ICANN84 | AGM – Middle East Space Session
Wednesday, October 29, 2025 – 15:00 to 16:00 IST

CHRISTIAN WHEELER: Hello and welcome to the ICAN84 Middle East Space Session on Wednesday, October 29th. My name is Christian Wheeler and I am the participation manager for this session. Please note that this session is being recorded and is governed by the ICANN Community Participant Code of Conduct, ICANN Expected Standards of Behavior, and the ICANN Community Anti-Harassment Policy. During this session, questions or comments won't be read aloud if submitted properly within the chat. If you'd like to speak during this session, please raise your hand in Zoom. When called upon, virtual participants will be given permission to unmute in Zoom. On-site participants will use a physical microphone to speak. Please state your name for the record and speak at a reasonable pace. I'll now hand the floor over to Amin Hacha. Please begin. Thank you.

ABDALMONEM GALILA: Thank you very much. This is Abdelmanam Galila for the record. I am the co-chair alongside my colleague Amin, who will share the session for today. Actually, the DNS Abuse topic is one of the topics that adds a stage of ICANN in many communities like ccNSO, SSAC, GNSO, GAC, and other communities within ICANN space. Actually, also, the DNS Abuse topic was discussed in a statement in 2021 by the Middle East Space, but at the moment, we're combining one of

the emerging technologies, which is artificial intelligence, in order to mitigate such a topic or such an issue of DNS Abuse. Actually, at the start of the session for today, I need to welcome all of you for the session on Harnessing Artificial Intelligence in DNS Abuse Mitigation. Actually, we use new technologies like AI in order to mitigate such proactive and active risks that could attack your organization from the point of view of the five categories of DNS Abuse categories.

As our region for the Middle East advances rapidly in the digital transformation projects carried out by the government, and from e-government services and fintech to smart cities and the national cloud infrastructure, the domain name system as a foundation remains invisibly unsecure or invisible foundation. It is risky. It could be attacked. It enables DNS, enables every digital services, every digital transaction, and identity online. But this foundation of the DNS is increasingly under attack. DNS Abuse will have five main categories, phishing, botnets, malware, and domain hijacking. And all of these categories of DNS Abuse threatens not only businesses, but also affects the national security and public trust. At this time, we have AI that becomes a buffer alley, buffer alley for both two directions. The first direction to mitigate DNS Abuse as a proactive one, and also to encourage or assist attackers in order to go for DNS Abuse mechanism. I will stop at this moment and open the floor for my colleague, Amin, who is the co-chair of Middle East Space. Amin, the floor is yours.

AMIN HACHA

This is Amin Hacha speaking for The Record. Good afternoon, everyone, joining us in person or virtually online. It's a pleasure to welcome you all in the Middle East Space session at ICANN 84. As many of you know, this space is a platform for our region community to share and update exchange experience and discuss how global Internet policy connects with our local priority. I would like to extend my warm welcome to all the speakers and for all the participants with us, share your insight and experience, and make this discussion more meaningful. I will move now to listen to our friend, Seher Sagiroglu Ayhan. She is GSE of Middle East Manager of ICANN, and she will tell us more about the Middle East.

SEHER SAGIROGLU AYHAN

Thank you, Amin. Hi, everyone. Welcome to Middle East Space session. Today I am here to give you a brief update from Global Stakeholder Engagement Middle East region. Can we move slides? All right. Many of you know our team. When I look into this room familiar faces, and many of you know our Middle East regional team. So I am working with Bahar Esmat and Fahd Batayneh. We are working to strengthen our relationship within the region, more than 24 countries. We are also trying to expand technical capacity and grow regional participation in global Internet governance. Can we move on? So for those who are attending Middle East Space session for the first time, I really wanted to give a brief explanation about what GSE function is and what we do in the region. That's why we have this graphic. This graphic shows the growth of our engagement activities in the last five years. As I said, we are providing outreach

and engagement services in the region, and when we look into these engagement numbers, you will see that we have more than 300 activities across 24 countries. We have some key highlights, for example, deploying first L-Root cluster in Egypt, and also we have been working with different type of engagement, different type of stakeholder groups, mainly composed of governments, technical community, academia, as well as civil society. And last week, as you see in this graphic, last week we posted our report showing the growth of our engagement in the region, and also you can have more information in this report. I will be sharing the link in the chat box when I'm done with this update. Can we move on? Yes. And this is another slide that I wanted to show you will see some engagement numbers based on ICANN topics and based on technical capacity building. As you know, ICANN has been heavily working on next round program because we wanted to make sure everybody has information to make informed decisions about their application. IDNA-UA is another important topic that we are heavily collaborating with our stakeholders in the region. Last but not least, DNS security is another topic that we are trying to increase awareness and build capacity. Next slide, please.

So what is next? In the first week of July, we published our next five-year regional plan, and that plan was developed in alignment with ICANN fiscal year 2026, fiscal year 2030 strategic plan. Upon further deliberations with our community members, by the way, let me pause here because I wanted to take opportunity to everyone who joined this community group and provided insights your inputs and

feedback is crucial for us to develop this plan. Upon further discussions with the group members, there are three strategic objectives covered in the plan. As you see, they are listed on this slide. And this five-year regional plan will be executed through different annual implementation plans, which will include specific initiatives, projects, and engagement efforts aligned with the region's priorities. And I will be also putting this link into chat so you can have a look into this plan. One slide again. This slide is just listing key activities that are upcoming in the following months. But just for your information, I really wanted to note that this is not the full list of our engagement in the region. I just wanted to inform you about our key activities. For example, Middle East DNS Forum is one of the significant events that we wanted to maintain every year in the region. And most of the times we are collaborating with our regional partners and we also want to be also trying to have this event in different countries every year. Middle East Adjoining Countries School on Internet Governance is another flagship event where we want to engage youth and young professionals in the region. Also, this School on Internet Governance is coordinated in collaboration with RIPE NCC and ISOC. Middle East Space, as we gather here today, we are also trying to keep our community members updated and use this space as a platform to share information about our activities and technical training seminars on different topics. One of the important project that we are getting excited this year, we are in collaboration with American University of Bahrain that is aiming to complement integration of universal acceptance into their academic curricula. This is an ongoing project that we will get into

this year. Can we move on? Yes, this is the end of my slide. I'll be happy to take if you have any further questions. And I also want to invite each and every one of you to be in touch with us, because we are not all alone in these engagement activities. And we really want to expand our reach to different countries within Middle East region. Thank you very much.

AMIN HACHA: Thank you, Seher. Before to move to start our topics of today, I will ask from the room if there are any questions want to ask for the region.

UNIDENTIFIED SPEAKER: Thank you, Amin. Just a simple question, just it caught my attention in the presentations that you mentioned something about hackathon organizations. Is it a practice that you do it on a yearly basis?

SEHER SAGIROGLU AYHAN: We are trying to do it when the chance are coming up. But of course, there is no specific timeline for it. For example, two years ago, we had this. Last year, we had this opportunity in Bahrain. A year before, we had this opportunity in different country. So we are trying to make it possible as we hear interest from regional entities and our stakeholders. If you are interested, I would be happy to have this conversation with you after the session.

UNIDENTIFIED SPEAKER Yes, definitely. Thank you.

AMIN HACHA Thank you. We have another question online from Haidar Hamzoz. Please.

HAIDAR HAMZOZ Hello, everyone. I'm so sorry not joining you in person because I'm at the airport. Sorry for the noise in the background, my flight today. So thank you so much. I'm Haidar Hamzoz from INSM. It's a digital rights foundation, nonprofit from Iraq. And I have a question to Ms. Seher. I appreciate for your slides, very informative. I like the statistics and the infographic that you use. It's amazing. But I still see that 3% in the past five years engagement with civil society. It could be very low, especially I wish to see which countries that are most active, which is which country less active so we can, as a civil society, not just playing role in Iraq, but also in the region, to encourage and bring more voices from countries that may be not active anymore or things like that. I'm not sure also how is the engagement with women, especially DNS abuse based on the gender also a trend when it comes to our region. And it should be taken into consideration. And I think for the next planning for the five years, it's very important to include more voices from the region that are not active and how we can help in that to increase the percentage of 3% into more, especially from civil society organization that are

specialized in internet governance and technical governance. So it's not a question, it's more about feedback. But I mean, the only question I have, what is the list of maybe top five countries that you see it's active in your region? So I have better understanding than how I can help as a civil society member. Thank you so much.

SEHER SAGIROGLU AYHAN

Hi. You made a very good point. To be honest, I don't capture the data based on gender. But this is something that we can do for the next five years. Very good suggestion. Thank you for that. In terms of the civil society engagement, I totally agree that there is still room to grow. But as a GSE team, as you know, we are just three people. And we're also looking to improve collaboration with organization in different countries. In that sense, if you have any suggestion, any input for that, we'll be happy to take and try to focus on some specific areas with entities. The other question, you are one of the, could you please remind me the last question you are making? The five countries. Yeah, about the countries. I didn't use that graphic. Right, but I would say that. Turkey, Bahrain, United Arab Emirates, Saudi Arabia. I don't recall each and every country. But I can look into this data, and I'll come back with you additional details supporting this list of names. I appreciate that. Thank you.

HAIDAR HAMZOZ

Thank you so much. I appreciate your help. And that's our responsibility. I'm not blaming you here. That's also part of our responsibility. That's why I'm asking. So I can bring more voices

from civil society, from countries not active, and also to share more voices from women community as well. Thank you so much, Seher, for listening.

AMIN HACHA Thank you. We have another question from Abdulrahman, please.

ABDULRAHMAN ABOTALEB Thank you so much. I'm very happy to see all of you today. And thank you, Seher, for your presentation. I just have a small question. I'm glad that the ICANN organization moved from the introductory phase to make real relationship with the community in the Middle East. But could you please just give us a hint, what is the less collaborative stakeholder in the community? And how did you address these challenges to bring all stakeholders to collaborate and in your plan? Thank you.

SEHER SAGIROGLU AYHAN Abdulrahman, if I understand your question correctly, you want me to list the type of entities that we are working in the region? Am I correct?

ABDULRAHMAN ABOTALEB No. I just want to know who's active with ICANN, who's more collaborative, the governments, the civil society, the academic sector, which stakeholder is the most collaborative, and which one is the less?

SEHER SAGIROGLU AYHAN: When we look into our collaboration, I would say that we have very close coordination with governments. And we also have very good coordination with universities. For example, in Turkey, I have been reaching out. I have been working with different universities, try to increase capacity on DNS security. Technical community is one of the strong area that we are putting a lot, because we are working with network operator groups. We are working with registrar and registries in that sense, because DNS abuse and DNS security, as you know, is one of two topics that we are trying to build capacity. Yes, I think these are the first three that I could flag to you.

AMIN HACHA: We have Baher online with us, please.

BAHER ESMAT: Yeah, thank you. Thank you, Amin. And hi, everyone. Sorry for not being able to attend in person Haidar at the airport. So just to address Abdulrahman's question, and I think to add to what Seher has said, clearly the civil society and the business community are two stakeholder groups where we need to engage more with. And when I say the business, I mainly talk about businesses outside the internet service providers or hosting providers, the broader business from organizations like banks or large corporations that run networks and so on. So and back to also Haidar's point about the civil society. So any suggestion or recommendation you can

make to help us engage better with these groups, we will be happy to work and collaborate with you. Thank you.

AMIN HACHA

Thank you, Baher. No more questions? OK, perfect. So now we go in our main topics of the session. So as we all know, DNS abuse, which include activities such as phishing, malware distribution, boot net, and spam, continues to evolve. At the same time, artificial intelligence is transforming the way we understand and respond to the threat. The question we are exploring is how can we harness AI responsibility and effectively to improve DNS abuse mitigation? The AI can process vast amount of data, recognize suspicious pattern faster than humans, and even predict malicious domains before they cause harm. But it also raises question about accuracy, privacy, and accountability. So in this session, we will look at both the opportunity and the challenge, and discuss how AI can become a trusted partner in making the DNS safer for everyone. Now, I will give the floor to our guest speaker. Sorry. I forget. I will pass the floor to my colleagues, Abdalmonem, to speak on the side of technical part introduction. Thank you.

ABDALMONEM GALILA

Actually, I will not better than our distinguished speakers for today. I just will explore some statistics about DNS abuse that are related to the Middle East areas. So what are the most attacked industries in the Middle East and the North Africa region for the first quarter of 2024? Actually, most of the sector are related to the government. As

I said, the government did massive work for the e-government services online to bring all the citizens to become online and connected. At the same time, there are a large development in financial industries related to carried also by the government. Any other project, smart cities, that covered by also by the government. So the most attacked one is the government sector here. For in comparison between the first quarter in 2023 and the quarter 2024, the first quarter at 2024, the increased of DDoS attacks. I will speak here at one of the branches of DNS abuse, not even the category. It's one branch of one of the categories of DNS abuse. We will find that if we do this attack, we'll have government sectors the most affected one. In comparing 2023 and 2024, the first quarter, we will find that it increased for the government by 34% from the previous year, same quarter, followed by energy sector, IT, telecommunication, financial, retail, oil, gas, and manufacturing.

Second thing, from year to year, comparing both years, 2023 and 2024, we will find that for the government services, the number of the percentage of increase of DDoS attacks at the government services increased by 200-plus %. Energy sector by more than 200, but less than the government. And other categories, other sectors also already have an increased number, increased percentage of DDoS attacks. So what are the attacks here breakdown by the country for the Middle East areas? I found that most of the developed economic developed countries UAE, Saudi Arabia, Iran, Bahrain, Qatar, are the most affected by DDoS attacks. And what are the protocols that are affected by DDoS attacks as well? As an

example of DNS abuse, we will find that it is trivial that or logic that HTTPS or HTTPS is the most affected one, followed by TCP and UDP, DNS, and others. At this point, I will not go to dive into more explanation about more details about these statistics. And I will leave the floor again to my colleague, Amin, to start moderating for the other speaker. Thank you.

UNIDENTIFIED SPEAKER: So you gave us an overview of the DDoS attacks. But the presentation showed a problem. How are you addressing these challenges or problems?

ABDALMONEM GALILA: Yeah, actually, I will answer this question after a while at the end of the session, how to fight DDoS attack, as one of example. But DDoS attack is not the major one for DNS abuse. It's just a branch from one of the categories. So be patient somehow. So I will cover this at the end. No worries about that. Thank you very much.

AMIN HACHA: Thank you, Abdalmonem. And now we will move to our speaker to get more hearing to her, to Samaneh, director of security, stability, and research in ICANN. The floor for you.

SAMANEH TAJALIZADEHKHOOB: Thank you, Amin and Abdelrahman. Hi, everybody in the session. I'm Samaneh, the director of security, stability, and resiliency research

inside ICANN Org. Today, I'm here to talk about, so we hear in the ICANN community a lot about AI and the use of it in DNS abuse. My presentation specifically aims to clear out misunderstandings of what AI is in this context and also outline what we do inside ICANN Org, if we use it, and if, how. So this is, I am, my team locates inside the office of CTO. Maybe you have heard the name OCTO inside ICANN Org. I am here accompanied by one of my staff member, Dr. Sion Lloyd, who is sitting on that side of the room. In case of questions, you can also go to him afterwards. OKAY, so I'm starting by saying what is not AI. The message of this slide is the static classifiers that are used for years in ML, spam filters, reputation scoring systems, anomaly detections, they are not AI. They are just simple ML. And there is nothing wrong about it's just that it's not AI. The rule-based automations, things like, they are called rule sets. Things like if this, then that logic are also not category of AI. Traditional natural language processing pipelines, featured engineering models, supervised deep learnings, they are all subcategory of machine learning, as well as the predictive models. These are narrow, deterministic, and require explicit training and maintenance. In a lot of the cases where the term AI is used these days, these models fit the best and also are less resource consumed. What is or begins to resemble AI are generative models. And by the way, you hear that we use, so in the context of the term AI, most of the use cases refer to generative models, the GPTs. And I think people are less specific when they are talking about it. But GPTs are the generative models. Large language models are one example of those. Their specifications is that they are autonomous agents. So

they plan, decide, execute. Yeah. Of course. Thank you. They're reinforcement learning systems. So they optimize strategy by automatically and dynamically change labels and labels. So this doesn't necessarily involve a human or manual training of a set. The multimodal reasoning models, where they digest text, vision, and code to infer relationships and behavior. And also, the last category are the meta-learning or self-improving pipelines, where they're modifying their own training processes based on performance that they see. These systems are adaptive decision-making systems, not just pattern-finding or pattern-feeding.

What's the shift when these systems came into industries, also including our system, in terms of security in general, but specifically DNS abuse? So their main function, a GPT's main function when it comes to DNS abuse, is that they lowered skill and cost barriers, meaning that entry barriers are lower. A lot more people can launch attacks or understand it and attempt to launch it. Early stages of an attack cannot be automated and optimized, so scale and lower barrier to entry. And DNS abuse in the infrastructure layer is the one most affected, because it's coding for a malware distribution or botnet command and control. Instructions are easier now to generate and to send around. Most defenses on the other side, at least when it comes to DNS abuse, still rely on ML, not autonomous intelligence. Again, disclaimer, I'm not saying one is better than the other. I'm just explaining the landscape that there is. So I'm going to walk you through the whole attack chain before and after GPTs came into this space. This is not only the use of domains, but from

the whole chain, from creating a profile, writing a code, etc. So before GPTs, you had to have manual intelligence systems. Now they are LLM-driven profiling. So the language models are used into profiling what scaling and profiling what the target should be. Then the weaponization, so actually targeting the attack. Used to be that generic phishing kits. In this case, I'm only discussing phishing as an example. Generic phishing kits would be sold in underground markets. They had to be created by professionals who knew how to do it, professional coders or SMEs in this space. Now, with LLMs, creating kits are easy. Not only that, but also can be easily personalized due to the help of large language models. Also, deep fake is easier. In terms of delivery, it used to be delivery of an attack, let's say delivery of a phishing attack. It used to be static email or smishing SMS. Now, its adaptive delivery would be via multiple channels, polymorphic. Exploitation used to be known exploits, so exploits that are known by certain group of attackers in the wild. Now, AI assists into finding exploits that are not necessarily known by the whole landscape or generating new exploits. I think the main message is clear. As you see, the difference between before and after, AI helped in scale and speed.

Again, an example of phishing in terms of how scale is different. Now, maybe you have noticed already from the phishing emails you receive, they look very legit. They are way more personalized from the accounts you probably have subscription at. Deep fakes at the video and voice level for CEO fraud is now way more prevalent. The same goes for adaptive iteration to bypass spam filters for emails.

For example, we used to not see a lot of spam because our filters would detect it, but now the emails are so personalized that it's harder to detect. When we are talking about spam, spam filtering goes back to more than 30 years ago, this technology. How they help specifically to amplify DNS abuse? Well, the attack surface is expanded. What do I mean by attack surface? Simply domain names. Domain names can be registered easier, created easier, and also content can be created easier using the models. The ML-based detectors, so the static detectors that I explained, face adversarial examples and drift, so it's harder for them to detect at this amount and at this level of personalization. Response windows shrinking from hours to minutes because of the scale of the attacks and also how easy it is to create a phishing chain. Response windows need to adapt to it, and also there is a need for behavior correlation across the DNS providers, the content providers, hosting providers, and certificate authorities, which is something that would affect this space a lot. On the defense side, the impact would be, for example, things that we also will be looking into, algorithmic discovery of domain variants, because string registrations and also patterns in string registrations are now easier to do, and we ourselves at SSR OCTO are doing research on that to find domains that are associated with each other, so basically a bunch of domains. Generative DGAs, blending real world to evade filters, instant deployment of SSL certificates, which has always historically been a loophole in malware and phishing distributions, and also they are autonomous management of life cycle, so everything basically, most of the things would be soon autonomous management, which would really

impact defense. In this space that we are talking about, most of the AI defense are now supervised ML, machine learning models, correlations, statistics, and pattern recognitions that are not reason or planning autonomously. What would it be if GPTs come to the defense side? They would be reinforcement systems adapt in real time, and also generative red teams, blue teams, purple teams, etc.

So what are the considerations for using AI in this space for us, actually? There are many, as Amin and Abdulrahman already pointed out. Some of the ones that I thought are less talked about in this space are the expectations. When the actors in this space come and say we have AI-powered detection, that creates a certain expectation. So we have to be careful if we are just using machine language models, using the term AI-powered detection would only create, would only weaken your position, because now the attackers think that you have more advanced technology, whereas you don't. So that's one thing to take into account. And my personal capacity, I'm of the opinion that AI-powered detection is not necessarily better and more advanced, but it's important to manage expectation. Accountability. When autonomous agents make a decision and they execute it, the biases that it creates in the data or the rule sets need to be taken into account. This is a topic that has not been discussed in this community, and I think this week I tried to ask this question, but it was clear that it has not been taught about yet. Which is no problem, but it's good to bring into the attention of our community members. Allocating resources. So it's important to be careful for the policy bodies specifically not to chase

hype, instead of funding interpretable, audible machine learning models, which could work in certain cases best. And also, we should be mindful about not confusing regulation. Legal frameworks for autonomous systems get applied to statistical models, creating noise in this space.

Now, what ICANN Org? Is ICANN Org using AI? There is no short answer to that. If I need to give a short answer, the short answer is no. We are not using GPTs in decision-making in terms of autonomous agents. No, ICANN Org is not using that, and I haven't heard of any plan doing that. However, we are using large language models to identify patterns or build certain things for our research. We also test if there is any need to use large language models over traditional ML models. What would be the use of it? What would be the cost of using those resources? Is it beneficial? We use ML models to predict work for DNS abuse, things like scores, predicting malicious actors, etc. However, we are also, in any ways, practicing with LLMs to learn the new models, the downsides, the drifts, and also to see if and when they will be effective for our use cases. In the next couple of slides, I'm going to walk you through some of the work that we are doing in our group. One of the most recent works that we are doing is discovering associated domains. I'm sure during this week you have sat in sessions where there were discussions about upcoming PDPs, the Infermal report, and also what should be the content of these PDPs. One of the key points there were discovering associated domains. So, if domains can be registered in bulk, which are the ones that are associated with each other for DNS

abuse? So, registered by one attacker. We are using many features, both temporal and lexical, fed into a random forest, trained on manually attacked associated domains. This is just a simple ML model, and the features are the ones listed on the slide. In another work, we are working on measuring DNS abuse uptime. This is the amount of time that a domain is up and running from the moment that it's detected as being malicious. We've published our work. It's peer-reviewed and published in IEEE CNS. There has been work on this topic in the community for a couple of years. We are building on top of that, building more robust measurement tools. Also, this is not a straightforward question, because attackers have all kinds of techniques to suggest that the domain is not up any more, changed location, changed website, and we are building a tool that detects all of that. This specific metric would talk to how registries and registrars are mitigating, how fast they are mitigating domains for DNS abuse. Then we also work on parked page evaluation. This is the work of Sion, who is sitting in the room now. Earlier, work in this topic has been published also in IEEE SMP workshop. We have methods to identify parked domains, detect different types, see new trends, and how is this used to facilitate DNS abuse. That was about what we do in the SSR OCTO team. Now, going back to the main topic of this presentation, in short, it's important for our community to separate the AI hype from measurable ML performance. We suggest that if community members are going to adopt tools, which is good, at least audit for true adaptability and also for hallucinations of the model. Prioritize detection fusion across DNS content and certs. Also, on the defense side, these models, the

adaptability of them, are also really good for exercises, which could also be for DNS abuse. Last but not least, it's important to educate ourselves, and anybody who uses a business query to get a business response from a model for a set of data is to use precise language and do additional research on what the models give you. Because internet these days, and also specifically models, they hallucinate a lot, and it's full of, I'm going to be even more, misinformation or hallucinations of the models. That would be it from my side. I'm happy to take questions if there are any.

ABDALMONEM GALILA Thank you very much, Samaneh, for the presentation. Actually, I learned some points from your presentation. The first one is that I couldn't use GPTs for decision-making. The first one. GPTs itself could be one of the sources of DNS abuse. Second thing is that I think there is no ethical we have ethical hacking. Hacker and ethical hacker. We don't have any ethics related to the use of domain name or these GPTs in order to mitigate from the early beginning such kind of DNS abuses. So, do you have this document of the use of DNS abuse that's already in place, maybe at ICANN or in other communities like ITU or other? Thank you.

SAMANEH TAJALIZADEHKHOOB Thank you for your question, Abdalmonem. Just a point that I mentioned that ICANN Org is not using GPTs for decision-making, but they can be used for decision-making. It's just that they should be taken. The result of the business question should be taken with a

grain of salt. That's why I said it's important that stakeholders who use it do their own research as well and do not take everything that the model gives for granted, as in the absolute truth. ICANN org does not yet have a document, but we are working on having one. So stay tuned for that.

ABDALMONEM GALILA: This document will be a guide for all registries in order to follow, in order to use GPTs. There will be enough encouraged to use GPTs and it will be secure. Then go for using GPTs for decision or for making some sort of codes in order to develop something and to include something like this. Thank you very much. Also, for other things that you said inside your presentation, use it to mitigate DNS abuse. What Samaneh said as an example is that we need to really monitor your domain names from time to time on a regular basis. This is one of the kinds of mitigation. You need to update your software and your systems in order to be most updated to mitigate such kind of abuses. The second guide I will complete after this. Thank you, Amin.

UNIDENTIFIED SPEAKER: When you say that ICANN org, they don't use AI in their decision-making, what do you mean exactly? Decision-making policies, for exampleDid that answer your question?

SAMANEH TAJALIZADEHKHOOB: In the context, so the autonomous agents of the GPT models are at the moment in different industries or companies are used for making autonomous decisions. So in different life cycles, different functions, what I meant that ICANN org has not adopted any autonomous agents and does not have plan to do it for any decision-making processes.

ABDULRAHMAN ABOTALEB: Thank you so much for this insightful presentation. I just want to ask from your perspective, what is the most realistic short-term step that the Middle East community can take to start integrating AI responsibly into DNA security work in our infrastructure?

SAMANEH TAJALIZADEHKHOOB: I'm not sure if you would like the answer, but I think the first assessment should be is it needed to be integrated? Because we are hearing this word a lot and it's kind of first assessment should be does it add value to the current systems, defense systems that you have and if so, how? For example, in terms of one of the use cases that I can think of is the scaling issue. If phishing is going to be scaled into a larger scale, the defense systems should adapt to it. If you are having a defense against phishing, then you need a system that can adapt to that scale. Then you need GPTs. But if not, then there is hardly a use for it. Or if you are a small registry or registrar that do not necessarily need the cost of scaling. So the first thing to look into is what is the problem you are trying to solve and what would be the

	added value of generative models as a tool, similar to other tools out there in the case of your specific problem.
AMIN HACHA	Thank you. Any other questions?
UNIDENTIFIED SPEAKER	Hi, I just wanted to know why you are not using autonomous agents?
SAMANEH TAJALIZADEHKHOOB	Inside ICANN Org, there is no use. I am talking from the research team's perspective, but at the moment there is no use case for us to do that. They are mostly used for automating decisions that require scale and we are in a multi-stakeholder model. So there is inside our type of working, there is no use case really to do it.
AMIN HACHA	Any more questions? Do we have anything online? No?
SEHER SAGIROGLU AYHAN	Thank you. This is Seher for the recording. I just wanted to forward an apology from Christian because he is not able to make it. So we have more time for discussion. Thank you.
AMIN HACHA	Thank you, Seher. Thank you for our main speaker and all who contributed by question. Now we'll move to what's next. So it's clear

that AI is not just a trend, it's becoming an essential tool. What's next for our community is to build collaboration between technical expert, policy maker, registry, registrar, and researcher to ensure that AI tools are transparent, ethical, and effective. We also need to focus on capacity building in our region. So that Middle Eastern stakeholders can develop and deploy AI-driven solution locally, tailored to our language, our need, and our internet environment. Let's continue this dialogue beyond this session. I will move to my colleague, Abdalmonem, to put his point of view about what next we expect to do. Please.

ABDALMONEM GALILA Actually now, as I continue work of DNS abuse, DNS abuse now with emerging technologies at the stage of middle east space alongside other important topics or important issues that will be handled. And at this time, we will cover more details about this at the mailing list and already going over that. And the second topic for today, the second bullet that will be covered for ICANN 84. As usual, we have ICANN fellows.

CHARBEL CHBEIR Thank you. Hello, everyone. My name is Charbel Chbeir. I'm a lawyer specializing in cyber security and digital transformation. I'm also a [inaudible] international expert. I also serve as president of the ISOC Lebanese chapter. I have a previous participation in ICANN. But this is my first time participating as a fellow. Once a fellow, always a fellow. As you all know, ICANN is a world unto itself. Even when we

feel knowledgeable about it, delving deeper reveals that we need to enhance and deepen our understanding to contribute effectively in the right areas. That's why I decided to apply for the fellowship. It serves as the best starting point to familiarize myself with the vast community. Today, I am proud to be a fellow here at ICANN with our lovely mentor, Glen de Saint Gery. As we approach the end of the annual general meeting, it will conclude tomorrow. I can confidently say that it has been truly rewarding. I'm also pleased to have the opportunity to speak in this session about harnessing AI and strengthening DNS, abusing mitigation, where I will highlight the Lebanon perspective and initiative in the crucial area. Lebanon, like many other countries in the MENA, faces significant challenges in combating DNS abuse. With increasing reliance in digital infrastructure, our country recognized the importance of strengthening DNS security. Artificial intelligence plays a vital role in enhancing DNS abuse mitigation by leveraging machine learning algorithm and predictive analyst. We can detect anomalies, predict, analyze, automate response. Now, every technical and technological method that we do without robust legal framework, there is a code that I want to say in French, and I will translate it into English. Anything we do in technical perspective doesn't cover whatever we can to reduce the threat of any attacks on cybersecurity. Therefore, in the laws, one of the most important books in cybersecurity said in the preamble, there is no way to cover any kind of dangers without leveraging or doing a robust legal framework. In Lebanon, we're working to establish a robust legal framework that aligns with international standards like ISO 270001,

GDPR, DNS abuse standards, EU directive of artificial intelligence. We have recently established a ministry of technology and artificial intelligence that I myself am advisory to the ministry. The ministry of technology and AI in Lebanon is working to harness the potential of AI to drive digital transformation and enhance cybersecurity. The ministry initiative aims to develop AI, power solution, build capacity, and we are doing collaboration with the regional countries. In conclusion, by harnessing the power of AI, othering the robust legal framework, and collaborating regionally, we can strengthen DNS abuse mitigation and create a safer online environment for all. Thank you very much.

AMIN HACHA Thank you. Now, please, go for it.

[SINA] Hello, everyone. It's [Sina] from Iran. Now living in Germany, doing my PhD. Back in Iran during my bachelor's degree, I was working as a network engineer in an ISP, and currently, during my PhD., I'm doing research on various kind of Internet security measurement. We basically measure the security estate of the host on the Internet, different kind of network devices, routers, switches, end hosts, servers, etc. Glad to be here among you, and there is much to be done in our region. Hope that we can do something to improve. Thank you.

AMIN HACHA Thank you, Sina. And now, please, Riyadh.

RIYAD Zehrah Thank you. Riyad Zehrah from Yemen. I would like to take this opportunity to say it is the first time that I'm here. I would like to take this opportunity to say it is the first time I meet my citizen, Abdulrahman. This is the first time we group in the same location. Welcome, Abdulrahman. During this, the event, I have learned so many things. I have learned a lot of things. I have learned a lot of things. The country has so many challenges. I will hopefully use what I learned, the connection I have gathered, to improve the quality of life of my citizens. I would like to take this opportunity to say thank you. The mission is big, I know, but I ask from you and from God.

FURKAN ÇOLHAK Hello everyone. Furkan Çolhak I'm student in applied cybersecurity currently in Berlin. At the same time, I'm a researcher at the Istanbul [inaudible] University, critical infrastructure and cybersecurity research center. As we all know, DNS is a critical infrastructure of the internet. I'm currently focusing on developing some AI tools on enhanced DNS security. Thank you for everything.

FARZANEH BADII I just wanted to say that the issues of mitigation of DNS abuse is very valid and we should focus on that. But another thing in the Middle East we struggle with is the registrants and end-users' digital rights and access to domain names. I think that we need to also, in parallel,

or at the same time that we look at mitigation of DNS abuse, we have to look at rights-respecting mechanisms and see how mitigation mechanisms have actual rights implications on domain name registrants and end-users in the Middle East. And that's it. I don't think we have much time. If we can put down the agenda as well later on, that would be great. Thank you.

SEHER SAGIROGLU AYHAN Thank you, Farzaneh, for pointing this out. When I look into this room, I see so many friends from civil society organizations, technical communities in the region. I think it is time to have further communication between us. For example, we have friends from ISOC chapters, we have friends from NOG groups. I think it is time to coordinate and how we can start discussion or improve this coordination. And I also wanted to acknowledge the presence of our fellows because fellowship program is one of the programs that we are always taking opportunity to meet with new people, young and young professionals and also trying to reach out new audiences. I appreciated your time to making it. I hope that we could have this session dedicated for the upcoming space sessions. Thank you.

AMIN HACHA Thank you, Seher. Anybody want to ask any comments? As we come to the end of the session, I want to thank everyone, our speaker, all our participants in person and online, and the organizing team for making this discussion so engaging and valuable. Let's keep

working together, learning together, and building a safer, more resilient Internet for our region and the world. Thank you again.

[END OF TRANSCRIPTION]