third problem is cybersecurity's contested nature. Attackers are mostly anonymous, so it is unclear who the enemy really is. And the fourth challenge is the ambiguous impact. So it is difficult to judge cybersecurity risks in advance, and it's even more difficult to measure the impact of new cybersecurity policies, which makes it difficult to call for investment. Next slide, please.

As we can see, there is a lot of ambiguity and lack of awareness on cybersecurity, which leads to challenges faced by policymakers. So, what can be done to tackle them? Next slide, please.

Researchers have come up with a concept of message framing, which is communicating a complex problem in a simple and convincing manner. Since policymakers and specialists are often criticized for not being able to convey their message to explain it to the public and since cybersecurity is a very complex phenomenon, very long and difficult to explain, it has to be reduced to a simple message capturing the essence and showing the importance of cybersecurity to the people. Next slide, please.

Researchers propose a strategy for cybersecurity message framing in order to raise people's awareness on cybersecurity consisting of six steps or rules, first of which is not to exacerbate cybersecurity, not to exaggerate the risks, to put it in a really realistic perspective, because exaggeration will only make the problem worse.

The second rule is to make it clear who the villains are, who are we really fighting with, who the enemies might be, who can we expect a threat from.

Third rule is to put the heroes in the spotlight, so demonstrate who, for example, in the country is protecting cybersecurity, what are their capabilities, successes.

The fourth rule is the show the cybersecurity's importance for society, so to connect the need for improving cybersecurity with economic growth or national prosperity.

The fifth rule is to personalize and connect cybersecurity to daily life of people, so to demonstrate how it can affect people's everyday life, in what ways.

And the sixth rule, the last one, is to connect the two other issues that are interconnected with cybersecurity, such as politics.

And the next slide is a thank you to all of you. That's all for me. Thank you.

DEBORAH ESCALERA: Thank you, Weronika. Very well presented. Do we have any questions for Weronika? Any questions in the chat or anybody want to raise their hand? Okay, thank you so much. If you have any follow-up questions for Weronika, you can e-mail us or e-mail her directly. We can provide her e-mail, or you can e-mail us at engagement@icann.org.

Okay, so the next person, who was not able to make the presentation today, is Antronos Mulugeta, and he wasn't able to make it today, but he submitted a video presentation. I've never done this before, this is

new, so I'm going to share my screen and see how it goes, and hopefully everything will go okay. Can you see this?

ANTRONOS MULUGETA: Hello everyone. I am Astronos [inaudible]. I just want to say if you have any question, any suggestion or comment, please use my e-mail address to contact me [inaudible] e-mail address, so if you have any questions about this presentation, you are really welcome.

So when it came to a topic that would be [inaudible] how can we help ICANN with artificial intelligence? [inaudible] to make it more specific and say applying artificial intelligence on the domain name system security. So [later I tried to see] when this domain name system was invented. It was invented in 1980 without any protection to ensure the data or [inaudible].

So, by that time, the Internet wasn't as wide as today or as big as today, so they didn't concern the security issue or they didn't much concerned about the protection, so they just made it without protection. But nowadays, as Internet becomes wider and bigger, [inaudible] and also, this allows the attacker to divert users from the intended destination to those of an attacker's choosing.

So when the Internet Engineering Task Force first looked at this problem, they tried to provide a solution, so they invented the DNSSEC, which is the domain name system security extension, which is to strengthen the data origin authentication, data integrity in the domain

name system by using the digital signature based on the public cryptographic key.

Let me say [inaudible] data origin authentication, data integrity, when I say data origin authentication, it means—when I say domain name system in the first place doesn't provide the data origin authentication, it means that domain name system doesn't provide assurance that the data associated [inaudible]. And when we say in the first place it doesn't [inaudible] data integrity, it means that it doesn't provide [inaudible] if the data in the domain name system response has been modified or changed. So in the first place, this domain name system wasn't so secured, as we can see. But after the DNSSEC was implemented, this domain name system extension provide the assurance of the data origin authentication [inaudible] data integrity, so it becomes more secure.

But when we see how this domain name system extension works, it isn't automatic. It's supposed to be enabled by the operator and also by the domain name system owner. That means every domain name owner has to know about this domain name system extension to make the Internet more secure.

There are different domain name owners, there are businesspeople for example, [inaudible] use example to explain [inaudible] website that has a domain name, a business website that he uses to sell his products. So this guy, as I said, is a businessman, so he doesn't have that much knowledge on the technical part, so that means he can't enable the

DNSSEC [inaudible] for the security purpose. That means the hackers can use the same page as [he created and take his] customers.

So my idea is to protect those people, why don't we make this system automatic? I think we apply artificial intelligence and make this system automatic.

When it came to this part, I think there are people who are outside of the technical [part,] so when you try to explain what artificial intelligence is and what machine learning is, artificial intelligence is like a wide branch of computer science that's concerned with building machines or systems which can perform tasks that require human thinking ability or human reasoning ability.

So from this [inaudible], I just want to introduce a specific part to apply on this area, so I just choose the machine learning artificial intelligence. So when you see what machine learning does and how it works, this machine learning, this part of artificial intelligence works by training machine [to perform this machine learning to a specific part] which is supervised learning. Supervised learning is one part of a machine learning which is used to label data or define data, with defined data, train a machine.

So, I know this is a most technical topic and a very complicated topic, but let me try to just mention a few words, how can we apply this machine learning or artificial intelligence? I think we can train a machine to just [sense when a] new domain name system is registered, then automatically [enable] the DNSSEC to improve the domain name system security.

So my idea is to make a machine that can sense when a new domain name system is registered and automatically enable DNSSEC without the need for enabling by the domain name owner and by the operator. I think this would improve the Internet security.

So my research is—I didn't get into conclusion, but I'm still working on it, so my research is whether we can make it automatically enabled by using this machine learning or not. So [I want to] see what others are doing on this area, on the Internet security area to make the Internet more secure. Different experts are working on how to apply machine learning to detect [inaudible].

I know this is a bit complicated and this is a more technical [inaudible] algorithm is like one of the algorithm [inaudible] which his for the registration and classification [inaudible] and they are also using—additional information, they are also using Python as a coding base.

I know we can't cover this vast topic with these [given] minutes, but this is all I have for today. If you have any question, as I mentioned in the beginning, you are very welcome to contact me via my e-mail address. Thank you very much for [inaudible] and also, I have a special [inaudible] so I'm preparing my presentation. Thank you, all of you, and have a great day.

DEBORAH ESCALERA: Okay. I think that was a little difficult for the interpreters, so that portion will not be on the transcript. And I think there was some questions for Weronika that I missed. So, did somebody have a question

for Weronika that I missed? Can you raise your hand? Anybody? Okay, if there's nothing else, I'm going to move on.

Our next presenter is Veronica Piccolo. Veronica, are you online?

VERONICA PICCOLO: Yes, I'm here.

DEBORAH ESCALERA: Okay, Veronica. Again, you have ten minutes, and just speak slowly and clearly. Welcome, veronica. Thank you.

VERONICA PICCOLO: Thank you. Welcome, everyone. I'm going to talk to you about a case law rendered by two Italian courts in 2019 and 2020 in matter of intellectual property rights protection, and specifically on how those decisions can hamper the Internet integrity of the Internet and the critical properties of the so-called Internet way of networking. Next slide, please.

This is the agenda. I will give you a little bit of background and I will talk about the Internet way of networking, and explaining then what dynamic injunctions are and the impact on the critical property of the Internet, on the Internet way of networking, and then I will do my call to action. Next slide, please.

So, a little bit of background. In 2019, an Italian media company sought an injunctive relief against Cloudflare. Cloudflare is a provider of

content delivery network services, DDoS mitigation, Internet security and distributed domain name server services.

The Italian company  claimed that Cloudflare customers were illegally reproducing many of its TV shows, and this demanded Cloudflare to remove or disable access to those websites.

In such cases, the Italian regulation forces that the Internet intermediary service provider must terminate or prevent the infringement only when required by a national court or an administrative authority.

In 2020, we had a similar complaint issued by the national football league and Sky Italy for illegal live streaming of football matches. In this case, the remedy was hard because Cloudflare was ordered to disable its content delivery network services towards some of its customers. Next slide, please.

So, what's the Internet way of networking? The Internet way of networking states it’s a project undertaken by the Internet Society which states that the Internet owes its success not only to the technology per se but to the way it operates and evolves.

When you come to think of it, we can do many activity over the Internet. We can study, we can connect, we can share, we can organize thanks to the Internet. And we do it because the Internet grows that way, and we need to recognize what makes the Internet useful for everyone until now. So the Internet society developed five critical property that are more ethical principles than technical properties. Next slide, please.

Okay, the first property is accessibility. In other words, whatever country you are from or you are in, you will always be able to connect to the global network. What you need is a device and an access point and you are on the Internet. You can reach out to or work with everyone in the world.

The second property is openness and interoperability. We must think of the Internet as a LEGO house. We can have a block over the underlying structure, and we know that this block will always fit, allowing permissionless innovation everywhere and always.

The third property is decentralization. We know the Internet is a network of networks. Each independent network chooses to connect with the others and each one of them benefits from belonging to the same network.

The fourth property is common global identifiers. In other words, a common language to understand the IP addresses and the way in which packets of data are delivered from point a to point B.

The fifth property doesn't need introduction, because it's net neutrality. Next slide, please.

So in my country, there is a trending practice to fight online piracy which consists of demanding the court to shut down not only currently active pirate websites but also future websites that may have the same second-level domain. We call this alias or aliases.

In other words, whatever top-level domain follows that same second-level domain, whether existing or to be activated, it would be subject to

shutdown. It's peculiar also because dynamic injunctions are self-enforceable. When infringing content is mirrored in alternative website with the same second-level domain name, the intellectual property rights owner won't need any further court order. He will go straight to the Internet intermediary service and ask them to shut down.

And the dynamic injunction affects not yet existing infringement and possibly websites displaying legal content. And above all, if infrastructure operators don't comply with the order, they can be deemed liable for damages. Next slide, please.

In the case, the court ordered Cloudflare to disable its content delivery network service in a targeted way, so targeting specific IP addresses or domain names.

So, what I'm doing about this topic is to explore which of the five critical properties are being impacted by this case law. I've also investigated property two and three, but I know that this case surely impacts on property five, that's net neutrality, because infrastructure operators cannot be deemed responsible for the content their customers send over the Internet and neither they should be asked to control the data and perform targeted content delivery.

This is most true when we think to what happened last week with Fastly content delivery network service provider. Many of the websites were in blackout for an hour. Next slide, please.

Okay, my call to action. This is an issue that is worth discussing at every level, at ICANN policy forum, within the ICANN community, at the IGF,

whatever community or stakeholder are being impacted by such decision or such case law that it's widespread in my country, but I know that also other jurisdictions have been trying to take inspiration by this case law.

So, what I'm going to do is start observing if some related issue has been discussed within the GNSO and specifically by the Internet service providers constituency and the intellectual property constituency, to understand what they are doing, what they think, if they know about this. And if not, if there's any representative from those stakeholder groups, please be aware of this issue.

I think that my time is up, so I will ask Deborah to go to the next slide and wrap up. Thank you for listening.

DEBORAH ESCALERA: Thank you, Veronica. Very well done. Do we have questions for Veronica? I don't see any hands up or questions in the chat. Good job, Veronica. Okay, I want to make sure I don't miss it this time. Okay. Wonderful. Good job. We're going to move on to Shivam Sharma, our next presenter. Hello Shivam, welcome. Okay, you have ten minutes, and as a reminder, please speak slowly and clearly. Thank you.

SHIVAM SHARMA: So basically, I'm going to discuss about the cybersecurity of IoMT devices. Next slide, please. What is IoMT? IoMT stands for Internet of medical things. It's a subset of IoT technology which is Internet of Things. It's a collection of healthcare devices which include sensors,

healthcare [inaudible] applications which are connected to the Internet and which send patient data to a cloud that can be remotely accessible by the health practitioner or doctor which can reduce the chances of [inaudible]. Next slide, please.

So these are some of the IoMT devices, like personal wellness, like smartwatches, like fitness bands, and some clinical-grade wearables like for monitoring diabetes or like measuring blood pressure. So these are some clinical wearables.

Next is digital pills. These are pills which contain sensors inside them and reach into the stomach of the patient [inaudible] and starts sending data outside of the body, which can be viewed through a device like a smartphone or a t ablet by which the health practitioner can [inaudible] some more details about exactly what's going on inside the body.

Next is automatic wheelchairs. These are some automatic wheelchairs which are automatically controlled. Next is telehealth. Telehealth is seeing a doctor that no longer requires physical interaction. So basically, in this case, it doesn't require a doctor to visit a patient physically. For that, there are some different [kiosks] or some kind of videoconferencing services by which a doctor can see details of the patients and provide health consultation remotely.

Next is mobile retina camera. These are some contact lenses which can be worn in ice, so they provide all the data to the smartphone or some kind of portable device. Next we have some robotic surgical instruments. Basically, these devices are used for endoscopies and laparoscopies. This provider or doctor who stream inside view of body

so that they can get more view of parts of the body through these cameras.

Next is portable pathology. We don't have to visit a lab for testing, so we can use some device at home to collect the data from patients. Like if we are going to perform a blood test, we can take a sample at our home and the devices collect all the data and upload to a cloud from where the doctor can access all the data.

Next, these are some [inaudible]. Next slide, please.

DEBORAH ESCALERA: Shivam, I'm sorry to interrupt. Can you maybe adjust the volume on your computer or your headset? We're getting a lot of feedback and static. I'm not sure what's going on there.

SHIVAM SHARMA: Sorry for that. Let me change my headphones.

DEBORAH ESCALERA: Okay, thank you. Are you using a headset, Shivam?

SHIVAM SHARMA: Yeah, I'm using a headset.

DEBORAH ESCALERA: Okay, good. Thank you.

SHIVAM SHARMA: Am I audible?

DEBORAH ESCALERA: Yes, please proceed. Thank you.

SHIVAM SHARMA: So now, it's IoMT architecture, so how these IoMT devices work. So basically, they are different sensors that are [inaudible] in the body of a patient, like some [vital] sensors, like blood pressure or like rising diabetes or some smart fitness band which collect the data through sensors and then transmit that data to a device which further transmits either through Wi-Fi or some kind of telecommunication method like 4G or 5G and that forward the data to the cloud from where the doctor can access all the data and provide a health consultation to the patient remotely. Next slide, please.

So, as we look at the growth of IoMT devices, according to a report by AllTheResearch, in 2018, IoMT market was worth 44,000 million and it's now growing at a rate of 24.4% year over year during the period of 2016 to 2026. And in 2026, it is expected to reach around [$254 billion.]

So during the forecast year, the smart wearable category is likely to dominate in the market. So in 2018, the worldwide IoMT market was dominated by smart wearable devices which accounted for around 27% of the market. Point of care kits had the largest CAGR of all, 30% in the global IoMT market, and the real-time monitoring application predicted to increase at a CAGR of [25%.] Tracking and alerting

applications will increase with a CAGR of [21%.] So basically, CAGR is just compound annual growth rate. Next slide, please.

These are some benefits of IoMT devices, like this cuts down the medical costs. So, suppose a patient is suffering from some kind of common disease or that doesn't require any immediate hospitalization, so the doctor can provide a remote consultation through Internet. All the data will be forwarded to the cloud. From there, the doctor will access the reports and provide a health consultation remotely. So it will reduce the chances for hospitalization and also reduce the cost.

Again, it will also improve the patient experience, so there is nothing to ... Patient doesn't have to worry about anything, so he or she doesn't have to go visit a doctor. Next is enhanced manageability of medical drugs and medical adherence. It will provide a proper management, so the smart devices will be able to manage all the things automatically and provide a good experience, and also, these devices reduce the chances of errors, because these devices have good accuracy, so that will provide a good result, and it will also provide better control over the wastage in the healthcare sectors because a lot of things are going wasted. So it will also help to reduce some kind of [inaudible] and it will provide more efficient services which will result in better outcomes of the medical treatment. Next slide, please.

Some of the disadvantage of IoMT are like as Internet is g rowing, there will be chances of some kind of security breaches or cyberattack as day

by day, some kind of cyberattacks are increasing. So these attack and infect devices.

And the management of EMR basically, electronic medical records, is challenging because if we are collecting the data of patients, we will have to follow some kind of compliance like HIPAA, FHIR, so this is really a time taking process to comply with all the standards. And in Europe, there are some rules like GDPR so we have to make sure that we are following those rules. And there are some medical standards like FHIR and SMART. These require some more time for implementation. Next slide, please.

Some of the risk associated with IoMT devices, like to develop these devices requires a long development lifecycle, so basically, if we made a device, we have to make sure we are continuously updating it through some kind of patches and having some updates to make it more secure.

The main aim of these devices is patient safety, so [not] security, but nowadays, as technology is changing day by day, so it will improving the security of these devices also. And there are some devices, like take the example of Fitbit, it uses Bluetooth technology to communicate, which can be hijacked by a hacker. So we can collect all the patient's data, including location and all the health details, which can impact the patient.

And some of the devices have a hardcoded password, which is another major risk which can allow hackers to easily hack those devices if they are able to get access to these devices, so they are easily able to collect all the data from the device.

And unencrypted communication. The communication is going in unencrypted form, so it will be chances that it can be read by a third party like by man-in-the-middle attack which can read all the data.

Next is lack of device management. Basically, to manage these devices, we should make sure that we are following all the requirements and we are continuously updating all the devices and our staff is trained properly how to deal with if there is a cyber breach or some kind of cyberattack, so how to deal with that situation. Next slide, please.

These are some kind of attacks associated with these devices.

DEBORAH ESCALERA: Shivam, you're over time so we need to wrap it up, please. Thank you.

SHIVAM SHARMA: Okay. So basically, these are attacks—so I'm not going to explain this, I'm limited of time. So these are attacks like tag cloning, tampering and eavesdropping, attacks that can impact IoMT devices. Next slide, please.

How to improve the security of these devices? We should not use [inaudible] device passwords, we have to update these passwords to some strong credentials, we have to provide some patching timely so that if there are any security vulnerabilities, they will be fixed timely, and make sure that our network is more secure so that it can stay away from any unauthorized network access. And there may be chances that our employee can use these devices for some kind of bad purpose, so

make sure that we whitelist according to the requirement. So suppose an employee is not using a device, make sure we don't allow them to access those devices, and make sure that these devices should be monitored [24/7] so that if any malicious activity starts, it will be stopped immediately.

Next is lack of containment. [It's not only important to repel attacks.] We have to make sure that we are able to handle the attack before it's going to happen, so we have to make sure our infrastructure is secure. Next slide, please.

In future, there may be challenges that it will improve]the healthcare infrastructure, so there will be more devices coming in next few years. This is all. Thank you so much for your time. If you have any question, please.

DEBORAH ESCALERA: Thank you, Shivam. Looks like Riccardo has his hand up. Riccardo, what is your question?

RICCARDO NANNI: Thank you. Thanks, Shivam, for your very good presentation. I'm not an expert in IoT, but I'm curious about it, and I read that IoT has pushed a lot of development of non-IP forms of connectivity, of interconnection, networking. Does that carry the same kind of security issues of IP connectivity for IoT, or are they qualitatively different? Thank you.

SHIVAM SHARMA: Actually, can you post your question on chat? I think my headphones are not working.

DEBORAH ESCALERA: Okay. Thank you. And then Daniil, can you do the same? Because we've run a little bit over time and we only have very few minutes left and I want to make sure that Riccardo has a chance to present and have time for questions. So Daniil, if you can post your question in the chat as well, I would greatly appreciate it.

So our final presenter is Riccardo Nanni. Riccardo, you're next, and please keep in mind we're going to do ten minutes and then we'll use the final five minutes for your questions. Thank you, Riccardo.

RICCARDO NANNI: Thank you for the floor and thank you for having me. I'm sorry, I don't have a real headset but I'm trying to reduce any type of feedback by having headphones. I will be talking about Internet fragmentation from the general, down to a case study, back to the general implications. Next slide, please.

All right, let's start with some definitions of what we mean by fragmentation. [Some started by] defining it in many different ways as the different availability of information and services in different places under different rules. This of course would be a very broad definition and would treat fragmentation as a very catchall phrase. For example, would we argue that we're facing Internet fragmentation when we can't access the same Netflix content in Italy and in the US? There are

regulatory implications, there is some sort of market fragmentation, but to call it Internet fragmentation would probably be a very big stretch of the imagination.

So some definition tried to create taxonomy of fragmentation, governmental, commercial and technical for example. Others tried to incorporate the concept of net neutrality and check if it had anything to do with Internet fragmentation. Next, we have the strictest definitions of Internet fragmentation as incompatibility of basic standards, protocols, different IPs, different noncompatible transport protocols, whereas [inaudible] would take another name, another label.

So these are all the taxonomy, many different definitions of fragmentation that we have. And I tend to focus on the technical one, giving all the other phenomena a different name. Next slide, please.

So to show what I mean when I talk about fragmentation and to show why at least at the technical level, we can be optimistic about the Internet remaining overall unified. I'd like to show you a case study made on Chinese stakeholders and their engagement at ICANN and more in general in their engagement in the governance of unique identifiers.

Of course, when we talk about fragmentation, we tend to talk about many great powers, not just China. Can be Russia—we've talked about Russia today—but some people also accused some US-based projects of favoring Internet fragmentation. I simply take China because that's my geographical field of expertise, so it's the one in which I'm stronger.

Observing Chinese stakeholders, we see that at the beginning of ICANN's history, China seemed to take a very confrontational stance towards ICANN. When it came to the recognition of Taiwan as a member of GAC, on which form with which name, the Chinese government stopped participating in ICANN activities. However, private organizations or public organizations, even state sponsored ones, kept being present.

And then for many years, actually, Chinese stakeholders and the Chinese government kept participating in ICANN and they became big promoters of internationalized domain names, which of course carry a lot of interest, economic and political, and cultural in the Chinese character namespace.

Initially, there was some quarrel between ICANN and China on who should have the lead on Chinese character domain names. So there was even the fear that China would establish a separate DNS. But that didn't happen, and actually, Chinese stakeholders are fully involved in ICANN, in IDN work.

And here is when we see a [inaudible] between ICANN and China. China gets back participating fully into the Governmental Advisory Committee, it hosts a big ICANN meeting in Beijing in 2013, and in 2014, the then president of the cyberspace administration of China endorsed multi-stakeholderism at ICANN 50. Next slide, please.

And this of course had implications on Chinese stakeholders' stance on aspects related to Internet fragmentation and the governance of unique identifiers. We see for example that after the IANA transition, the

China GAC representative becomes vice chair, signaling stronger involvement for the Chinese government as well. And meanwhile, Chinese stakeholders, even private ones like Huawei, became increasingly influential in other fields related to critical Internet resources and unique identifiers, such as the IETF.

However, new geopolitical conundrums emerged at the ITU, a multilateral [venue,] when Huawei, the ministry of industry and information technology and other Chinese actors presented the so-called new IP proposal.

But despite these forms of ambiguity, we see that Chinese stakeholders have become increasingly involved in ICANN. And with the next slide, I will show you the implications of this. Next slide, please.

Okay, what we have now is that after all those years of confrontation, the Chinese stakeholders, including the Chinese government, became more involved in ICANN. They used the same DNS and protocols as other countries. They participate in ICANN. They are influential in the IETF. And skipping all the methodological parts, but I mainly used qualitative methods, including expert interviews, to collect this data.

The reason why this happened is because powerful global companies, powerful global actors want network benefits. Split standards would force companies such as Huawei to produce different devices for different markets as they should be able to connect to different non-interoperable standards, whereas it's much easier for a global company to be able to produce one type of device on a global scale. This is much more profitable.

So, what can happen is that states like China, like Russia, may tend to have a stronger influence in domestic regulation, in what can go on in the Internet, on what kind of activities citizens can conduct on the Internet in order to cast their political influence while leaving standards alone in a way to allow domestic companies to thrive. And this is what the kind of steps that China took in its engagement in ICANN, the IETF, and critical [Internet resources] and Internet governance at large, one may say. Next slide, please.

So what we see now is that technical Internet fragmentation is a weapon of the weak, whereas strong actors prefer to retain network benefits. Maybe they want to be able to control traffic, especially when it comes to information and when it comes to civil society getting organized. But when it comes to technical standards, they want to be able to produce the same devices everywhere and market them everywhere and retain [inaudible] network benefits.

What does it tell us about Internet fragmentation? It tells us that the most powerful actors are trying to have an interest in keeping the Internet unified and that only the weakest actors may be trying to fragment the Internet at the technical level. And this makes the Internet, again, IPs, TCP/IP, the very technical core of the Internet a very resilient one. After all, China has a strong censorship, but at a technical level, all it takes to overtake it is a VPN. Of course, this can be very politically dangerous, to use a VPN in some contexts, if you belong to some groups for example, for example, it is the case if you belong to the Uyghur population for example. But at the technical level, all it takes is a VPN.

So this is good news for the Internet remaining unified at its technical core in a way. And while there remain instances of contestation, instances of ambiguities, instances of geopolitical clashes over very essential aspects of the Internet even at the technical level, the system as it is seems to display some resiliency. Next slide, please.

And this is my conclusion. Thanks for your attention. I'd be happy to answer to your questions.

DEBORAH ESCALERA: Okay. Thank you, Riccardo. Are there questions for Riccardo? Any hands or anything in the chat? Daniil, go ahead.

DANIIL GOLUBEV: Thank you, Ricardo, for your wonderful presentation. It was extremely knowledgeable and coherent. I would like to ask about what is your possible prognosis about the future state of fragmentation. Do you think that unification of the Internet will prevail, or maybe your prognosis will not be so optimistic and some segments will become isolated and fragmented. Thank you.

RICCARDO NANNI: Thank you for your question. That's actually a very relevant one. I'd say there will be some form of market fragmentation, as in many western countries not wanting, for example, Chinese actors in their domestic infrastructure, even the more telephony-related one like for example 5G and vice versa. So there might be a market fragmentation. But when

it comes to the standards, I see a convergence trend, and this has been the case both on IP and DNS, but also on 5G for example.

When it came to 3G, there were many more incompatible regional standards or national standards. Even if they were recognized by the ITU, they were then only deployed at the local level and were not interoperable with the standards of the same generation deployed elsewhere in the world and still recognized by the ITU where now we have a much stronger convergence in this sense. We have three 5G standards, but they are interoperable, at least this is what the ITU said when they approved it.

So there's a convergence in standards because as I said, big companies prefer to be able to produce devices globally, and rather than having their own standards in a way, they want to have big, important [chance] in terms of patents of the global technology and then be able to market devices and networks everywhere benefiting from global [scale] economies.

But at the same time, what we can see, again, is a commercial fragmentation led by governments, and we can see a trend towards stronger regulation. This is true in Russia and China where we see the government becoming more and more influential in censorship, in data localization regulations, but also in Europe and the US, the Trump administration has been very interventionist—look at the clean network project for example, but look also at the European Union. GDPR is a very advanced data protection regulation, but it has also strong extraterritorial effect.

Now, of course, for me as a European Union citizen, that's very desirable. I feel very protected by GDPR, so I'm totally supportive of it and not criticizing it. All I'm saying is that the European Union is also trying to carry some weight in the digital market and in the future development of digital technologies, and that also includes future Internet standards because Internet standards will have an impact on the future development of artificial intelligence, for example, and vice versa, and artificial intelligence is also [deeply entrenched in] 5G, both with 5G as an enabler of artificial intelligence and vice versa, artificial intelligence incorporated in 5G networks.

So if you have a strong control on data, you also have a strong leverage when it comes to any form of artificial intelligence development, because data is really the raw material.

So long story short, stronger state intervention at the regulatory level, possibly also in terms of information control, this is at least what we see in China and as far as I understand, in Russia, but I'm no expert on Russia. But a convergence of standards. I hope this answered your question. Also, it was very roundabout in some points.

DANIIL GOLUBEV: Yes. Thank you very much.

DEBORAH ESCALERA: Okay. Fantastic. We are right at the top of the hour. Thank you, Riccardo. Excellent presentation. And to everybody who presented

today, all of our NextGen, excellent job, fantastic. I'm so proud of all of you. You did a wonderful job.

I'd like to thank everybody who attended today. Thank you to Fernanda Iunes who ran the slides today. Thank you to our interpreters, and of course, our fantastic tech team who supports us throughout the meetings, at every meeting. And please join us for part two of the NextGen presentations tomorrow, taking place at 8:30 UTC, 10:30 CEST time. Thank you to everybody. I appreciate your support and I appreciate you attending today's part one of the NextGen presentation. Good job, everybody. Fantastic. Thank you for being here. Any questions, please send them to—

CHERIE STUBBS: Thank you, Deborah.

DEBORAH ESCALERA: Thank you. Engagement@icann.org if you have any additional questions and follow-up questions for our presenters. Thank you so much for being here today.

CHERIE STUBBS: Bye all.

**[END OF TRANSCRIPTION]**